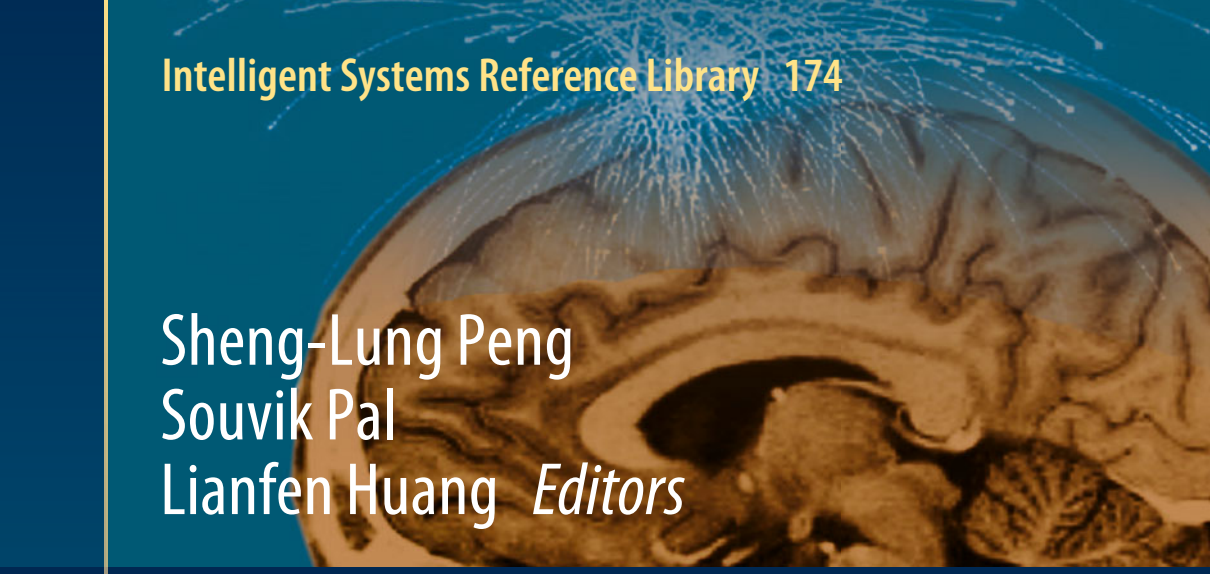
Intelligent Systems Reference Library 174



Sheng-Lung Peng
Souvik Pal
Lianfen Huang *Editors*

Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm

Springer

Intelligent Systems Reference Library

Volume 174

The aim of this series is to publish a Reference Library, including novel advances and developments in all aspects of Intelligent Systems in an easily accessible and well structured form. The series includes reference works, handbooks, compendia, textbooks, well-structured monographs, dictionaries, and encyclopedias. It contains well integrated knowledge and current information in the field of Intelligent Systems. The series covers the theory, applications, and design methods of Intelligent Systems. Virtually all disciplines such as engineering, computer science, avionics, business, e-commerce, environment, healthcare, physics and life science are included. The list of topics spans all the areas of modern intelligent systems such as: Ambient intelligence, Computational intelligence, Social intelligence, Computational neuroscience, Artificial life, Virtual society, Cognitive systems, DNA and immunity-based systems, e-Learning and teaching, Human-centred computing and Machine ethics, Intelligent control, Intelligent data analysis, Knowledge-based paradigms, Knowledge management, Intelligent agents, Intelligent decision making, Intelligent network security, Interactive entertainment, Learning paradigms, Recommender systems, Robotics and Mechatronics including human-machine teaming, Self-organizing and adaptive systems, Soft computing including Neural systems, Fuzzy systems, Evolutionary computing and the Fusion of these paradigms, Perception and Vision, Web intelligence and Multimedia.

** Indexing: The books of this series are submitted to ISI Web of Science, SCOPUS, DBLP and Springerlink.

More information about this series at http://www.springer.com/series/8578

Sheng-Lung Peng · Souvik Pal ·
Lianfen Huang
Editors

Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm

Springer

Editors
Sheng-Lung Peng
CSIE Department
National Dong Hwa University
New Taipei City, Taiwan

Souvik Pal
Department of Computer Science
and Engineering
Brainware University
Kolkata, West Bengal, India

Lianfen Huang
Department of Communications Engineering
Xiamen University
Xiamen City, Fujian, China

ISSN 1868-4394 ISSN 1868-4408 (electronic)
Intelligent Systems Reference Library
ISBN 978-3-030-33595-3 ISBN 978-3-030-33596-0 (eBook)
https://doi.org/10.1007/978-3-030-33596-0

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The main aim of this book is to bring together leading academic scientists, researchers, and research scholars to exchange and share their experiences and research results on all aspects of IoT ecosystems. It also provides a premier interdisciplinary platform for researchers, practitioners, and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of IoT and analytics. This edited book covers a wide range of IoT-enabled technologies. This book aims to explore the insight paradigm of the IoT technologies which will bring a smooth platform for the scope of industry–academia. The wide-range contents will differentiate this edited book from others. The contents include functional framework and protocols for IoT-based system, intelligent object identification, intelligent sensors, 6LoWLAN, wearable sensors, WBAN, IoT communication and domain model, RFID technology, data aggregation, IoT service life cycle, microVMs, big data analytics, transportation protocol, energy-aware protocols, IoT device and component integration, data-intensive security and privacy, self-adaptive cyber-physical systems in IoT-related topics. The above topics are likely to be embedded with the IoT-enabled technologies for future generation automation.

The book is organized into 6 parts and 24 chapters.

Chapter 1 discusses IoT technologies which are mixture of sensors and actuators are used by the IoT networks to formulate the system intellectual and innovative. IoT is a well-balanced platform where everyday device procedures turn into intellectual, everyday communication turns into helpful, and everyday processing turns into intelligent. Although internet of things still in the hunt for its very own pattern, shape, and architectural structure. IoT helps in developing most powerful industrial systems, various applications in household, smart city, agriculture, healthcare centers, environmental and transportation, many more.

Chapter 2 integrates these roles in smart architecture and applies it to probe critical problems in domains such as transport, energy, environment, and telecom. The discussion on IoT-enabled system proposes novelties such as digital divide of supply versus demand and workflow; graph-based learning of state space

formulates energy efficiency of IoT node. The case study for vehicular traffic reveals that IoT-enabled system offers reliable, easy to scale, AI integrated and efficient communication that can complement performance with the existing networks.

Chapter 3 deals with IoT architecture which describes the gateways or fog, an analysis engine, and an insight layer. These layers are embedded between the cloud and the edge devices. The insight layer employs various learning modules onto the data in the cloud. The fog layer is the most significant layer that improves the efficiency of IoT architecture.

Chapter 4, firstly, exposes the all-applicable semantic interoperable standards in smart city applications to become a semantic Web of things in comprehensive survey manner. Secondly, the unsupervised clustering mechanisms are discussed for performing analysis on IoT sensor data and highlight with much more attention toward the issues, challenges, and current research directions. Finally, this chapter concludes with proposed semantic reasoning mechanism for unified accessible resources in IoT smart city applications.

Chapter 5 presents the overview of wearable sensors for tracking physiological and physical changes in daily life, their basics, and applications. Wearable sensor-based systems have enormous potentials to be completely explored, and it is anticipated that advancement in technologies will afford the transformation how health care will be in the future. It highlights the significance of localization in on-body area network, and it gives an overview about evaluating the performance of localization systems. It also presents the several types of sensors and methodologies to fuse the data generated by sensors. Since we foresee a future where the existence of miniature devices communicating through packet radio in both indoor and outdoor environments.

Chapter 6 gives a review on the prevailing techniques that use IoT sensors to monitor and prevent perishable food spoilage. An outline of suggestions to increase functioning of sensors using new methods has also been listed.

Chapter 7 presents a comprehensive description of the technical opportunities and challenges in the design of sensor information processing systems for wearable. A systematic survey of the state-of-the-art architectures for sensor fusion for different application classes of wearables is presented. A discussion on design considerations for architecting sensor processing systems, including hardware, networking protocols, and algorithms at the edge, cloud level is provided. The chapter is concluded with a discussion on innovation directions in smart sensing and information processing in wearable devices.

Chapter 8 applies in particular to smart computing on a big scale such as cyber-physical systems (CPSs), cloud computing, the Internet of things (IoT), the Internet of everything (IoE), robotics (mechatronics), renewable energy systems, autonomous vehicles, and intelligent cities/devices. CPS integrates networks, computations, and physical processes to control process, respond, give feedback, and adapt to changing conditions in real time. Success of Industry 4.0 is confronted by disruptive CPS difficulties regulated by IoTs and IoE; integration with machine learning, IoT, and cloud computing and growing but challenging concentration on

the main fields of big data analytics, virtualization, and automation. The chapter synthesizes existing literature to highlight drastic alterations that Industry 4.0 will apply on manufacturing systems and processes.

Chapter 9 reviews the available cloud IoT literature and presents a holistic vision on the cloud IoT integration components. The chapter also presents seamless applications dispensed by cloud IoT platform and contemplates discussion on factors driving cloud IoT integration. The work in this chapter also highlights security issues affecting IoT-layered architecture including vulnerabilities inherent in the cloud.

Chapter 10 addresses various healthcare applications which are IoT-based, along with some healthcare technologies. Many promising and enabling technologies are nowadays working for IoT-based healthcare solutions, and thus, it is important to put some lights on those technologies. In this respect, the following analysis focuses on some core technologies which have the prospective to revolutionize IoT-enabled healthcare services.

Chapter 11 adds the following things namely learning and evaluation of IoT-supported parameters such as hardware and cloud platforms to determine the suitability for e-healthcare services, analysis of existing IoT-based wearables solutions for e-healthcare Identification of encounters related with IoT-aware e-healthcare domain, analysis of the integration of WIBST and IoT attained from this arduous study. The challenges and benefits of IoT-based applications for healthcare have also been outlined later in the chapter.

Chapter 12 deals with IoMT environment, a private blockchain network is created containing all the participants of a hospital including doctors, laboratory technicians, patients, and clinical laboratories, etc. There exists no necessity to carry the report by the patients during every visit, as the data is already available in the network. The data is completely decentralized to avoid failure, data loss and to provide faster recovery. Whenever a change is attempted by a third person in the database, a notification is sent to all the members of the group.

Chapter 13 deals with the contemporary available innovations which associates the data mining from different Internet-oriented bioinformatics tools and techniques, server leads to genotype remodeling, in silco therapeutic approaches, drugs' discovery along with the evolutionary trends for mass community services and better future implication. A significant drive also taken to highlighting the possibility for upcoming research on IoT-based healthcare centered laid on numbers of well-known topics and challenges linked with intelligent cyber-physical smart universal contexts.

Chapter 14 attempts to develop a model based on "quality function deployment (QFD)" approach using IoT platform to augment the real-life data management system which would interact and share between all the stakeholders conforming the spirit of selective data privacy and confidentiality. This would also strive to bring reforms in the existing process of planning, strategy formulation, and project implementations.

Chapter 15 is painted the running programs in India and also depicted possible nomenclature and program with industrial environment and context as per the international trends. The future potential of such program has been depicted with SWOT for making a true Digital India with smartest and effective way.

Chapter 16 enumerates the IoT data management frameworks, challenges, and issues. Also, deployment of IoT data management for smart home and smart city is described.

Chapter 17 deals with interconnecting objects of IoT. Firstly, this chapter discusses the pragmatic implementation scenario of a SIoT platform. This is done by analyzing the various IoT research work till date and in turn listing out the major characteristics that could be reused for our research. Secondly, this elaborates how the IoT objects form interrelationships autonomously. This has been done by taken up various concepts of relationship formation such as parental object relationship, co-location object relationship, co-work object relationship, ownership object relationship, and social object relationship. Thirdly, this chapter discusses the interlinking of IoT with the established concept of social networking analysis (SNA), wherein this chapter is interlinking objects of IoT with the rules built thorough SNA, thus forming a human-bound relationship with their objects. And finally, this chapter deals with the new challenges and open issues of SIoT with the architectural elements that will pave the way toward this future-driven SIoT paradigm.

Chapter 18 provides state-of-the-art review of the latest researches about effective data management in IoT ecosystem. Finally, the issues and challenges present in effective data management, information linkage, and security of IoT devices and system are highlighted along with the future research directions.

Chapter 19 discusses the security issues in IoT. With the advent of the Internet of things (IoT) era, the size of the network has extended beyond all the limits that have ever existed. It has spread all over the world. Perception layer that is the lowermost layer in IoT architecture is characterized by wireless sensor networks (WSNs) and resource-constrained embedded devices. These devices are fairly limited in terms of memory, computation, power, and energy. It makes them vulnerable to a large number of attacks. Information security is of utmost importance as IoT systems automate critical applications such as traffic control. A number of solutions have been provided by the engineers and researchers such as blockchains, intrusion detection systems, lightweight cryptography, and various protocols.

Chapter 20 contributes a thorough insight into the possible threats to time synchronization in backbone WSN of IoT, existing security measures with qualitative and quantitative analysis, and their scope and limitations. This will further help the research community to develop lightweight and efficient secured time synchronization protocols for IoT.

Chapter 21 discusses the security vulnerabilities in WSN with the use of blockchain technology. Primarily blockchain applied in support of recording fiscal transactions where connections encoded (pre-arranged) and kept back with participants, on one occasion transaction confirmed by blockchain it cannot be modeled

or else wipe out; if any modification is applied it is easy to map out and recognize. Blockchain technology position in IoT security, challenges, and research problems is discussed in brief.

Chapter 22 presents a review of IoT security and forensics. It started with reviewing the IoT system by discussing building blocks of an IoT device, essential characteristic, communication technologies, and challenges of the IoT. Then, IoT security by highlighting threats and solutions regarding IoT architecture layers is discussed. Digital forensics is also discussed by presenting the main steps of the investigation process. In the end, IoT forensics is discussed by reviewing related IoT forensics frameworks, discussing the need for adopting real-time approaches and showing various IoT forensics.

Chapter 23 discusses security vulnerabilities with blockchain technology to bring transaction processing and intelligence to devices as well as privacy issues, scalability and reliability problems in the IoT paradigm. The technology inclusion of blockchain and the IoT in the government system could accelerate communication among citizens, companies, and governments.

Chapter 24 discusses security issues in IoT. Different IoT applications generate enormous amounts of data and also require Internet connectivity all the time for communication between the devices. As the data is communicated via wireless networks, the major challenge lies in the domain of security such as data confidentiality, data reliability, data authentication, privacy. Blockchain can be the missing link for settling privacy and reliability issues of IoT. The connected devices and their communications can be tracked and stored on the tamperproof ledger of blockchain to ensure reliability and data security of IoT network.

We are sincerely thankful to Almighty to supporting and standing at all times with us, whether it is good or tough times and given ways to concede us. Starting from the call for chapters till the finalization of chapters, all the editors were given their contributions amicably, which it is a positive sign of significant teamworks. The editors are sincerely thankful to all the members of Springer especially Prof. Lakhmi C. Jain and Prof. Thomas Ditzinger for providing constructive inputs and allowing an opportunity to edit this important book. We are equally thankful to all the reviewers who hail from different places in and around the globe shared their support and stand firm toward quality chapter submission.

New Taipei City, Taiwan — Sheng-Lung Peng
Kolkata, India — Souvik Pal
Xiamen City, China — Lianfen Huang

About This Book

The edited book *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm* is intended to discuss the evolution of future generation technologies through Internet of things. The main focus of this volume is to bring all the related technologies in a single platform, so that undergraduate and postgraduate students, researchers, academicians, and industry people can easily understand the IoT-enabled technologies.

This book uses data and network engineering and intelligent decision support system-by-design principles to design a reliable IoT-enabled ecosystem and to implement cyber-physical pervasive infrastructure solutions. This book will take the readers on a journey that begins with understanding the insight paradigm of IoT-enabled technologies and how it can be applied in various aspects. It walks readers through engaging with real-time challenges and builds a safe infrastructure for IoT-based future generation. This book helps researchers and practitioners to understand the design architecture through IoT and the state-of-the-art in IoT countermeasures. It also differentiates heterogeneous platforms in IoT-enabled infrastructure from traditional ad hoc or infrastructural networks. It provides a comprehensive discussion on functional framework for IoT, object identification, IoT domain model, RFID technology, wearable sensors, WBAN, IoT semantics, knowledge extraction, and security and privacy issues in IoT-based ecosystems. This book brings together some of the top IoT-enabled experts throughout the world who contribute their knowledge regarding different IoT-based technology aspects. This edited book aims to provide the concepts of related technologies and novel findings of the researchers through its chapter organization. The book explores IoT-enabled insight paradigms which will be utilized as a part of betterment of mankind in the future era. Specifically, the far-reaching references of various works and executions will be observed to be significant accumulations for engineers and organizations. The primary audience for the book incorporates specialists, researchers, graduate understudies, designers, experts, and engineers who are occupied with research and healthcare-related issues. The edited book will be organized in independent chapters to provide readers great readability, adaptability, and flexibility.

Key Features

1. Addresses the complete functional framework workflow in IoT-enabled ecosystem.
2. Explores basic and high-level concepts, thus serving as a manual for those in the industry while also helping the beginners to understand both basic and advanced aspects in IoT-enabled ecosystem-related technology.
3. Based on the latest technologies, and covering the major challenges, issues, and advances in IoT-based environment.
4. Exploring intelligent object identification and object discovery through IoT ecosystem and its implications to the real world.
5. Explains concepts of IoT communication protocols, 6LoWPAN, M2M technology, and RFID in IoT environment for the betterment of the smarter humanity.
6. Intelligent data processing and wearable sensor technologies in IoT-enabled ecosystem.
7. Exploring IoT service life cycle, microVMs, big data analytics in IoT-based environment.
8. Enabling IoT semantics, knowledge extraction, and analysis.
9. Exploring security and privacy issues and challenges related to data-intensive technologies in IoT ecosystem.

Contents

About the Editors

Sheng-Lung Peng is Full Professor of the Department of Computer Science and Information Engineering at National Dong Hwa University, Taiwan. He received the BS degree in Mathematics from National Tsing Hua University and the MS and Ph.D. degrees in Computer Science and Information Engineering from the National Chung Cheng University and National Tsing Hua University, Taiwan, respectively. His research interests are in designing and analyzing algorithms for combinatorics, bioinformatics, and networks.

He has edited several special issues at journals, such as Soft Computing, Journal of Internet Technology, Journal of Computers, and MDPI Algorithms. He is also Reviewer for more than 10 journals such as IEEE Transactions on Emerging Topics in Computing, Theoretical Computer Science, Journal of Computer and System Sciences, Journal of Combinatorial Optimization, Journal of Modelling in Management, Soft Computing, Information Processing Letters, Discrete Mathematics, Discrete Applied Mathematics, Discussions Mathematicae Graph Theory, and so on. He has about 100 international conferences and journal papers.

He is now Director of the Library and Information Center of NDHU and Honorary Professor of Beijing Information Science and Technology, University of China. He is Secretary General of Institute of Information and Computing Machinery (IICM) in Taiwan. He is also Director of the ACM-ICPC Contest Council for Taiwan. Recently, he is elected as Supervisor of Chinese Information Literacy Association and of Association of Algorithms and Computation Theory (AACT). He has been serving as Secretary General of Taiwan Association of Cloud Computing (TACC) from 2011 to 2015 and of AACT from 2013 to 2016. He was also Convener of the East Region of Service Science Society of Taiwan from 2014 to 2016.

Souvik Pal has completed Ph.D., MCSI; MCSTA/ACM, USA; MIAENG, Hong Kong; MIRED, USA; MACEEE, New Delhi; MIACSIT, Singapore; MAASCIT, USA, and is Associate Professor at the Department of Computer Science and Engineering, Brainware University, Kolkata, India. He received his B.Tech. degree in Computer Science and Engineering from West Bengal University of Technology, Kolkata. He has received his M.Tech. and Ph.D. degree in Computer Engineering from KIIT University, Bhubaneswar, India. He has worked as Assistant Professor in Nalanda Institute of Technology, Bhubaneswar, and JIS College of Engineering, Kolkata (NAAC "A" Accredited College). He has also worked as Head of the Computer Science Department in Elitte College of Engineering, Kolkata.

He has published several research papers in Scopus-indexed International journals and conferences. He is Editor of seven Elsevier/Springer/CRC Press/Apple Academic Press Books and Author of one cloud computing book. He is Organizing Chair and Plenary Speaker of RICE Conference in Vietnam and Organizing Co-convener of ICICIT, Tunisia. He has been invited as Keynote Speaker in ICICCT, Turkey. He has served in many conferences as Chair, Keynote Speaker, and he also chaired international conference sessions and presented session talks internationally. He also serves as Reviewer and Editorial Board Member for many journals and IEEE/Springer/ACM conferences. His research area includes cloud computing, big data, wireless sensor network (WSN), Internet of things, and data analytics.

Lianfen Huang has completed Ph.D. and received her B.S. degree in Radio Physics in 1984 and Ph.D. degree in Communication Engineering in 2008 from Xiamen University, Xiamen, Fujian, China. She is now Professor and Doctoral Supervisor in Department of Communication Engineering, Xiamen University. She was Visiting Scholar in Tsinghua University in 1997 and the Chinese University of Hong Kong in 2012. She is now Key Laboratory Director of Digital Fujian on IoT Communication, Architecture and Security Technology, and has hosted and participated in number of national funds, 863 national key projects and enterprise projects. She has more than 20 licensed patents and published over 100 SCI or EI papers. Her current research interests include IoT and wireless of embedded system, communication network, and signal processing.

Part I
IoT Foundation and Framework

Chapter 1
Internet of Things: Foundation

Bhanu Chander and Gopalakrishnan Kumaravelan

Abstract The word internet of Things (IoT) is disclosed as frequent technologies as well as research disciplines that allow the internet to reach out to the existent world of physical objects. Uninterrupted innovations in computer networks, hardware's, micro-electro-mechanical systems and software's along with connection solutions since the last decade lead to expansion of the internet of Things. Wireless Sensor Networks (WSNs) essential to IoT by traverse the disparity within the physical as well as cyber worlds. In IoT, Wireless sensor networks (WSNs) are exceptionally indispensable sensing activities translate physical phenomenon into digital signals moreover transmit these signals to the interrelated cyber-world for suitable comfortable processing and analytics. A mixture of sensors and actuators are used by the IoT networks to formulate the system intellectual and innovative. IoT a well-balanced platform where everyday device procedures turn into intellectual, everyday communication turns into helpful, everyday processing turn into intelligent. Although internet of things still in the hunt for its very own pattern, shape, and architectural structure. IoT helps in developing most powerful industrial systems, various applications in household, smart city, agriculture, healthcare centers, environmental and transportation many more. Nowadays IoT is an essential area in machinery, policy, and manufacture along with engineering spheres. These technologies exemplify broad field of policy systems, networked products, sensors which take advantages and disadvantages in computing command, electronic miniaturization and system inter-connections to suggest clean potentialities which are formerly not offered. Since the construction of IoT, it has seen the emergent concern in architectural layout, as well as adaptive networks for advanced correlation, stuck between heterogeneous IoT devices to IoT systems. Numerous companies, as well as research organizations, presented an ample variety of projections in relation to the possible impact of IoT on the internet along with the financial system for the period of the next ongoing years. Cloud computing facilitates

B. Chander (✉) · G. Kumaravelan
Computer Science and Engineering, Pondicherry University, Pondicherry 609605, India
e-mail: gujurothubhanu@gmail.com

G. Kumaravelan
e-mail: gkumaravelanpu@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_1

flexible source provisions that turn into extremely popular for lots of appliances because of cloud computing likely to satisfy IoT desires such as pre-processing, shield (hiding) data, visualization tasks. Internet of Thing systems recently appeared as dynamic global network transportation with self-configuring potentials, in which things can act together, communicate among them as well as with the environment through the internet by swapping sensor data. They can counter independently on events and control them by triggering styles with or without direct human involvement. While talking about IoT It is important to know validation and testing methods of Internet of Things furthermore for an IoT framework to be trustworthy and reliable, a few nominal sets of measure should be fulfilled to get integration and interoperability of IoT. The overview of the chapter design is to help the reader to find the research way, exchange of ideas close to IoT in light of competing about its predictions. Moreover it summarizes up-to-date about IoTs which can help a new reader easily understand about IoT and motivate the reader to work, research on IoT improvement.

Keywords Internet of things · Wireless sensor networks · Testing methods · Privacy · Applications · Services

1.1 Introduction

Internet of Things (IoTs) is one of the emerging topics in recent time in terms of technical, social and financial consequences. From the past decades, there is a significant development in the fields of wireless communication technology, information and communication systems, industrial designs and electromechanical systems encouragements progress new technology named as Internet of things. The most important intention of Internet of things is to connect all or any devices to the internet or other connected devices [1–3]. IoTs is the collection network of home appliances, physical devices, vehicular networks and added devices fixed with sensors, electronics, and actuators along with network connectivity which make-possibility for mentioned objects to gather/accumulate and exchange information/data. IoT works as a massive network of organized things and people allocate those gathered resources in relation to the way they are utilized and also know regarding the surrounding atmosphere. Here each and everything typically identified with its corresponding computing system however it proficient to inter-operate inside the existing internet infrastructure [1, 4, 5].

For simplicity, IoT has a particular circumstance that can connect a variety of things, where everything has the capability to communicate with other connected devices. It starts with the network and goes forward into everything that connected. It allocates people and things to be in connection any-time, any-thing, any-where, any service, and any-network path. From the latest updates in the IoT field, there will be more than 30 billion things/devices continuously online and higher than 200

billion things/devices infrequently online by the year 2020 [1, 2]. In the early hours of 2000, Kevin Ashton one of the pioneer researcher of MIT institute AutoID Lab who made ground base work that comes out nowadays as the Internet of Things (IoT). Ashton who work rigorously, Proctor and Gamble may progress its production as a result of connecting RFID information to the internet. It is great if all objects, devices dressed with wireless connectivity's, identifiers; exchange a few words each other moreover supervise through computer-based systems. In 1999 RFID article Ashton stated like "if we had computers that know everything there was to know about Things/Devices, those can accumulate data without any kind of help from us, with help of that data/information we are able to track, calculate everything furthermore we are capable to tremendous reduction of cost, loss, and waste. We would recognize when things looked-for recalling, replacing, whether they are fresh or Passover their best. Here, we need to make powerful computers with their own means of gathering information/data, so they can observe, react to the world themselves. Sensor technology and RFID facilitate computers to observe, identify and understand the world without the involvement of human intervention entered data". At the time of Ashton statement there were many obstacles are stated to answers but coming days more than a few obstacles has answered/resolved. Most importantly the cost and size of wireless equipment has gone down extremely. Many electronic companies are in process to build Wi-Fi as well as cellular wireless connectivity into a broad territory of devices. According to ABI study, more than twenty-eight billion wireless fragments distribute in 2020. Cellular data exposure has been enormously enhanced by means of many networks to provide broadband speeds. Moreover battery tools, solar recharging has been built into numerous devices. So coming years billions of things/devices will connect to the network. The hardware design company CISCO's IoT's Group stated that across 50 billion allied devices by 2020 [1–3, 6–8].

Internets of things agree on devices to be sensed or else controlled distantly across offered network communications based on that perspective it creates more possibilities for direct incorporation of the physical world through to computer-based systems in addition results produced in the form of accurateness, effectiveness, financial benefits and reduces human involvement.

1.2 Background

Internet significantly changes the way of human life, interaction among people from professional life to social relationships. Internet of things takes an additional step where internet enabling communication between small/smart devices that leads to a mixed set-up of physical plus virtual objects. Interoperability is the capability of dissimilar IoT devices and services to transfer accumulated data and usage of transformed data. Most of the current IoT initiatives straightly spotlight on applications and objects that deal with disparate requirements, although other hands leave concentration on connectivity and interoperability. This will affect

functionality, unnecessary services, problems on change management and limits resources usage chances. So there is a need for IoT initiatives to focus more on interoperability as well as connectivity which will provide security mechanisms to allow desperate devices as well as services to join. By providing efficient interoperability IoT devices and services can able to interact with greater efficiency, provide the greater capability, great choice with low cost. There are numerous reasons which could stand as reasons for poor interoperability and connectivity those are: *Poor information visualization and analysis*—present IoT services made little focus on data visualization and analysis which suggests incalculable insights to the system, *Poor context-awareness for services*—till now there are no significant requirements for suitable service context description in IoT services, due to inadequately mold semantics proliferating a variety of unfairly designed semantics and confused semantics for services, *Lack of standardized description of services*—At present scenario need of proficient principles for proper IoT device services, data description and information services. The efficient integrating solution for heterogeneous IoT could advantage from integrated modeling procedures to endow with appropriate facts possession and demonstration of the IoT field, *Poor device service classification*—IoT initiatives categorize device services depend on device service categorization. These services discoverable if an examination is prepared for service or device identifier, there have to be a new path service organization to provide accommodation such as dynamic invention services [1–4].

1.3 Architectural Formation and Communication Models

Internet of things (IoTs) is a collection of intelligent devices and that aims to correlate those devices over the network. The architectural structure of IoT concerns communication protocols, smart objects, security, scalability, and interoperability among heterogeneous devices Fig. 1.1. Sometimes things/devices may move from its own location to other places in real-time relations by surrounding atmosphere moreover some adaptive designs for dynamic interaction with other devices, the decentralized design affords IoT efficient event-driven capacity [6, 9, 10].

1.3.1 Architecture Formation

Sensing Layer: Internet of Things (IoT) measured as a physical interconnected set-up, in which things monitored, maintained remotely. The most important task in IoT system is sensing which is done through intelligent sensor nodes and RFID. In the sensing layer of the IoT system, the wireless sensor nodes or RFID tags devices easily, by design sense and swap information between dissimilar things. Mentioned

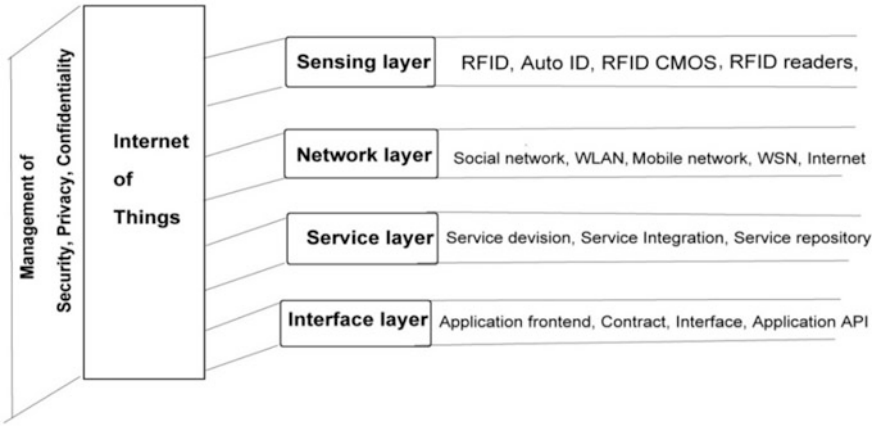


Fig. 1.1 Pictorial representation of internet of things architecture

superior technologies advance the potentiality of IoT sense, identifying connecting more and more devices easier. Sensing and unique identification are successful steps for huge industrial and academic networks such as IoT network [6, 11, 12].

Network layer: Network layer makes a platform for all the connected devices/things together and allows devices to exchange accumulated information with other connected devices. It automatically discovers and maps network for dynamically transforming network devices, where devices need to be automatically assigned to their roles such as deployment, scheduling work modules, connect with any other network devices when it's needed. In order to design IoT network layer, developers must take concern of addressing about network management technologies whether it is mobile, fixed or wireless and data signal dispensation, protection and confidentiality and service retrieval [6, 9, 13–15].

Service layer: Service layer of IoT communicates on middleware technology which facilitates various functionalities to integrate effortlessly. The main activity of service is to involve specifications of middleware which was designed industrialized by different groups. The middleware technology produces a cost-efficient platform for IoT based applications, where the hardware, as well as software platforms, can be reprocessed. Service layer progress service-oriented issues such as storage management, search engine, communications, and information transportation. Service discovery, service composition, trustworthiness management, and services APIs are some components of the service layer in IoT [6, 9, 10, 13, 14].

Interface layer: In IoT the huge amount devices occupied were prepared by dissimilar industries and companies moreover do not allow the same network protocols. As a result of this, there are numerous issues raised in devices communications, information exchanges among dissimilar things/devices. So there is a great demand for interface layer to shorten interrelation of things, if not have any interface layer continuous increase of devices in IoT turns to more difficult to

communicate, operate, connect and disconnect. An interface outline is a pack of service principles moreover describe the specification between applications and services [14, 16, 17].

1.3.2 Communication Models

The Internet Architecture Board (IAB) elucidates a governed architectural manuscript for how small; well-dressed objects of IoT systems communicate connect in provisions of their methodological communication models. Here some communication models mentioned which mostly used by IoT devices/objects [1, 4, 18–21].

Device to Device communication: In IoT, Device-to-Device communication model symbolizes paired devices without any intermediate server, straightforwardly connect and communicate with each other. These devices use many internet networks in communication and to establish direct communication devices use protocols like Bluetooth, ZigBee, etc., This communication model strictly follows one to one communication protocol to exchange information to achieve their respective functionalities. Home based internet of things appliances like bulb-switches, door-locks, washing machine, microwave, refrigerators, and air-conditioners commonly utilized a device to device communication where they send undersized data packets through low rate data requirements. One main drawback of Device-to-Device communication is it forces to deploy/select similar category devices because device-to-device statement protocols are not well-suited.

Device to cloud communication model: In Device to cloud communication model, IoT devices straightforwardly hook-up to cloud service provider which monitor interchange data plus restrictions message traffic. Cloud connection facilitates abuser to achieve remote access to their states through Smartphone and also upgrade software updates. This model utilizes an existing wired or wireless connection to create a connection among device and internet protocol network that connects to cloud service in the end. Here, device and cloud service must be from the same vendor.

Device to Gateway communication model: In device to gateway model, an IoT device connects through application layer gateway (ALG) that provides services as a mouthpiece to reach cloud service. Application software runs on local gateway acts as intermediary among device and cloud moreover it provides security-related functions when data is on transmission mode. Smartphone turns to be a local gateway device that runs an application to communicate with a device and dispatch data to a clouds service. Home-based automation applications use Hub devices are on the type of device to gateway models, where Hubs play as a local gateway among individual IoT devices as well as a cloud service.

Back end data sharing model: In Back-end data sharing communication model facilitate import, export plus evaluate smart/small devices records from a cloud service in recipe with records from further sources. Means these models permit the

records or data composed by individual IoT device to be combined then examined. This type of communication model allows data portability when it needs; the abuser can able to shift their records while they change among IoT devices. Back end data sharing model is effective as much as IoT system designs.

1.4 IoT Key Elements, the 3C Concept—Advantages, Disadvantages

1.4.1 IoT Key Elements

Internet of Things system was a combination of various functional blocks to smooth the progress of communication, automation, sensing, management, identification, actuation of a system [5, 7].

Communication: Communication block build communication link amid devices, remote servers. Generally, transmission blocks handled at the transport layer, network layer plus data link layer of the IoT system.

Security: IoT devices communicate over the internet or any other communication providers where security plays a very important role. Security function in IoT provides function like authentication, data-message-content integrity, authorization, access control, and data security.

Management: Management provides functionalities to suggest or governs an IoT system in order to complete the originated work.

Device: Device provides services like sensing, monitoring, control, and management IoT activities. Basically, IoT devices accumulate data from the surrounding environment, exchange with other devices. Moreover, process data locally to perform locally assigned tasks or transform data to cloud servers or back-end servers for processing data. An IoT device consists with more than a few interfaces in support of communication with further devices equally in wired and wireless communication some of them are interfaces in sensors, video-audio interfaces, internet connectivity, memory, and storage. Devices collected data will be in different forms which progression by data analytics schemes to produce valuable information.

Services: Internet of Things provides several categories of services such as devices discovery, data transferring, device control and device modeling.

Application: Application layer play a key position in IoT structure in provisions of users where it acts as an interface. Appliances allocate abusers to visualize and evaluate the system condition.

Connectivity: In networking, there is no guarantee for a complete tie with major network devices. The new technologies meant for networking in particular IoT networking provides small cheaper scale networks, IoT been establishing these small networks among its system devices.

1.4.2 The 3C IoT Concept

Communication: Major role of Internet of Things (IoT) is toward communicated information or data to respective systems as well as people. Similar to state of equipment, sensors data that monitor accumulate data from patient essential signs. In past scenarios do not access information before directly; it was composed recurrently or else by hand. Nowadays, we have a bunch of assets to track data/materials. Location finding is most important for materials which are in a move like planes, but that will observe when it was in particularly organized localization. IoT helps in the transportation industry, which can provide real-time tracking and position, damage to parcels. IoT in secure home applications provides control over the home appliances [1–4].

Cost Saving: Innovation of IoT reduces cost investment in many industrial companies. Continuous observation indicates actual performance and condition statement of equipment. In particular, the industrial company's lost huge amount of money when a machine fails but with the inclusion of wireless sensor technology IoT can help company money by minimizing the machine failure as well as run the business according to company plans. A modern sensor capable to monitor subjects such as driver behavior respective with speed, home appliances energy consumption, vehicle fuel consumption so the customer can view all the above-noted results make their energy consumption levels moreover provides an opportunity to cost saving [1–4].

Control: In a digital world, a business run on device conditions like a company or consumer able to control a device remotely. Some kind of business completely and remotely shutdown or turn on of a specific equipment/device. Industrial companies build cars with inclusion of IoT, Those cars operate remotely like the customer can lock unlock and control over operations. Most of Home-based IoT applications like washing-machine; microwave, windows, garden works and doors control by customers are automated. For example, once a performance measure established for a process it sends alert messages if there any unfortunate things going to happen like as if machine crucial part bolts about to open, the process will send an alert message and company make a machine out of service and schedule maintenance service [1–4].

1.4.3 Advantages

Improved Data collection: Many contemporary data collected works suffer against its own design boundaries for methodological usage. But IoT overcomes those limitations and deployed where human exactly wants to analyze the real world. **Improved customer interaction**: Most of the present analytics from unsighted marks along with errors in accuracy where IoT ended above problem to accomplish more effective collaboration with customers. **Reduces waste**: IoT clearly make

many fields improvement, most of the present analytics came with outer impends, however, Internet of things endow-with real-time, real-world information lead to the more effectual organization of sources, not more to waste. **Technology optimization**: the unchanged technologies which are utilized to improve customer experience may also improve device use. Based on these IoT undo important functions as well as field data.

1.4.4 Disadvantages

Internet of things produces significant advantages in the real world however it contains some considerable issues as well [5, 18–22].

Flexibility: flexibility of IoT systems defined as how a device integrates easily with another device or system. But IoT devices hard to judgment themselves through numerous conflicting or locking systems. **Security**' IoT systems develop a network of consistent connection devices communicating over the internet. There is some little drawback on security measures which lead users to various kinds of attacks. **Privacy**' IoT has a capability that can provide sensitive personal information in maximal detail devoid of users' active involvement. **Complexity**: IoT organizations are problematical in design, maintenance and their exploit of manifold technologies along with a large set of new-fangled technologies.

1.5 Internet of Things Technologies

There are some improved technologies used in the development and deployment of Internet of Things base products successfully. Those are RFID technology, wireless sensor network communication; cloud computing, Big-data, middleware, and IoT application software. The choice of the above-mentioned domains leans on modern state-of-affairs of IoT suitableness [3–7].

1.5.1 RFID Technology

Radio frequency identification (RFID) initiates automated recognition as well as data capturing with radio waves and a tag. Based on RFID skill the phrase "Internet of Things" was proposed to associate absolute identification of interoperable connected devices/objects. In early 2000s Auto-ID lab attributed the word "Thing" where IoT got its unique figure. Auto-Id and EPC-global combination aimed to architect the definite replica of IoT. Both the organizations have the same agenda on progression of Electronic Product Code (EPC) for backing the ample applicability of RFID tags in up-to-date transaction network. Here, tags contain information in the shape of

EPC. At present, there is three kinds of tags available Passive RFID tags—Transfer radio frequency energy starting at the originated reader to tag, in order to influence the tag. Electronic trolls, supply chaining and item tracking are some noted applications for passive RFID tags moreover they no more battery power-driven. Active RFID tags—Active tags hold external sensors that can monitor humidity, pressure, and temperature and other surrounding environmental conditions and initiate communication in the association of reader. Active RFID tags have individual battery resources. Sensible manufacturing, hospital, and laboratories are some of the application areas for Active RFID tags. Finally Semi-passive RFID tags—make use of a battery to power the microchip at the same time of transmitting by capitalizing power from a reader [3, 4, 5, 6, 7, 23–28].

Unique or Ubiquitous Identifier (uID) is an additional choice of identification in IoT, the main proposal was to establish incorporation and improvement of middleware deliverables. For the reason of suitable low-cost small size RFID still leads the way of IoT services since its origin. However, the new developments in computer network protocols and heterogeneous devices soon will overcome the usages of RFID. Near field communication (NFC), wireless identification, wireless sensor, actuator networks along with sensing proposals are some of them. The amalgamation of any of the above techniques with RFID will show a new path in the Internet of Things [7].

1.5.2 Wireless Sensor Network Transportation

In the past, wired sensor networks are applicable to limited appliances which produce low results. However, the innovations in wireless, computer networks, and ICT systems introduce a new-fangled approach of computing as well as communication architecture known as wireless sensor network (WSN). WSN is one of the key components in favor of IoT scheme success. WSN is a compilation of sensor nodes or motes, comprehend by appropriate principle node called a Sink or Cluster head. Scalability, robustness, reliability, and energy efficiency parameters required when designing a WSN power-driven system [7, 27, 29, 30].

In IoT, WSN consist of spatially assigned autonomous sensor-equipped devices headed for supervising physical or ecological state-of-affairs moreover collaborates through RFID systems to enhance tracking condition about “things/devices” such as their locality, activities. WSN has a huge advantage that it tolerates special network topologies and multi-hop communication to handle energy consumption. WSN is frequently applicable in transport, temperature sensitive products, jet engines-turbines-wind farms for preventive maintenance, preprocessing data in real time, maintenance and tracking systems.

Here are some wireless communication standards which are used in IoT system services—IEEE 802.11—also called Wi-Fi it is a collected works of wireless local area network principles. 802.11a—functions at 5 GHz band coming to 802.11b as well as 802.11 g function at 2.4 GHz, 802.11ac functions at 5 GHz and 802.11ad

functions at 60 GHz some of the important communication standards come under this category. IEEE 802.16—is also well-known as universal interoperability for Microwave Access or WiMAX, which was collected works of wireless broadband services. WiMax provides data rates as follows for mobile stations 100 Mb/s coming to fixed standard stations 1 GB/s. 2G/3G/4G mobile communication—Till present, we contain three special generations for mobile connections those are 2G—GSM/CDMA, 3G—UMTS/CDMA2000, 4G—LTE and data rates (2G to 4G) starts 9 Kb/s to 100 Mb/s. IoT devices work on the above-mentioned standards can be in touch over cellular networks. IEEE 802.15.4—identified as Low Rate Wireless Personal Area Networks (LR-WPAN), which provides low price, a low-speed transmission that reduces energy consumption in devices. LR-WPAN principles data rate starts 40 Kb/s to 250 Kb/s, functions at 965 MHz to 2.4 GHz. IEEE 802.15.1—is called Bluetooth, which was fitting for wireless data diffusion in movable devices with low cost, low power. A Bluetooth data rate starts from 1 Mb/s to 24 Mb/s and functions at 2.4 GHz [7].

1.5.3 Cloud Computing

Cloud computing works as technology or representation of on-demand distributed data processing, with help of internet a few scalable information resources and capacities provided as service to external users/devices. IoT connected devices create a massive quantity of data shared through the internet. Many of IoT appliances required gigantic data storage space and processing speed in order to take immediate decision-making, data visualization, device management, data analytics and prompted broadband for stream audio-video data. Cloud computation performs at the supreme backend for handling data created by IoT devices and processing them for IoT procedures, humans in real-time. Cloud computing basic concepts follows as Software as a service (SaaS), Infrastructure as a service (IaaS), Desktop as a service (DaaS) and Platform as a service (PaaS) [7, 23, 29].

1.5.4 Big Data

IoT introduces the automated talented standardize and command of connected devices over vast areas through sensors and other computing potentials. Most of IoT services are real-time based so It is very important to have a well-organized model to assemble small amounts of data and transmitting to a centralized location for processing and send back to sensors for appropriate performances. Capacities of IoT devices, sensors and size of the different data types need to be processing which would be extremely large and varied. All of the above-mentioned personalities closely associated with big data. Big data has tremendous responsibilities in IoT, where it introduce a data storage support to store and integrate with prearranged as

well as shapeless IoT data. Hadoop design in big data beside with various supplementary databases creates a distributed file storage area to store as well as resourcefully manage varied kinds of data composed by sensors and RFID readers. The job of big-data on IoT is incredible, although the most observable applications will be in analytics, data security, and data storage spaces [7].

1.5.5 Middleware

Internet-of-Things (IoT) was the collective element of the potential Internet with omnipresent computation. IoT demands connections by means of mixed actuators, raw sensors, aggregators and dissimilar field context-aware appliances, preserve protection and confidentiality. Consecutively to satisfy the above-said demands, IoT should need software platform definite as middleware. Middleware, a software sheet introduces among software appliances that formulate on behalf of software developers to achieve easier transmission and input/output. Simply middleware made the connection between complex different programs that were not originally built to connect with others. As mentioned previously complicated distributed communications of IoT through different devices require a simplified advance of innovative appliances and services, hence adding middleware in IoT system development is essential. Openlot, FiWare, Middlewhere are some examples of middleware. Progress of middleware in the field of IoT is an energetic region to do research [5, 6, 7, 26, 27].

1.5.6 IoT Application Software

IoT enlarges development of numerous industry-specific as well as individual/user-specific applications. Because of IoT devices and networks substantial productivity, IoT enables Machine-to-Machine as well as Machine-to-Human applications. In Machine-to-Machine applications, the machine needs to ensure that the message is transformed, received in an accurate and timely manner. For instance logistics and transportation appliance to monitor, active status of product/goods, proper actions will take mechanically to evade spoilage when connectivity is out-of-position. In Machine-to-Human appliances, offer visualization of current data to end-user which permit interface with surroundings. In IoT, It is essential to design intelligent devices (sensor, actuators) can able to monitor, identify and potentially able to resolve the problem without human intervention [6–8].

1.6 Applications of IoT

Internet of Things a novel technology model as a large-scale network of machinery and devices able of interconnect by everyone other to collect and exchange information/data. Because of its characteristics IoT renowned as the most important sector for future technology, more importantly, it gaining measureless attention from a wide verity of industries. There is no need to say that contemporary hype around the Internet of Things was massive. It looks like every day a new company comes with a new kind of IoT enabled product or service. Whatever it may be the factual importance of IoT for Endeavour completely apprehend once the IoT related devices are capable to correspond with other associated devices moreover integrate into the company of customer support services, inventory systems, business intelligence and analytics. At present IoT illustrations extended from smart integrated homes to human wearable things to healthcare. Here, IoT becomes part of every aspect of our lives moreover IoT applications are not only enlarging the well-being of our daily lives and also giving us more control by simplifying everyday work life along with special responsibilities [2, 3, 31, 32].

We measured what the really popular Internet of Things applications are right now Fig. 1.2.

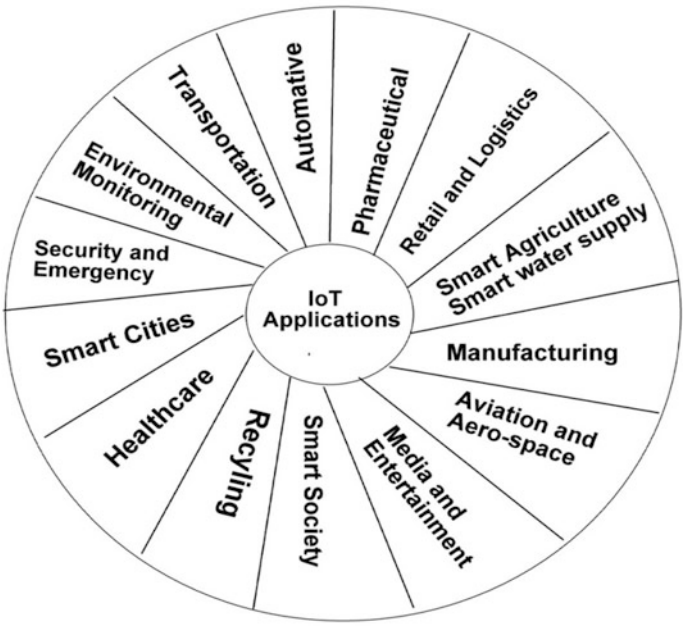


Fig. 1.2 The paradigm of the Internet of things application

1.6.1 Smart Society

Globe can be transformed toward well-connected well-dressed society as a result of applying pioneering perceptions of Internet of Things.

1.6.2 Traffic Management

Many researchers confirmed that there are possibilities of executions for the machine to machine solutions in traffic administration, it combines an IP Multimedia Subsystem.

1.6.3 Link Data for Society

There must be an extreme examine reserved on transmission and network features of IoT devices those employ for sensing, the dimension of existent world substances. There is some semantically linked architecture which performs connectivity of objects that perform interoperable description in the structure of associated data.

1.6.4 Urban Management

Urban management platform developed on behalf of understanding IoT base well-groomed cities connected through smart/small sensors and system sustains via data organization, cloud base incorporation that forms a transformational component of the presented cyber-physical scheme. There is work going on Smart platform that Google map assimilates with Go-IoT application for remotely monitor digital home.

1.6.5 Road Quality Monitoring

Road quality monitoring, alert message making can be processed through in-vehicle Smartphone linked with smart sensors toward IoT cloud platform. Here we embed a new energy expert mobile accelerometer inside Smartphone for continuous monitoring road condition.

1.6.6 Smart Cities

Inclusion of IoT systematically changes smartness of cities takes in numerous applications as monitor space for parking vehicles, monitoring and detecting vibrations in building and bridges, observing sound volume in sensitive areas, intelligently control street lights according to weather conditions, detection of waste and trash material levels and collection, indicating alert messages in the view of unconditional weather or traffic jams or accidents.

1.6.7 Healthcare

There are plenty of benefits afford as a result of IoT inclusion in healthcare management those are complete and correct electronic patient testimony maintenance, track and recognition of patient to progress work-flow of hospitals, identification, authentication of patients in order to reduce harmful incidents to individual patients, automatic data collection and transforming data to other hospitals which reduce the processing time and procedure auditing, sensors which takes healthcare to another level, where sensors embedded on patient body for real-time collective data on patient health conditions moreover alerting over patient behavior. Intelligent sensor nodes accurately monitor patient blood-pressure, heart-rate, cholesterol level temperature and blood-glucose levels, etc.

1.6.8 Retail and Logistics

Internet of Things with retail and logistics provide many advantages includes monitoring storage conditions of product and trace purposes, guides in shopping complex based on pre-arranged lists, payment processing in gyms and retail shops, automate product rotations in shelves, detection of freshness of product like time and data indications without particularly looking it, item location, storage incompatibility detection, making arrangements while products on transportation etc.

1.6.9 Security and Emergency

Introduction of IoT made tremendous changes in security and emergency applications some of them are perimeter access control to restrict people to enter into secure regions, liquid detection in laboratories and explosive gas levels, detecting radiation levels at nuclear stations surroundings, detection and create alert messages on leakage of gas, chemical, coal mines, and detecting breakdowns in vehicles.

1.6.10 Smart Agriculture and Smart Water Supply

Agriculture with IoT strengthens the work and productivity of agriculture filed thorough monitoring temperature, moisture and analysis quantity of vitamins of product. Examine weather conditions in fields to predict rain, snow and wind changes. IoT in water supply examines the condition of river and seawater whether it is usable for drinking purpose or agriculture usage. Detection of pressure variation in supplying pipes, water levels in reservoirs and rivers, dams.

1.6.11 Aviation and Aerospace

IoT assists to improve the security and safety measures of aerospace services through unfailing identifying forge elements. Aviation continuously suffers from suspected unapproved parts means the aircraft part that is no guarantee to meet with approved parts. This can be improved with the help of securely attached RFID tags, an authentication achieved prior to establish them in an aircraft.

1.6.12 Environmental Monitoring

Deployment of wireless sensor nodes as well as IoT devices in the certain environment was one of the best and talented applications in IoT. The sensor can monitor pollution levels send out alert messages, an indication of dangerous gas levels, forest fire detection, floods, and hurricane indications, etc.

1.6.13 Media and Entertainment

Based on user location ad hoc news gathered and transmit to the user, that is based on which multimedia device is present at that time. Moreover, complete video footage of incident forward to a particular user with help of deployed IoT technologies.

1.6.14 Recycling

With the help of IoT and wireless sensor nodes continuously observe various industrial cities and environmental programs to take account of automobile emissions to inspect air condition, detecting eco-friendly materials, electrical material, etc.

1.6.15 Transportation

IoT devices help to screen passengers and bags at airports, railways accurately. Screening Goods transported by international cargo where security demands take top priority. Container self-scan and weigh themselves turn to easy task with the inclusion of IoT devices on containers. Monitoring long-distance traffic jams through Smartphone's etc.

1.6.16 Manufacturing

Embedding IoT devices with the machine can send alert messages regarding huge damages before it occurs, and that machine send under examine to fix the problem, by doing this companies product will not deny for a long period time. Moreover with an intelligent system structure and information schemes, fabrication processes optimized as well as whole lifecycle of a product starting from fabrication to disposition can be observed.

1.6.17 Pharmaceutical

In transporting, storing processes security, safeties are extreme importance in pharmaceutical. Drug products need specific storage conditions, continuously monitored for detecting any violating conditions while transporting, adding smart labels, tracking them in the supply chain and observing their behavior with smart sensor will provide many benefits. The attached tags and smart stickers on the drugs can also provide instructions regarding safety usage instructions, dosage level, and expiry information of drug and authenticity of medication.

1.6.18 Auto-motive

At present era advanced production of aircraft, cars, machines, buses, trains and bicycles equipped with intelligent sensor nodes and actuators with low power consumption technologies. These will monitor and report various parameters regarding automatic doors/windows locking system, breakdown systems, pressure in tires, refreshing air automatically. Vehicle-to-vehicle and vehicle-to-infrastructure communications will drastically change and advances intellectual transportation system. While the attaching devices to particular part restrain information related to date and place of the product were introduced, name of the manufacturer, product code, serial number, location and type of product.

1.7 Testing Models of IoT

Internet of Things is an innovation to transfer, exchange information toward a more connected world that linking everything with it. Each object/device has its own unique identification, protocol procedure accessibility, known about its status position and intelligence within the merge of device services and intelligence, provides the result as a mixture of both physical and internet connected world with the impressive impact of personal as well as societal surroundings. As mentioned above information, coming years count of electronic device usage increases tremendously and it is irrefutable. As the result of continuous growth in IoT connected devices and services/solutions has raises numerous equivalent challenges such as technical connectivity, security and privacy services, devices sizes, protocol and architecture designs etc. [8, 33–36].

Generally, systems, as well as devices, are easily prone to errors, IoT always considered an as big system that represents a collection of devices, so it has lots of errors those can directly impact on inhabits lives. Testing, debugging and validation deals with errors within the sphere of technical demanding. IoT facing foremost demand in technical field owed to the extensive amount of devices, invisibility and unreliable connectivity, dynamic topologies, and protocols however specific IoT devices might enclose a restricted set of functionalities easy to test. But turns complex to test and validate similar kind thousands of devices deployed in a particular region. If the system is self-control and self-adjustment, It will more complicated tasks or not entirely repeatable for testing as well as validation intentions. Such systems enthusiastically assign resources with optimization objectives in provisions of battery consumption, migration computational desires, etc. [33–37]. Internet of Things is an arrangement of hardware, software, design architecture with the aim of initiate real-world objects to intermingle by adjacent situations like sense it, communicate with interrelated objects as being inter-connected thing/object. For the assurance of IoT systems reliability, security, scalability, and performances there is a need for testing special layers and components of the system starting from low-level to higher-level specification components. IoT devices are strongly connected and dependent so it's hard to draw attention on the low level to higher level components.

1.7.1 Testing Levels and Methods

Testing levels divided into various models depending on test scope and objective. By applying testing method items/devices internal design, implementation and structure being tested which are not known to the tester. The main purpose of applying various testing methodologies was, in the process of any development make sure that designed software or hardware has capable to operate different environments across different platforms. Basically, Test is defined as "A test is the

process used to discover whether equipment or a product works correctly or to discover more about it" or "A test is a deliberate action or experiment to find out how well something works". Here dissimilar levels of testing methods are defined below [8, 38–45]:

Unit testing: Unit testing acknowledged as the initial level of testing, as the name suggests unit is a small part of any software. Unit testing deals with individual/single or components of hardware and software are tested. Mainly used to check individual units of software performing it functionalities as designed or not. Unit testing enhances self-assurance to change/maintaining the individual code, normally it performed by-hand nevertheless automating process will accelerate delivery cycles and enlarge test exposure. **Integration testing**: integration testing combines individual components and tests them as a group. The main aim of this type of testing is to check and expose the interaction of failures among integrated component units that are designed to perform the specific assignment. **System testing**: System testing where the entire system, as well as an integrated system, is tested whether it meets specified requirement functionalities from end to end. **Acceptance testing**: Acceptance testing is the concluding step of whether the system reaches the last phase for delivery or not. It ensures that product is fulfillment with the entire original business criteria and that congregate the end users require. It also enables a customer/user/authorized individual to find out whether to accept the system or not.

1.7.2 Generic Testing Schemes

Block-box testing: Block box testing content is not visible to anyone—only information about system module, input-output are known. It also called a behavioral testing module which finds behavior and performance errors, incorrect and missing functions, errors in data structure and database. Tester need not know how the software implemented and about programming languages.

White box testing: White box testing internals visible and known which provide information to build various test case scenarios. It also called at the same time as Transparent-box testing, Glass box testing, Clear-box testing. Generally, white box testing not made in support of failure detection; tester individually selects the input to implement paths through the code and find out the proper outputs.

Gray box testing: Gray box testing was an amalgamation of Block box with White box testing schemes. In Gray box testing internal structure is partially known and it mainly used for failure detection.

Agile testing: Agile testing method follows the best outcome of agile software development. it is the iterative development model where functionalities of customer and design team collaborate, where features are tested as they are developed.

Ad hoc testing: Ad hoc testing performed without any certain planning information and documentation. Ad hoc testing executed only once unless not find any defects. It is also named as random testing, where it conducted informally and

randomly without any formal expected results. Successes of Ad hoc testing absolutely depend on the potential of a tester, because testing conceded out with an understanding of tester regarding the appliances moreover tester tests randomly subsequent specifications/requirements.

1.7.3 Testing the Internet of Things

IoT is a collection of different hardware and software components, services, modules and architecture designs produced by different companies with different properties. Which needed to be tested for testing results like whether there functionalities working as they designed or not. And because of dynamic topologies, security and privacy, large scale system structure, high heterogeneity, interoperability, and connectivity makes test automation difficult [38–45].

Edge Testing: Edge testing performed at edge or low-level parts of IoT services such as micro-electro systems, controllers to test out edge device against their condition. **Fog Testing**: Fog testing applied on middle layers of IoT systems which are coming in the device to entryway communication models. Fog computing has capable of potential evolution that is conducted to determine the relative conflict of an object. Most of the middle layers are connectivity assist layers those assist connection between devices and the internet, so there must take care of network and security testing while performing fog test. **Cloud testing**: Cloud testing is one type of software test that checks cloud computing services. Cloud testing concerns cloud infrastructure, scalability and dynamic configuration. Cloud testing does at different levels like a testing entire cloud at a time, testing across clouds private-public, testing within cloud internal features, testing cloud at application requirement. However, cloud testing still has open challenges and problems which are needed to be solved. **Security testing**: Security testing deals with privacy and security of IoT enabled device services for consistent quality of IoT services. IoT devices contain important sensible information (like patient information, building structure, web cameras data, etc.) which is easy targets for illegitimate entities; safeguard of information concern as a very necessary task.

1.7.4 IoT Test-Bed

IoT test-beds which allow testing IoT system as a whole at a time starting from low level to high level. The key consideration about IoT test-bed is its scope of design, most of IoT test-bed implemented on one key technological logic that can address only one particular type of IoT technology, it called as single-domain test-bed. A test-bed called as multi-domain test-bed, which merges dissimilar IoT technologies into a general experimental facility. Renewed test-bed must be either indoor/Mote lab or outdoor/CitySence. Indoor test-bed provides simple connection

to power cabling for control and administration purpose for easy to manage and accessibility [46, 47]. Whereas outdoor test-beds provides wireless communication for increasing reliability. Both must be sheltered in opposition to malicious attacks and threats which are repeatedly occurred. Mote lab [15, 16]—the first test-bed which works as basis framework for many testbeds, TutorNet [15, 16]—abuser has control over resource reservation start and end point times and list of motes, if the allowed time period over reservation will fail, Knasei [48]—It is one of the examination test-bed with various functional services, co-simulation support, event injection possibilities, control over mobile robots etc., FRONTS—purely wireless in-band management, Senslab [49]—purely on energy management and measurement supported for every node, DES test-bed—movement steps planned, TWIST [50]—provide bases for a variety of other test-beds, City Sense—two important features realism and domain specification make it has permanent outdoor installation, its control plus management plane exclusively based on wireless hookups, Vizbee—it main purpose is to combine RFID receivers with repeaters, Flocklab [15, 16]—by using adapter board results provides sophisticated qualities as energy utilization, mote monitor and emulsion of radio behavior. CITC test-bed [15, 16]—mainly used to try out in a distinctive atmosphere united with definite frequencies in order to learn the RFID efficacy in a specified atmosphere.

1.8 IoT Frameworks

A software framework is a platform for developing interrelated formation which points out what kind of programs should be made and how they interconnect. In order to accomplish interoperability and integration in the Internet of Things (IoT), the designed IoT framework must enchant dependable, reliable, scalable and some important measurement. Here we are presenting some IoT frameworks starting scholarly to organizational do research, mostly spotlight on adding chips, devices in IoT [4, 51–56].

1.8.1 AVIoT

AVIoT kinds of IoT framework in support of visualizing, authorize things or devices in well-dressed atmospheres like hospital management and smart home appliances by the end-abusers. AVIoT frameworks allocate end-abusers, to relate its web-based visual authoring tools to program, indefinite behavior of IoT equipment. For this reason, end-abusers without any understanding in relation to internal structure and communication protocols estimations and define the behavior of things or devices. There are some principled processes followed by AVIoT framework those are ***Interactive IoT Authoring***—here abuser can add, delete and edit virtual things from the list of given set of physical things. Moreover, abuser

may also reposition things from one place to another and those things rediscovered in the fresh locality through the physical server. ***Abstraction of sensors and actuators***—here physical equipment abstracted and virtualized in IoT environments are defined themselves as a node, in order to interrelate with other virtual things. Furthermore, the node defined based on features like name, the position where used, type of thing, type of visualization and functional script code. ***Interactive IoT Visualization***—here consumer web-browser/web-application along with server used to assist visualization, to promote the organization of physical/virtual things. Here server capable to store information with regards to visualization and authorizing things [4].

1.8.2 AllJon

AllJoyn an open source IoT frame focused on connectivity, assimilation of things without consideration of own manufacturers, announcement modules and operating systems. AllJoyn framework demonstrates compact network detection among devices by summarizing the details of physical transfer, provide API for connection things. In the process of notice adjacent devices API create sessions among devices for secure communication. This, in turn, trims down the security intimidations and amount of devices rendering to the internet threats. AIIjoyn framework encloses two important components those are AIIjoyn Apps and Alljoyn Routers. ***Alljoyn Apps***—directly communicates with Alljon Routers after that communicates with other Apps through Routers. It has subcomponents **Alljoyn App Code**—contains the logic of App, Alljoyn service framework—holds common services like as sending notifications, controlling device. **Alljoyn core library**—supply support for service/device discovery, session/object creation, handling methods/properties. **Alljoyn Routers**—facilitates communication among different Apps. It has three common patterns for communication those are Bundled Router—one to one relationship, Standalone Router—enables communication to multiple Apps, Router on a different device—run of other device allows communication from Apps.

1.8.3 Calvin Framework

Calvin a hybrid framework for IoT and Cloud compute representations to clarify the complication communication-protocols, distributed computing, and different cloud programming software's. It diverse the IoT application development into four aspects those are ***Describe***—developers details, express events, input-output affairs, prerequisites to activate action of an actor. ***Connect***—connect ports of already described actors with Calvin Script lightweight language. ***Deploy***—describe deployment of connected components in distributed run time. Progress simple

employment by transient the appliance script of an anticipated application. Manage —management of updates, error recovery, resource usage and scaling [4, 51].

1.8.4 Frasad

FRASAD (FRAmework for Sensor Application Development) framework allows developers to propose individual IoT appliances by utilizing sensor node field approaches. FRASAD framework succeeds model-driven concept where application code created from the intended model through communication procedure. FRASAD adopts three levels of abstraction for Model Driven Architecture (MDA) approach those levels are Computation ***independent model***—represent actual information without any structural and technology information, ***Platform based Model***—holds application requirements and logic, ***Platform Specific Model*** —the specific operating system of implementation [4, 53, 54–56].

1.8.5 Eclipse Smart-Home (ESH) Framework

Eclipse smart-Home outline mostly works as a section of software integrated into hardware to produce combined synchronization of connectivity things among everyone and also with an external network. It shows an easy declaration of IoT systems who gain from its automation, interfaces. ESH is open sources and widely used in smart home domain moreover independent connectivity features of the hardware. ESH build on four stacks: ***Operating system***—the primary function ESH runs on Windows, Linux, MacOS equally. ***Communication and connectivity***— ESH has wide range of acceptance in smart home appliance because of its connectivity and communication. It may provide offline statements inside home range objects. ***Data management and messaging***—ESH utilizes the persistence method for database storage and SSE or MQTT for messaging. ***Remote management***— firmware update configuration of allied devices and remote monitoring. Run time environment—written in Java with Apache Karaf and jetty HTTP server [4, 54, 55].

1.9 Security Issues in IoT

IoT is growing technology made a huge notice on both industrial, scientific academic domains. IoT assimilates digital and physical worlds into one ecological system that makes new intelligent internet technology. This intelligent internet technology proposes huge business value in special associations moreover endows with opportunity for various presented appliances in health-management, transportation, smart home, many other regions. On the other hand, as an

up-to-the-minute growing technology, Internet of Things tolerates from numerous security problems which are most challenging from other fields because of its resource constrained IoT devices/systems and compound environment. Researchers have been initiated and make available well-organized security explanations in IoT, but mostly deal with resource restraint devices along with scalability concerns. A few technologies associated with set-of-connections, cryptocurrency, Block-chain are presently transfiguring the world of the Internet of Things [57–67]. Security includes all techniques that aim to protect, undertaking the protection of information and restore against malicious attacks. IoT is the biggest arrangement with an amalgamation of small, well-dressed devices endow with sensitive personal data if any leakage of this information causes many issues so IoT security takes first place while its design and deployment. In general securities of computer set-of-connections, information schemes consist to afford the following services.

Privacy: It guarantees customer identity details should not be traceable or identifiable from their previous actions and behavior in the system.

Authentication: Devices must be authenticated with each other before transferring message or information. Authentication makes sure that the data source is pretended individuality.

Availability: Resources must be available when the user wants means services of a system must be obtainable for genuine abusers.

Confidentiality: It guarantees with the intention of information can alter by legitimated sources only; information prepared meaningless to unofficial abusers, processes.

No-Repudiation: it makes sure that dispatcher of information/packet/message cannot refuse having sent that in the future.

Integrity: it guarantees to data is not changed by illegitimate or third-party entities either accidentally or intentionally.

1.10 Internet of Things Simulators

Cooja simulator: The cooja is simulator platform built-up in favor of contaki operating system. It is java base simulator helps evaluate exact permanent software that might be uploaded into physical nodes. Cooja allocates system developers to analysis their code, system logs prior to operation it on distinct target [8, 63, 68].

iFogSiM: iFogSim applicable in fog computing simulation and modeling's for scheduling priorities as well as resource management from corner to corner of edge and cloud resources under dissimilar circumstances. IFogSim simulator mainly targets on resource management policies and their impact on network congestion, operational costs, energy consumption, and latency. It mainly targets simulate edge devices, network links, and cloud data centers to evaluate performance metrics [8].

Cloud2Sim: Cloud2Sim presents distributed contemporaneous architecture for CloudSim simulation. It can extend to have several instances to evaluate cloud and VM workloads from numerous nodes and transmit back to the data center broker.

There was an adaptive procedure made and executed to elastically scale resources made accessible to the simulation [8].

IOTSim: IOTSim developed on top of CloudSim setup to examining IoT big data processing, restoring MapReduce process. It makes a possible generous examination of impact with the performance of IoT-base appliances by industrial as well as marketable associations [8, 64, 69].

SimpleIoTSimulator: It was an IoT devices and services simulator which able to construct analysis base atmospheres compromised for thousands of sensor nodes on solitary central processing unit system. Contains numerous network protocols can intelligently realize information of recorded packet connections from genuine servers as well as sensors furthermore mold activities about its pretend devices against that data [8, 65, 70].

MBTASS: The Model-Based Testing as a Service (MBTASS) which is a recipe of model-based testing along with service-oriented clarifications. MBTASS thoroughly test IoT plus data platforms further modularity of the explanation permit incorporation test among dissimilar IoT platforms [8, 66].

MobIoTSim: MoboTSim is completely IoT device based simulator developed for android based devices. It helps researchers be trained to form IoT devices handling without any need to buy real smart sensors moreover analysis, express IoT appliances using several devices. The designed schemes interconnect with gateway service within the cloud like IBM Bluemix to manage simulated devices, sent back notifications against critical sensor values. The main target of MoboTSim is developers be able to inspect the performance of smart/miniature IoT systems with hand-held device [71].

TOSSIM: TPSSIM is completely made for WSNs simulator; build with a particular objective to simulate TinyOS procedure. TOSSIM supports python and C++ programming interfaces with various levels of simulation. TinyOS is effortlessly transformed into simulator engine by distinct proceedings; hence make things easier it more effectual [72, 73].

Arduino Unit: Arduino unit is a unit testing framework, as trivial library developer and researchers without problems check their systems within Arduino board, in spite of their little energy assets [8].

IoTFIY: IoTFIY an IoT application development without any hardware dependence. It makes the availability of practical lab for constructing fixed models in favor of system scaling and data generation [8].

MAMMotH: It is a comprehensive IoT simulator, capable to imitate ten thousand procedures for one virtual machine. It has 3 different states of affairs those are mobile devices allied through GPRS to sink station and shape star topology, WSN connects with sink station through GPRS and with inhibited sensors to proxies wherein the back-end it connects large scale IoT simulator. For reduce the communication problems present in IoT scenarios devices simulate one telephone system link for every node and capable of hold up or crash messages [70].

1.11 Open Research Challenges

1. Some well-designed IoT systems are deployed in dangerous environments where physical defense is unfeasible to accomplish. So invaders straightforwardly connect with physical access with IoT services/devices Fig. 1.3.
2. As mentioned IoT is a collection of devices will have a variety of data in type, size, and information. These kinds of data verities should be occupied with futuristic technologies which have multi-variation architecture, researchers must focus on it.
3. IoT still now deteriorates on traditional network infrastructure information and communication technology. It will affect by whatever is connected with it, this huge amount of linked devices prepare real-time collected statistics which must be direct with eminent bandwidth path. Consequently, there is need for uniform high bandwidth architecture base to handle this problem.
4. IoT service devices like real-time monitoring sensors are designed to confidentially implant in the atmosphere. Such devices not actively monitor or noticed by user moreover devices are not clear and no plan to make an alert to the user about security problem arises. Hence it is technically not easy a user to be familiar with that a security breaches to IoT device has happened.
5. Most of the frequently acknowledged service narration languages make service deployment and integration of resources of IoT services difficult. There is a need for authoritative service invention processes furthermore object naming services to extend the IoT proficiency.

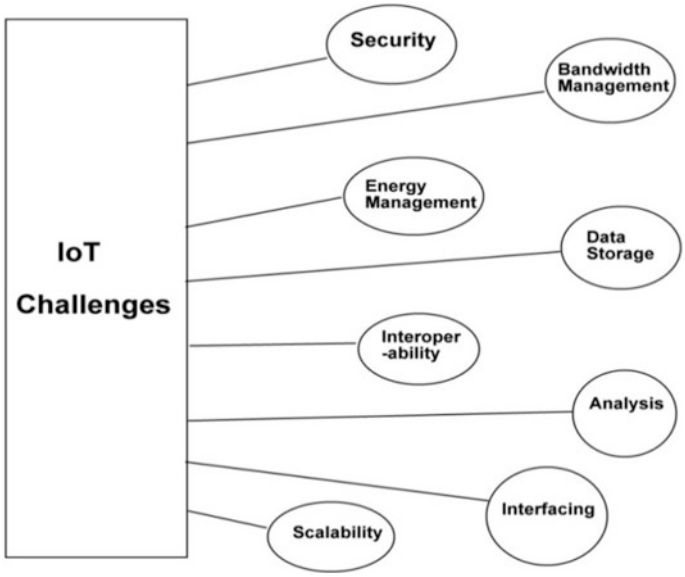


Fig. 1.3 Pictorial representation of internet of things challenges

6. User does not have any information about data streams produced by IoT devices and interior functionalities of devices which are used in his IoT system. This will turn to security vulnerabilities like device performs unwanted functions and collects more data than user intent.
7. Industrial companies must focus on challenges raised at hardware and software coexistence in the region of IoT. Dissimilar devices collaborate with a variety of communication protocols through TCP/IP would definitely shape web services which shall be installed by assorted middleware explanations. To overcome the above stated problem heterogeneous protocols shall develop.
8. Most of IoT systems are a collection of identical or near identical devices but this type of systems with the same characteristics will suffer from the impact of one potential single security vulnerability.
9. IoT system devices, in general, enclose constraints of memory and processing command, which make harder on behalf of testing the software operation on them moreover, makes testing reactions more elastic to ecological change.
10. In IoT, data plays a major role in decision making. Collected raw data value is only feasible after the filtering progression executed on it. To overcome the stated problem appropriate architectural framework is obvious that can handle data mining, analysis, as well as proper decision-making services.
11. Many IoT systems deployed in uncertain environments anticipated lifetime with many long years and associated with high technical material. Because of the uncertain environment, it is difficult to make the IoT system to upgrading or reconfigure and sometimes devices will be left as orphaned devices with no means of extensive term prolong.
12. IoT is symbolized for a huge network with numerous collected devices; data engendered in express speed and generated data too much hefty in dimension, existing database administration system might possibly not properly deal. Hence IoT base data service-centric architecture must revise to handle this difficulty.
13. The higher level of IoT system is cloud, cloud compute testing is very difficult; however, there are silent breaches how to check cloud, cloud-related structures.
14. Large and high scale distributed systems dynamic behavior lead to new appearances that need to be tested.

Based on the analysis of IoT performances, it faces challenges in storage, analysis, interoperability, security, bandwidth management and energy management etc [67, 69, 70, 74, 75].

Data storage: IoT sensors, devices generate enormous quantity of records that must be process and store. The contemporary design of the data-center is not equipped to compact with the assorted nature and absolute volume of special and enterprise data. **Scalability**: With the emergent idea of IOT, it faces a foremost challenge of "scalability in IOT". Scalability is the capacity of a device to settle into the changes according surroundings and congregate the altering desires of expectations. **Interoperability**: Means capability to interrelate with additional systems. Each solution offers its individual IoT transportation, devices, APIs, and data

set-ups are principal to interoperability concerns. To facilitate flawless resource distribution among disparate IoT vendors, efforts by numerous academic circles and manufacturing bodies have come forward to assist IoT interoperability. **Security**: Security turns major concern wherever networks are position at bulky range. A few IoT appliances hold perceptive infrastructures and services. Other IoT appliances will progressively produce gigantic amounts of personal data about household, health, etc. Lack of security, privacy will build conflict to acceptance of the IoT by firm and folks. **Analysis**: As more data offered for process as well as analysis, the exploit of data mining instruments turn out to be inevitability. Advanced data mining models need to mine online data from sensor networks. **Bandwidth management**: Several IoT devices work wirelessly, some are connected. Most IoT devices make use of modest bandwidth; however the devices obtainable online means additional bandwidth will be required. As IoT develop, it will be required to make sure your set-up contain these revolutionizes. **Energy management**: Most significant key requirement for booming IoT platform procedure is associated to power expenditure as well as energy effectiveness, which bangs the entire appliance presentation, such as latency. Low-power IoT and novel battery explanations are required.

References

1. Lopez Research: an introduction to the internet of things (November 2013)
2. Pflanzner, T., Kertesz, A.: A taxonomy and survey of IoT cloud applications. EAI Endorsed Trans. Internet Things. **3**(12) (2018)
3. Lee, I., Lee, K: The Internet of things (IoT): applications, investments, and challenges for enterprises, Elsevier. Bus. Horiz. **58**, 431–440 (2015)
4. Onoriode Uviase Gerald Kotonya (2018) IoT architectural framework: connection and integration framework for IoT systems. In: Pianini, D., Salvaneschi G. (eds.) First workshop on Architectures, Languages and Paradigms for IoT EPTCS, vol. 264, pp. 1–17. https://doi.org/10.4204/eptcs.264.1
5. Tiwary, A., Mahato, M., Chidar, A.: Internet of Things (IoT): Research, Architectures and Applications. Int. J. Futur. Revolut. Comput. Sci. & Commun. Eng. **4**(3), 23–27 (2018). ISSN: 2454–4248
6. Xu, L.D. He, W., Li, S.: Internet of things in industries: a survey. IEEE Trans. Ind. Inform. **10** (4) (2014)
7. Ray, P.P.: A survey on internet of things architectures. J. King Saud Univ.—Computer Inf. Sci. 291–319 (2018)
8. Dias, J.P., Couto, F., Paiva, A.C.R., Ferreira, H.S.: A brief overview of existing tools for testing the internet-of-things. In: 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (2018)
9. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
10. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of things: vision, applications and research challenges. Ad Hoc Netw. **10**(7), 1497–1516 (2012)
11. Wu, Y., Sheng, Q.Z., Zeadally, S.: RFID: opportunities and challenges. In: N. Chilamkurti (ed.) Next-generation wireless technologies. Springer, New York, NY, USA, Ch. 7, pp. 105–129 (2013)

12. Ilie-Zudor, E., Kemeny, Z., van Blommestein, F., Monostori, L., vander Meulen, A.: A survey of applications and requirements of unique identification systems and RFID techniques. Comput. Ind. **62**(3), 227–252 (2011)
13. Han, C., Jornet, J.M., Fadel, E., Akyildiz, I.F.: A cross-layer communication module for the internet of things. Comput. Netw. **57**(3), 622–633 (2013)
14. Guinard, D., Trifa, V., Karnouskos, S., Spiess, P., Savio, D.: Interacting with the soa-based internet of things: discovery, query, selection, and on-demand provisioning of web services, IEEE Trans. Serv. Comput., Jul./Sep. **3**(3), 223–235 (2010)
15. Gama, K., Touseau, L., Donsez, D.: Combining heterogeneous service technologies for building an internet of things middleware. Comput. Commun. **35**(4), 405–417 (2012)
16. Zhou, H.: The Internet of Things in the Cloud: A Middleware Perspective. CRC Press, Boca Raton, FL, USA (2012)
17. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The social internet of things (SIoT)-when social networks meet the internet of things: concept, architecture and network characterization. Comput. Netw. **56**(16), 3594–3608 (2012)
18. Marsan, C.: The internet of things overview—understanding the issues and challenges of more connected world. Internet Soc. (2015)
19. Valerio, P.: Google: IoT can help the disabled. Information Week (2015)
20. Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., Aharon, D.: The internet of things: mapping the value beyond the hype. McKinsey Global Institute (2015)
21. Duffy Marsan, C.: IAB releases guidelines for internet-of-things developers. IETF J. 11(1):6–8 (2015); Internet Eng. Task Force, July 2015. Web. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf
22. Tschofenig, H.: Architectural considerations in smart object networking. Tech. no. RFC7452. Internet Architecture Board, Mar. Web. https://www.rfc-editor.org/rfc/rfc7452.txt (2015)
23. Giusto, E., Gandino, F., Greco, M.L., Rebaudengo, M., Montrucchio, B.: A dense RFID network for flexible thermal monitoring. IEEE (2018)
24. Ren, G.L., Khairi, N.A.B.F., Ismail, W.: Design and implementation of environmental monitoring using RFID and WSN Platform. In: 2016 IEEE Asia-Pacific Conference on Applied Electromagnetics (APACE) 11–13 December 2016 at Langkawi, Kedah, Malaysia (2016)
25. Nagpurkar, A.W., Jaiswal, S.K.: An overview of WSN and RFID network integration. In: IEEE Sponsored Second International Conference On Electronics And Communication Systems(Icecs '2015) (2015)
26. Sung, J., Lopez, T.S., Kim, D.: The EPC sensor network for RFID and WSN integration infrastructure, IEEE computer society. In: Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops(PerComW'07) (2007)
27. Bhanu Chander, K.: Introduction to wireless sensor networks, soft computing in WSN. CRC press, Taylor and Francis Publications (2018)
28. Khan, M.S., Islam, M.S., Deng, H.: Design of a reconfigurable RFID sensing tag as a generic sensing platform toward the future internet of things. IEEE Internet Things J. **1**, 300–310 (2014)
29. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): a vision, architectural elements, and future directions. Futur. Gener. Comput. Systems. **29**(7), 1645–1660 (2013)
30. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**(1), 52787–52805 (2010)
31. Bhuvaneswari, V., Porkodi, R.: The internet of things (IoT) applications and communication enabling technology standards: an overview, CPS. In: 2014 International Conference on Intelligent Computing Applications (2014)
32. Mihovska, A., Sarkar, M.: Smart connectivity for internet of things (IoT) applications. New Advances in the Internet of Things, Springer International Publishing AG (2018)
33. Coetzee, L., Eksteen, J.: The internet of things—promise for the future? an introduction. In: 2011 IST-Africa Conference Proceedings, May, pp. 1–9 (2011)

34. Nordrum, A.: Popular internet of things forecast of 50 billion devices by 2020 is outdated (2016). [Online]. Available: https://goo.gl/EnE3td
35. Stankovic, J.A.: Research directions for the internet of things
36. Taivalsaari, A., Mikkonen, T.: A roadmap to the programmable world: software challenges in the IoT Era. IEEE Softw. **34**(1), 72–80 (2017)
37. Mohan, N., Kangasharju, J.: Edge-fog cloud: a distributed cloud for internet of things computations, In: 2016 Cloudification of the Internet of Things (CIoT). Nov, pp. 1–6 (2016)
38. Beizer, B.: Software Testing Techniques. Dreamtech Press (2003)
39. IEEE: IEEE standard glossary of software engineering terminology. IEEE Std 610.12–1990, Dec, pp. 1–84 (1990)
40. Ostrand, T.: White-box testing. Encycl. Softw. Eng. (2002)
41. Linzhang, W., Jiesong, Y., Xiaofeng, Y., Jun, H., Xuandong, L., Guo, Z.: Generating test cases from UML activity diagram based on gray-box method. In: Software Engineering Conference, 11th Asia-Pacific Conference IEEE, pp. 284–291 (2014)
42. Edwards, S.H.: A framework for practical, automated black-box testing of component-based software. Softw. Test., Verif. Reliab. **11**(2), 97–111 (2001)
43. Koopman, P.: Embedded software testing. [Online]. Available: http://www.ece.cmu.edu/\~ece649/lectures/08\testing.pdf (2011)
44. Kirichek, R., Koucheryavy, A.: Internet of Things Laboratory Test Bed, pp. 485–494. Springer India, New Delhi (2016)
45. Bai, X., Li, M., Chen, B., Tsai, W.-T., Gao, J.: Cloud testing tools. In: Service Oriented System Engineering (SOSE), 2011 IEEE 6th International Symposium on soft testing IEEE, pp. 1–12 (2011)
46. Gluhak, A., Krco, S., Nati, M., Pfisterer, D.: A Survey on facilities for experimental internet of things research. IEEE Commun. Mag. (2011)
47. Zorzi, M.: From today's INTRAnet of things to a future INTERnet of things: a wireless and mobility related view. IEEE Wirel. Commun. **17**(6), 44–51 (2010)
48. Arora, A.: Kansei: a high-fidelity sensing testbed. IEEE Internet Comput. **10**, 35–47 (2006)
49. sensLAB.: Very large scale open wireless sensor network testbed. http://www.senslab.info/ (2010)
50. Handziski, V.: Twist: a scalable and reconfigurable testbed for wireless indoor experiments with sensor networks. REALMAN, pp. 63–70 (2006)
51. Persson, P., Angelsmark, O.: Calvin–merging cloud and IoT. Procedia Comput. Sci. **52**, 210–217 (2015). https://doi.org/10.1016/j.procs.2015.05.059
52. Alliance, A.: AllJoyn framework. Available at https://allseenalliance.org/framework/documentation/learn/architecture (2016)
53. Nguyen, X.T., Tran, H.T. Baraki, H., Geihs, K.: FRASAD: a framework for modeldriven IoT application development. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), IEEE, pp. 387–392, (2015)
54. Eclipse SmartHome. Available at https://eclipse.org/smarthome/getting-started.html#developers
55. Jo, D., Kim, G.J.: ARIoT: scalable augmented reality framework for interacting with Internet of Things appliances everywhere. IEEE Trans. Consum. Electron. **62**(3), 334–340 (2016). https://doi.org/10.1109/tce.2016.7613201
56. De Souza, L.M.S., Spiess, P., Guinard, D., Köhler, M., Karnouskos, S., Savio, D.: SOCRADES: a web service based shop floor integration infrastructure. Internet Things Lect. Notes Comput. Sci. 50–67 (2008). https://doi.org/10.1007/978-3-540-78731-0_4
57. Sfar, A.R., Natalizio, Enrico, Challal, Yacine, Chtourou, Zied: A Roadmap for Security Challenges in Internet of Things. Digit. Commun. Netw. (2018). https://doi.org/10.1016/j.dcan.2017.04.003
58. Sadeeq, M.A.M., Zeebaree, S.R.M., Qashi, R.: Internet of things security: a survey. In: 2018 International Conference on Advanced Science and Engineering (ICOASE), Kurdistan Region, Iraq (2018)
59. Ammar, Mahmoud, Russello, Giovanni, Crispo, Bruno: Internet of things: a survey on the security of IoT frameworks. J. Inf. Secur. Appl., Elsevier **38**, 8–27 (2018)

60. Kouicem, D.E., Bouabdallah, A., Lakhlef, H.: Internet of things security: a top-down survey. Elsevier, Comput. Netw. **000**(2018), 1–24 (2018)
61. Ning, H., Liu, H.: Cyber-physical-social based security architecture for future internet of things, advances in internet of things, January 14, **2**(1) (2012)
62. Chen, P.Y., Cheng, S.M., Chen, K.C.: Information fusion to defend intentional attack in internet of things. IEEE Internet Things J., 1:337–359 (2014)
63. Bagula, B., Erasmus, Z.: IoT emulation with cooja, In ICTP-IoT Workshop (2015)
64. Zeng, X., Garg, S.K., Strazdins, P., Jayaraman, P.P., Georgakopoulos, D., Ranjan, R.: IOTSim: a simulator for analysing IoT applications. J. Syst. Architect. **72**, 93–107 (2017)
65. Han, S.N., Lee, G.M., Crespi, N., Heo, K., Van Luong, N., Brut, M., Gatellier, P.: DPWSim: a simulation toolkit for IoT applications using devices profile for web services. In: 2014 IEEE World Forum on Internet of Things, WF-IoT 2014, pp. 544–547 (2014)
66. Ahmad, A., Bouquet, F., Fourneret, E., Le Gall, F., Legeard, B.: Model-Based Testing as a Service for IoT Platforms, pp. 727–742. Springer International Publishing, Cham (2016)
67. Vermesan, O., Friess, P., Guillemin, P.: Internet of things strategic research roadmap. Internet Things: Glob. Technol. Soc. Trends **1**, 9–52 (2011)
68. Pan, J., McElhannon, J.: Future edge cloud and edge computing for internet of things applications. IEEE Internet Things J. **5**(1) (2018)
69. Jeong, Yuna, Joo, Hyuntae, Hong, Gyeonghwan, Shin, Dongkun, Lee, Sungkil: AVIoT: Web-based interactive authoring and visualization of indoor internet of things. IEEE Trans. Consum. Electron. **61**(3), 295–301 (2015)
70. Looga, V., Ou, Z., Deng, Y., Yla-Jaaski, A.: Mammoth: A massivescale emulation platform for internet of things. In: 2012 IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS), vol. 3, pp. 1235–1239. IEEE (2012)
71. Pflanzner, T., Kertesz, A., Spinnewyn, B., Latre, S.: MobIoTSim towards a mobile IoT device simulator. In: Proceedings—2016 4th International Conference on Future Internet of Things and Cloud Workshops. W-FiCloud 2016, pp. 21–27 (2016)
72. Levis, P., Lee, N.:Tossim: a simulator for tiny os networks, UC Berkeley, September, vol. 24. (2003)
73. Li, Changzhi, Member, Senior, Muñoz-Ferreras, José-María: Overview of recent development on wireless sensing circuits and systems for healthcare and biomedical applications. IEEE J. Emerg. Circuits Syst., IEEE (2018)
74. Said, O., Masud, M.: Towards internet of things: survey and future vision. Int. J. Comput. Netw. **5**(1), 1–17 (2013)
75. Kabalci, Y.: IEEE 802.15.4 Technologies for S mart Grids, Springer Nature Singapore Pte Ltd. In: Kabalci, E., Kabalci, Y. (eds.) Smart grids and their communication systems, energy systems in electrical engineering (2019)

Chapter 2
A Framework of Learning and Communication with IoT-Enabled Ecosystem

Jay R. Bhatnagar

Abstract Internet of Things or IoT is fast emerging as the ubiquitous data-directed solution for autonomous all-machine networks. In this article we propose an IoT-enabled framework that performs two interlinked data-driven roles—communicating intelligence and intelligent communication. The first role points to harvesting multi-variate data which varies in space-time for knowledge and features whereas the latter role deals with control and inference derived from the sensed data. We integrate these roles in smart architecture and apply it to probe critical problems in domains such as Transport, Energy, Environment and Telecom. The discussion on IoT-enabled system proposes novelties such as digital divide of supply versus demand and workflow; graph-based learning of state-space and formulates energy efficiency of IoT node. The case study for vehicular traffic reveals that IoT-enabled system offers reliable, easy to scale, AI integrated and efficient communication that can complement performance with the existing networks.

Keywords IoT network · Deep learning · Graphical model · Mega city · Vehicular traffic · Energy efficiency · Environment · Communication theory

2.1 Introduction

The continuously rising inequity in the supply versus demand of growth indicators such as transport, energy, environment and telecommunication has presented many challenges and affected day-to-day human life. There are several surveys and research studies that have formulated qualitative and quantitative relationships among various features of these indicators in recent times [1]. One such study points to 55% of world's population reportedly burdening cities and consuming 3% of total earth's land resources and 70–80% of energy supplies for 2018. In order to

J. R. Bhatnagar (✉)
Computer Science and Engineering, Presidency University, Bengaluru, India
e-mail: jrb@iitdalumni.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_2

curtail the escalation of problems in these domains, a comprehensive plan and solution was proposed in the form of smart city or mega city [1–3]. A key aspect adopted in such solutions is the use of smart algorithms and data-driven capabilities by processing the parameters of indicators for data mining and knowledge discovery. The recent advances in machine learning techniques have led to powerful tools for analyzing complex space-time patterns in acquired data to perform real-time prediction and control [4]. This typically involves big data which has time-varying statistical attributes used in learning models that generate solutions or answers directly from the sensed data [4, 5]. Such algorithms along with conventional hardware yield smart architectures also called Intelligent Solutions (IS). The hardware and software components typically perform measurement and processing of data harnessed from the physical variables or parameters of interest of the indicators [6]. Most IS are primarily engaged in two modes of data-directed activities—control centric and communication centric modes. The modes give rise to complement and related networks—firstly, where systems aid end-to-end connect of human-access and interface with machine networks and secondly, where end-to-end roles fully involve machine actors. The IoT or Internet of Things [7] can be functionally described as distributed ad Hoc control with mostly binary actions or data at elements tied in a communication network. The rapid growth in IoT-enabled systems is notably due to two factors—miniaturization of hardware elements and need for ubiquitous connectivity combined with smart computing or control. In Fig. 2.1 we illustrate IoT ecosystem in the nucleus with issues related to

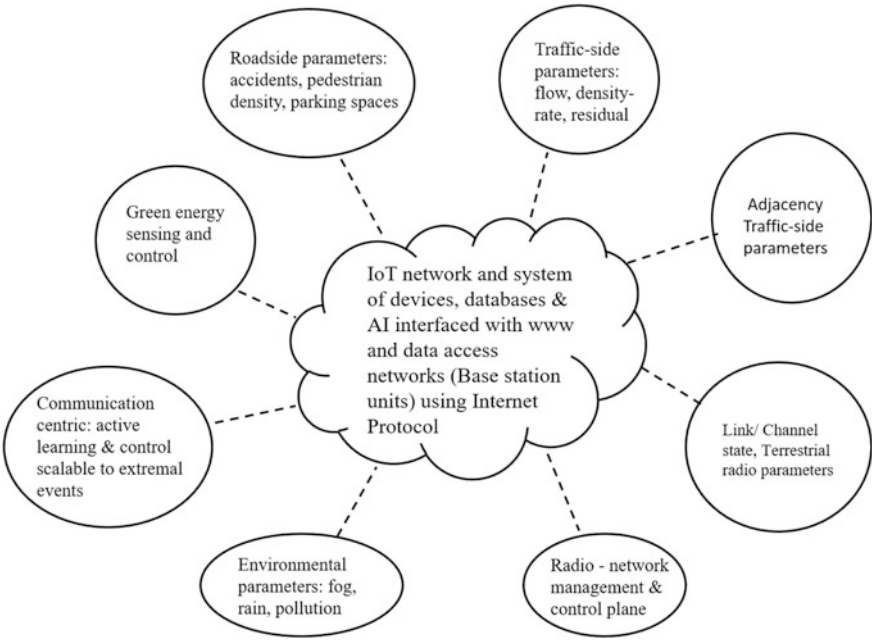


Fig. 2.1 Group of indicators in IoT enabled ecosystem for Mega city

sensing and management in the domains of—energy, environment, transport and telecommunication. We broadly adopt a communication theoretic approach to propose IoT-enabled ecosystem which is reliable, scalable, energy efficient with AI (Artificial Intelligence) abilities.

The first issue in this article treats the exponential growth of vehicular traffic that has competitively outpaced the growth of many supporting urban resources and infrastructure. Metro cities are now home to growing commercial, business and residential needs and thus are expected to provide rapid support to fast, secure and resource-efficient connectivity. Travel from a point to any other point in city suffers from many bottlenecks depicted by delay-connectivity profile of the road infrastructure resulting in a regenerative increase of delay and other traffic issues. Beyond a certain throughput or active vehicle rate on the road network, problems can escalate to continually aggravate the situation with increased congestion and delays. This provides us strong reasons for studying effective detection and correction mechanisms to tackle such issues. We conjecture that some form of the Moore's law can be formulated to model the growth indicators in such domains [8]. For example, in this case, traffic density in the exponent versus per unit road space can be applied to depict effective shrinking of roads incumbent upon growing vehicle population. A practical view emerging from this also reveals that resources like roads are really becoming noisier and compressed as vehicular density is increasing which points to increase in delays, pollution, accidents and congestion. Next, let us consider cellular network and some of its long-standing problems that continue to be hard and frugally addressed by use of adhoc solutions till time arises when these also may fail. Similar to situation denoting vehicular traffic, data networks also suffer from bandwidth-power limited resources that must accommodate increasing population of data-streams and users and meet some basic Quality of Service (QoS) for this traffic. Other long standing issues in telecom network include—maintaining reliable communication in presence of channel effects like heavy rain, fog and adverse environmental factors; provide a coverage that can guarantee QoS in patches of network that are remote or in the fringe areas with respect to Base Station (BS)—in fact, hotspots and weak coverage are typically hard problems that may continue to persist even after several iterations of cellular planning and resource optimization [9, 10]. There are other issues such as signal loss and poor coverage in urban dense clutters and in regions with heavy user-density or traffic in the radio network. Cognitive algorithms have been studied for deployment to assist network management plane to manage resources and streamline services in the network. These are based on radio measurements of channel characteristics, both physical and logical at frequent sampling times and this data is transmitted on common control and broadcast channels. Interestingly, learning from such measurement updates have been traditionally used in the physical, MAC and network layer at critical nodes like routers or central nodes that manage services and access to network resources. Network conditions such as activity or demand-side priority, prediction of demand and radio channel states can be typical in smaller areas and typically represented over a narrow area based on time-correlated observations. To the best of our knowledge no prior work or study has been done that utilizes these

points. An effective assessment and management framework such as IoT enabled ecosystem is expected to exhibit distributed sensing, minimum redundancy of updates and cover essential physical measurements to enable fast and accurate corrective actions. Notice that there may be many problems and situations that closely depict parallel between a vehicular network and data network. In this article, we introduce an IoT-enabled solution for smart traffic management using state-space model of traffic parameters that is useful in the detection and correction of issues leading to scalable, effective and timely managed traffic.

As seen in Fig. 2.1, another form of growth indicator which is time-cumulative is given by environmental parameters like wind velocity, pollution, composition of various fluids, health hazards, leakage and early detection of events which in some instances may scale up to bigger or connected problems. In this case, IoT-enabled ecosystem offers advantages both for slow sensing and very fast sensing needs in reliable and time-efficient measurement and inference. Another vital indicator for megacity is mapping area-wise distribution of renewable energy sources and implementing green energy sources that can provide additional support to distribution network of energy for medium to low electric mobile loads. Notable here is the widespread use of mobile computing and smart digital solutions and that collectively such equipment needs frequent recharge during movements. In this scenario, alternate sources of energy particularly green energy hold great promise in creation of a dependable energy network grid that can run along with the conventional power line network. As technology of sensing and energy conversion are steadily improving, green energy solutions are expected to become integral part of several mobile and central elements of the IoT ecosystem [11]. As a novel outdoor platform, we survey and discuss important parameters related to energy issues for IoT-enabled ecosystem formulated using conversion capacity and review some prior work in this direction. The IoT active-drones proposed in this work provide an energy and bandwidth efficient basis for communication of traffic, environment, energy and communication parameters along with ubiquitous connectivity based on IP (Internet Protocol) which covers local ad hoc networks and higher network entities of the cellular architecture.

The IoT platform can be implemented with existing hardware and programming tools to give a flexible connectivity enabling individual devices to participate co-operatively and ubiquitously with Internet Protocol suite which is shown based on four-layers of the OSI [10]. The carrier technology and network architecture with regards to physical layer mostly depends on the functions and communication needs of IoT-enabled network. However, generally, IoT is an adhoc sensor network with full-duplex ability to sense, store and communicate data or database and therefore autonomously manage various types and grades of services. Notably however, the data interfaces for human actions or machine actions inherently have two major roles—intelligent communication and communicating intelligence. In addition to the connectivity suite, other data-linked actions with IoT-enabled network elements are based on machine learning [8, 11]. We aim to integrate this into our solution and use specific types of deep learning neural networks to achieve

autonomous machine network. A learning network empowers the desired computational power to the proposed IoT ecosystem which finally aims to integrate actions with communication and knowledge discovery.

2.2 Intelligent Solution for Traffic: Prior Work

Most prior work in traffic control and light switching has considered simple parameters like vehicle count and other objects in time-domain analysis of static images [12–14]. The use of infra-red sensing or IR radar type detection methods has also been studied to monitor and control vehicular traffic however, IR is limited in terms of the range, span and higher energy consumed moreover, it also suffers from limited communication abilities for dynamic remote sensing of traffic data arising from different types of motion. This approach has other limitations as an open loop control system for setting of the traffic light switching with attributes and control fixed by microcontroller environment. Authors in [12] rely on communication between stationary road side, junction side and some mobile units to exchange traffic parameters though the method for detection of vehicles is not clear. Authors in [13] discuss vehicular ad Hoc network and propose simple camera mounted setup with traffic lights for monitoring vehicle count and density by video analysis of the acquired frames. Their work has shown a constrained method using statically mounted camera which performs visual acquisition that is sensitive to optical conditions or time of the day and illumination. Authors in [14] give comprehensive discussion of techniques based on video processing for ITS. Their work introduces various operating modes of lighting, traffic states and use of computer-vision techniques with static camera in average visibility conditions for short range detection. The work does not discuss insights related to technology, experimental frame work and video processing algorithm employed in the studies. Most of the recent research has shown Intelligent Transport Solutions (ITS) with an integrated system for smart management of traffic lights by deploying real-time video analytics and closed loop control of traffic parameters such as number of vehicles or density of vehicles on road. By closed-loop we mean that traffic pattern is iteratively detected and updated in the control algorithms and this is used to provide corrective steps in light timing and other aspects of traffic. In our view smart traffic management has two-fold tasks—(i) detecting traffic related parameters such as vehicle count and vehicle density and, (ii) correcting traffic parameters in closed-loop operation. Some of the computationally complex tasks like multimedia and video processing can be implemented with open source programming and embedded processors. Multiple snap-shots or video frames acquired over certain coherence-time are utilized to train the estimate of traffic parameters.

We list some of the main shortcomings in prior approaches—(i) employ limited area or range of acquisition combined with limited fixed or stationary sensing mechanism and constraints that can severely affect in event of occlusion, bad weather conditions; (ii) data is inaccurate and slow to track as the sensing regions

offer limited data only from select points close that are static with respect to traffic lights; (iii) issues like object occlusion, fades due to weather like rain or fog, channel variations can lead to many inaccuracies and delays in target objects. Moreover, other issues like range—resolution versus quality of sensing are typically not considered in the prior methods. Most prior methods rely on utilizing the frames or images which offer high quality snapshots of the targets; (iv) it does not explore the dynamics and correlated space-time nature of traffic flow arising from various sections of neighborhood spaces. Infact the close correlation between various paths of the connectivity graph of roads and intersections can be very vital if additional data is mapped and sensed by these models to cover traffic detection and correction.

2.3 IoT Based Smart Traffic Management

The frame work proposed in this article motivates the following main novelties and improvements in sensing, control and use of data related to vehicular traffic—(i) employ density rate as additional parameter to estimate time-dynamic behavior of traffic, (ii) employ mobile IoT-enabled drone set-up to collect more accurate real-time visual data of vehicular traffic over longer stretches, (iii) employ graph-based system and traffic data based on state-space in order to cover time derivates. This is aimed for giving necessary advisory with broadcast on website and interactive live access to end-users through the web portals [5]. In this work we propose an ITS framework with IoT-enabled drones that intermittently fly and span certain measurement area of traffic. These drones and other IoT subsystems employ solar green charging systems in flight and rest modes. The use of drones in on-off flight mode logically follows from the varying demands of traffic conditions in peak-traffic and moderate-traffic operations and, hence are more pragmatic than continuous processing. The on-off mode also offers advantage of higher energy efficiency and improving battery life of the active load systems. In order to improve the accuracy and to gain realistic estimate for flight or rest times of the drone, we introduce density rate as parameter that denotes changes in the density of vehicle count per unit area spanned over known time. If density rate is positive then traffic flow has positive gradient and if it is negative then the gradient is negative. This is used with other parameters to define the switch timings of traffic lights.

Figure 2.2. depicts the proposed lay out that shows functional set up for IoT-ITS. The scheme deploys drones to acquire data from two neighboring road stretches as images or time-limited video frames. The data from cameras C-1 and C-2 of IoT active drones D-1 and D-2 is wirelessly relayed through Smart Communication Unit (SCU) mounted in vicinity of the traffic light. In Fig. 2.2 the SCU is depicted as IoT hub.x. The number of such IoT hubs or SCUs can vary dependent on the density estimate of MS (Mobile Stations) or users and vehicles. In the end, SCUs partly function as secondary base stations in IoT activated D2D (Device to Device or Database) connection utilizing select resources of the network.

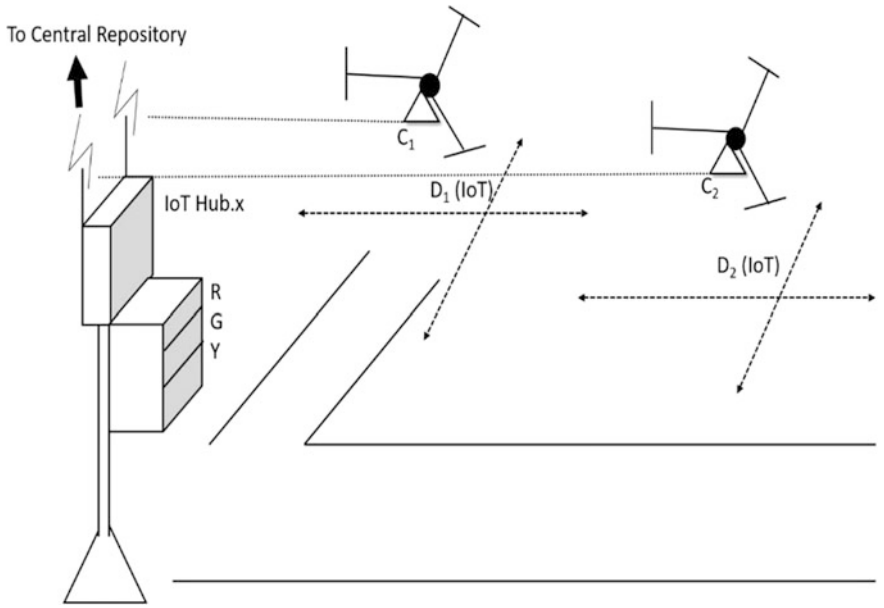


Fig. 2.2 System elements in IoT-enabled ITS showing SCU, drones at crossings

The SCUs can operate by stealing network resources from serving BS (Base Station) to support data access and also provide internet access with end MS (Mobile Stations). In this scenario mobile D-1 span covers the head x-y area onwards from traffic light as the drone moves at a suitable height and similarly, mobile D-2 span covers the subsequent tail area. The use of at least two drones helps sampling the physical space and dividing the coverage area while connecting SCU to acquire visual data. The use of multiple drones per stretch in this framework gives diversity of spatial-system sampling based on at least two sensors per sensing cycle. Moreover, multiple sensors can assist in correlations derived for error control of real-time visual data which helps in generating accurate features and extending inference over larger space. This information is sent to SCU memory ports marked for D-1 and D-2 respectively. The number of drones and covered span is recommended based on precision, spatial range and accuracy of sensors, other tasks such as time-multiplexed sharing between multiple traffic posts or dedicated drones for busy lights and shared resources for lower demand. The data access employs packet switched transmission IPv4 protocol, and the system can be designed to consume power efficiently for data towards SCU. More over the drones are frequently required to fly and update if traffic density and rate parameters show significant or increasing trend from previous observations stored in SCU. Since the drones are IoT-enabled so, live data feed can be relayed wirelessly using the SCU to remote databases and master stations. The captured data is mapped with real-time representation and processed to determine the overall traffic pattern both for detection

and correction. The data generated is transmitted to central repositories, besides SCUs, for analytics and real-time display on website or remote client applications run on mobile computing system. For most purposes, data refers to the features derived from observed samples that can be used for correction and necessary recommendations like managing traffic flow with predictive routing, creating diversion and avoidance of congestion and related problems.

SCU acts as the main computational and communication unit that determines crucial parameters handling the complete suite of intelligence capabilities like—processing images, handling variable length frames or feature-representation of various sources, determining—density, density rate; handling data and computations over communication links and in this example controlling flight times of drones. Density refers to the number of vehicular objects detected over a certain coverage area or cell from the images captured by IoT drone. Density rate reflects the change in density with respect to some known interval of time. As mentioned somewhere earlier, customarily, density was used to model the traffic flow conditions over a limited space. As discussed earlier we model system in terms of its state-space equations comprising of parameter data or measurement variables and its time-derivates. A vital command from the SCU intelligence features control of traffic switch timings with necessary correction of density rate parameter in closed-loop mode. The timing can be decreased or increased based on the current estimate of density rate say, based on a positive or negative gradient. In addition to sensing and communicating the traffic flow parameters, IoT-enabled drones can capture variety of direct environmental parameters like humidity, temperature and other parameters from images and sensors to detect ambient conditions that might influence traffic or driving conditions thereby incorporating the data for advisory and repository. This can help generate recommender data to facilitate driving with alerts and offer warnings that can be depicted with user-interactive web tools.

In Fig. 2.3 we consider a sub-graph of a vehicular traffic network where measurements are mapped with respect to central node of this sub-set denoted as N_j. In relation to the traffic parameter and state observations at the node N_j, IoT active drones also capture data related to adjacency traffic states, for example depicted by neighborhood space comprising of nodes N_k and N_{k+1}. The sub-graph depicts active states and local exchange with message passing of traffic states performed with help of SCUs [15]. The criteria to select a vertex as central node or location of SCUs in the belief propagation network can be based on factors such as relevant traffic and activity history at the location in the network, flow profile at node and connected routes, traffic density or rate parameters. A central node for the duration is chosen such that with a high probability the density or flow rate at this node exceeds predefined thresholds. Some of the nodes that denote commonly traversed or busy stretches between nodes in the city may also natural choices for central node. The central node can be viewed as data intensive point of the traffic graph, mainly concerning with acquisition of state information around the node N_j whereas control

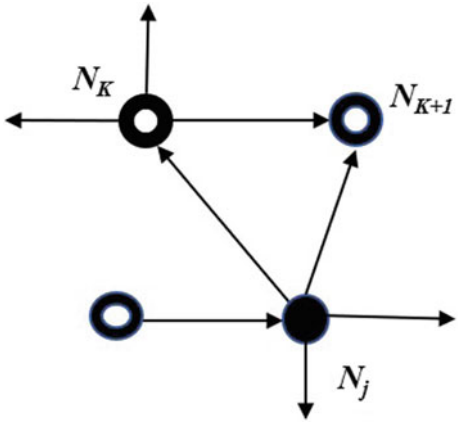


Fig. 2.3 Sub-graph on node states for traffic message passing

and other regulatory tasks can be controlled and deigned to remote nodes N_k and N_{k+1} in order to maintain closed-loop control for effective and low-complexity real-time management.

The proposed model shows the locally active paths and sub-graphs constructed from these can be effective in managing larger network with distributed constraints spanning a large coverage such as city. Prediction models play major role in such systems and discovering the correct set of sub-graphs, neighborhoods and topology properties can serve usefully in training the parametric conditions related to traffic. Some prediction models can involve correlated loading of busy states at various central nodes based on the states in its immediate neighborhood. This is essentially same as nearest-neighborhood estimation of traffic flow and the principle of similarity of traffic flows expected between physically close nodes and connected traversals like N_j and N_k, N_{k+1}. More nodes can be clustered and included in such connected sub-graphs to span the city infrastructure. Accordingly, data analytics tools and pattern clustering methods are applied to generate prediction model of traffic parameters for typical neighborhoods. In this case typicality refers to various statistical regularity conditions that are fulfilled spanning variable length observations [15]. For example, let us consider weekly, daily or hourly typical behavior of flow rate by constructing sub-graph of traffic parameters between nodes that are connected to span busy routes comprising multiple nodes. We extend the prediction model with additional parameters and state equations introducing loading factor λ_κ which denotes the accrued density estimate from other neighboring nodes which directly impact with respect to node k. We denote density parameter by variable ρ and density rate as given by $\delta\rho$. The loading factor is the algebraic sum or cumulative traffic flow density arising from a set of neighborhood nodes. Naturally, we aspire to include only those nodes in this estimate which show evidence of crossing threshold frequently enough to be regarded as a dominant neighborhood for node k. Here d denotes the direction of flow such that $d = 0$ denotes incoming

traffic and $d = 1$ denotes outgoing traffic for node k. If inward traffic is greater than outward flow, due to neighborhood conditions, then this is reflected in higher value of loading factor at the node.

$$\lambda_k = \sum_{\forall j \neq k} (-1)^d \rho_j; j \neq k \tag{2.1}$$

The prediction model can also incorporate second-order measurements for node k which provide gradient to the built-up of loading at the node denoted as R_k. This parameter essentially measures the difference of density-rate between incoming and outgoing traffic flows at the node as given by Eq. (2.2):

$$R_k = \sum \left[(-1).\delta\rho_k^{(\text{outgoing})} + (+1).\delta\rho_k^{(\text{incoming})} \right] \tag{2.2}$$

We now refer traffic states for the node k proposing system model based on state-space of flow variables where the state conditions are given by Eqs. (2.3–2.4)

$$\overline{\rho_k^{(n+1)}} = A.\overline{\rho_k^{(n)}} + B.\overline{\lambda_k^{(n)}} \tag{2.3}$$

$$\overline{\lambda_k}(\text{outgoing}) = C.\overline{R_k^{(n)}} + D.\overline{\lambda_k^{(n)}} \tag{2.4}$$

In order to depict possibility of multi-variable nature of states, we make use of the hyphenations on variables in Eqs. (2.3–2.4). The scaling factor or matrices A, B, C and D indicate observed transformations similar to state-space model [5, 16] which describes state variation at node given by Eq. (2.3) and state output at node given by Eq. (2.4). Note that the state variation is dependent on neighborhood nodes with parameter B and depending on previous state with parameter A. Likewise, we note that load state of the node as output to external system depends on density-rate at the node with parameter C and present loading of the node with parameter D. This gives a simple and effective solution resulting in real-time coverage and assessment with IoT. We discuss some of the advantages of belief propagation model which is used to provide learning of local state-space conditions at various nodes of vehicular network. The discussed parameters and model traffic states that show similarity over some localized nodes or cluster than the complete network. The physical variables of indicators covered by the article show typicality in patches randomly distributed in the span with additional need to develop databases for machine and user operations from distant locations. The first and second order time variations of flow factors convey displacement and velocity parameters related to the traffic big data parameters applicable at measurement nodes. The outlined model utilizes more data and its higher order derivative terms for learning vehicular traffic management over previous models. The graphical formulation of observation space, message passing along with machine learning functionalities proposed in this solution for traffic management can also be extended to some other IoT-enabled applications in energy, environment and telecom networks.

2.4 Implementation of IoT Drone Platform

The physical solution employs embedded computer vision and open source software like Open CV that can execute on Raspberry Pi 3 board to implement IoT drone and program set-up for control and communication suites using Internet protocol [7]. The set-up of embedded CV is recommended based on Quad-core ARM cortex processor A-53 which has nominal power usage versus performance characteristics defined for reasonably fast frame-rate processing of visual data. The features can be selected based on the robustness or invariance against channel variations with frames acquired aerially by drones flying at low speeds in coverage areas to compute various parameters. The ROI (region of Interest) markers are predefined in training phase to classify road-side conditions and traffic side objects such as detecting parking spaces, traffic states based on images of light motor vehicles (like two wheelers), medium motor vehicles (like cars), heavy motor vehicles (like truck, bus, freight carriers). Other objects like taxis and ambulance can also be trained and annotated from images. The training data employs shape, color and size features to distinctively map the object classes. Additional training is also provided to classify human objects that are slowly moving or stationary at predefined locations like road intersections for automatic switching of lights and to act on visual inputs for facilitating of pedestrian movements.

There has been considerable work in the direction of datasets generated for visual processing using drone platform. Authors in [17] report VisDrone2018 that provides a large-scale benchmark data set in processing of visual analysis to facilitate object tracking and detection on drone platforms. Other works include PASCAL VOC by Everingham et al. [18] that gives a vital benchmark for generic object detection as in it provides standardized test bed for object detection, classification, segmentation like ImageNet [19] for over 20 object classes from 21,738 annotated images. These works rely on box bounding to mark box shaped approximation of various object classes that are predefined from a training data set. Our work mainly views edge-based boundary or shape detection with colors for some typical vehicular objects and humans built using Open CV in embedded environment.

There are some interesting comments that stem from the proposed framework and analysis. The drone platform in our case is capable to operate in full-duplex. It transmits acquired visual images on IoT optimally utilizing both moving sensor and coverage along with data transfer speed and coverage that can be variables defined by SCUs and defined by features of traffic, which essentially is data-driven architecture. It can be useful to incorporate inter-messaging between drones and some lower-level SCU protocols with the drones to allow co-operative communication between the drones and also among neighboring SCUs. Infact the IoT-platform can be viewed as node in cellular topology with hierarchical roles attributed to the SCUs in terms of detection, inference and control type operations. Such functions inherently also depend on location, infrastructure to be controlled and criticality of parameters from the acquired observations. This type of network designed with IP

protocol is expected to consume modest portion of bandwidth-power resources. In this regard, the overall IoT-enabled network resources can be optimally utilized by greedy techniques that are mostly known to meet the performance needs with low complexity.

2.5 Communication in IoT Ecosystem

The functional goals in applying IoT-enabled solution to issues in various domains is for achieving twin roles of—CI (Communicating Intelligence) and IC (Intelligent Communication). Of these roles, CI is mostly associated with IoT functions like measurement, control and signaling type of data that tunnels bits from end sensors and devices towards learning architecture and databases and finally to map the relevant actions and inferences tied around the data. In this sense, CI mainly covers message passing and learning roles and broadly applies it to solve issues in the vehicular traffic network and data traffic network [9, 10]. Whereas the IC role is mainly attached to functions in the network plane associated with active roles in terms of control, allocation of resources and use of IoT to support voice and data connectivity. We point that provision of VANET (Vehicular ad Hoc Networks) was made under IEEE 802.11 in various microwave bands of 5–7 G Hz and 600–800 M Hz. bandwidth. The purpose of VANET was to provide a minimal communication between vehicles and road side units as part of Wireless LAN solution that piecewise builts driver assistance, warning and driving related information exchange in a limited manner. This solution only provides basic qualitative information from road side terminals and WLAN accessible to vehicle units pertaining to driving and traffic. The current wide-scale use of Google Maps and such real-time voice interactive online advisory services has nearly supplanted the roles and features offered by the VANET. The VANET has also not seen wide scale applicability since inception, other than in some developed countries like U.S and Japan where it is useful for some selective services rather than as comprehensive connectivity solution.

We refer to Fig. 2.4 which explains the network interface towards higher nodes of the network facing link via BS and on other side towards the SCU and IoT drones facing end-users of vehicular network. The stack of layered functionalities are mainly given to two roles—measurement and communication of intelligence between Device-to-Device (D2D) and similarly between databases for various parametric estimates in time-iterative manner, as typical of IoT system using the stack functionalities shown in Fig. 2.5. The other purpose is to act as store and forward relay for the uplink and downlink to support data-access services via IoT network. Additionally, network control plane is also supported by IoT measurement system which learns the physical radio channel and environment with real-time measurements, traffic parameters like flow, rate and demand side variables.

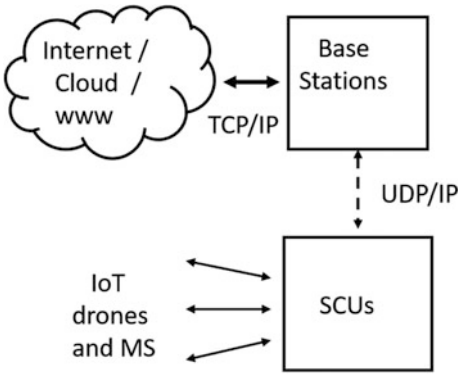


Fig. 2.4 IoT enabled architecture and Internet

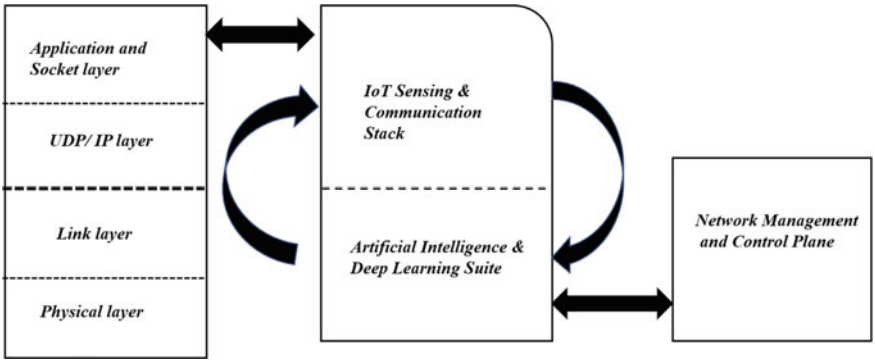


Fig. 2.5 Intelligent communication suite of IoT enabled node

The network management is central to all cellular planning and IoT brings a crucial backbone support for message passing of vital parameters related to both radio as well as vehicular traffic. In light of knowledge discovery from data, we note that IoT measurements are useful to train deep learning recurrent networks which utilize data itself with AI [6] to predict 3-tuple space comprising of—(demand profile, resource allocation/supply profile, issues or problems). The logic in so doing is to exploit the self-similarity of various parameters that exhibit a typical behavior over time [10]. Note that such measurements and estimates exhibit better similarity and prediction in local neighborhoods so that network plane can apply local solutions to cover the complete space with IoT-enabled elements like BS, SCUs, mobile sensors such as IoT drones and several other static IoT devices.

2.5.1 Communication Stack for IoT Network

We now discuss basic layer-wise stack for maintenance and control of SCU and IoT drones with the CI and IC functions [10]. Generally, known wireless local area network architectures have been discussed for use in IoT [7]. The wireless technologies for IoT implementation that are typically available in the literature nearly exhaust most known IEEE 802.xx standards [7]. This is owing to several factors such as—there is no global standard for IoT specifications suite, IoT hardware has elements which are mostly of low size, energy, traction and bandwidth; IoT signals covers bursty control as well as the more heavy switching needs of regular communication; IoT data must conform accurate and adequate communication with heterogeneous portions of the network containing IoT sensor elements, routers, cloud repositories and web-based applications. There is obviously need for more comprehensible and universal language and ontology needs at such different nodes. Various forms of wireless networks like Wi-max, Wi-fi, Zigbee, types of wireless LAN and even low-power Bluetooth are widely listed as candidates for IoT connectivity. Most of these communication standards are—limited in coverage, number of connects, throughput and access services. Additionally, these also suffer from limited use of resources and fail in scaling the network and exploiting the boundaryless property of the Internet protocol. We adopt novel approach in combining resource efficient protocols with co-existence of heterogeneous network conditions. We refer to Fig. 2.5 to give a functional description of the basic stack for IoT-enabled node.

Application layer:

Allows automated machine to machine and user interface to various databases mapped or registered on nodes covered by SCU and higher network entities. It offers interactive environment separately for machine and users to interface with variety of services enabling entity and host exchange in data-directed modes. Socket programming and basic security functions of session and presentation layers can also be integrated. It features operating system features capable of processing sensed database along with autonomous configuration and connect with SCUs and base stations. It can also assume the active role of analyzing data from other adjacent IoT devices and systems to generate timely report-maps which employ html embedded databases. This role is eventful in polling analytics from multi-space-time IoT measurements.

UDP/ IP layer or Network layer:

The addresses are short-term allocated to mobile agents or end-systems, managed by the interface with SCUs. The co-operative link can employ long-distance multi-hop paths with TCP/IP in referring the end-systems on uplink towards the BS. The UDP (User Datagram Protocol) is primarily meant to achieve efficient, real-time communication of packets without need of best effort or reserved service like TCP/IP. The datagram is employed for switching data flow since communication path towards end-vehicular users typically involves limited hops between

SCUs and end-systems. The dominant data is mostly measurements exchanged from various devices. More so, the data access sought by MS also associates multimedia and web which may mostly contain bulk transfer records. The overall purpose is to run very high rates with TCP/IP from BS and servers-side where reliability is constraint and to operate at slower rates with a UDP/IP from BS to MS over the SCUs. This also requires nominal power, memory and other needs in communication paths comprising of hops that separate BS from vehicular MS. This access technology and functioning not only appears efficient on IoT resources but also saves computational burden. In this manner the end-to-end links optimally integrate use of TCP/IP and connectionless UDP/IP suite.

In the mode of CI, datagrams typically carry measurement and signaling data from devices towards databases. The CI features data collection and this allows for timely updates of various parameters related to vehicular traffic sensed for learning network or the AI which drives necessary corrective actions. The link path followed is: $\mathrm{B.S} \leftrightharpoons \mathrm{SCU} \leftrightharpoons \mathrm{IoTdrones} - \mathrm{devices} \leftrightharpoons \mathrm{End} - \mathrm{users}$. Traditionally, routing tables are updated between nodes to learn optimal paths. In this case traffic states and measurements are learned using Message Passing Algorithm (MPA) used to train RNN (Recurrent Neural Network) Deep learning. This consolidates the state information derived from neighborhood nodes for control and allocation of services both in data and vehicular networks.

Link layer:

Forward error correction, link state information, channel measurements and other sensory measurement, flow and rate control functions associated for packet switching are handled in this layer. These are mainly associated to maintain efficient and reliable communication and functioning in tandem with controlling BS and end-systems of IoT cellular network. Allocation of communication resources may also utilize link state information in choosing signal design and coding scheme, evaluation of Quality of Service (QoS) and such other factors. Service-allocation in this architecture gives rise to time-dynamic mapping of resources with aid of prediction.

Physical layer:

Physical layer signal design and network management utilizes the training and learning models based on Deep learning RNN (Recurrent Neural Network). This allows effective use of CI for IC in this layer and covers—sensing, data representation of multimedia, error check and modulation, optimal power and management of physical layer resources. Almost all functions of this layer are based on recommendations offered by learning sub-systems.

2.5.2 Binary View of Coverage and Services

An important way to address resources by network plane and administer access and services for multi-access multi-user traffic is possible by the following binary

classification on the demand-side. We introduce the novel idea of viewing the mobile telecom network of subscribers or users as discretely sub-divided into—stationary or static users and mobile or vehicular users. The overall network functions also apply differently as the channel states and radio clutter are not the same for the static users who reside in commercial, residential settings with slow varying flat fade locations and the rather fast varying location and channel states of mobile vehicular users.

The reason for binary classification of user population emanates from the following reasons and assumptions [9, 10]:

(1) To plan and distribute radio infrastructure such as BS and Main Switches along with radio resources commensurate with the demand and location needs as distinct principles are applicable for cellular planning and cell lay-out of fixed or static versus mobile users,
(2) Residential, commercial and similar class of static users are expected to occupy dense urban radio clutter and such points typically demand high Signal-to-Noise-Interference Ratio (SINR) floor [9] due to attenuation, absorption and other forms of signal losses that are more spatially variant. This channel is mostly stationary since the clutter is fixed and the user movement is generally restricted. In such cases, the need of soft hand-off or relaying of services attached with MS from cell to another cell or BS to another BS is also not crucial due to the same reasons.
(3) Let the total user population that seeks data services on the whole be on average denoted by variable P. Actually, $P(t)$ can also be regarded as discrete valued random process but for simplicity we consider some mean path and value to base our argument of static versus mobile users [16]. The population is split into two segments—static and mobile vehicular users. Let us denote α_t as factor for static users and β_t denote factor for mobile vehicular users. We note the following with regards to conditions governing relationship between α_t and β_t. The additional movements or exodus of users roaming is a random variable which is not considered in this article as it may approximately count-in and count-out proportionately and this does not contribute to significant dynamics in terms of space-time allocation of resources in the short-term.

(a) $\alpha_{t.}.P + \beta_t.P = P$; where, α_t, $\beta_t \epsilon [0, 1]$
(b) The random variables, $\alpha_{t.}$ and β_t denote some parameters of a renewal-stochastic process, such that—$\propto_t + \beta_t = 1; \forall t \in \Re$. Notice, if α_t is birth-indicative then at the same time β_t is death indicate and hence negatively co-related. Notice that as α_t increases, implies users are depleting from the fractional $\beta_t T$ and vice versa. The co-efficients α_t and β_t denote negatively correlated random walks.
(c) As given in (b) above, $E(\alpha_t.\beta_t) = -\gamma(\tau); +\infty > \tau > 0; 1 \geq \gamma > 0$.

The condition $|E(\alpha_t.\beta_t)| = \gamma(\tau) \leq 1$ applies by application of postulates (a–b) and Cauchy-Schwartz product inequality to auto-correlation function.

The binary divide adopted by us is based on simple assumptions—radio channel and data-services (multimedia and other applications) needs for situations like mobile and static users are distinct and unique. Likewise, this dichotomy also separates the resource-access conditions and usage of resources under categories of α_t, β_t which typically denote the data-access pattern which is learned by the IoT data training a Deep learning network. Figure 2.5 illustrates this functional connect between typical OSI layers that are in use for CI and IC. The parameters pertaining to channel state and traffic are useful to train and manage traffic and aid to manage resources in network plane. The vehicular network performs mapping and update of traffic parameters with satellite communication links that routinely acquire image data to perform recognition tasks with video and image processing. However, the quality of images sensed by satellites and relayed towards earth stations is often influenced by random weather and channel losses due to long separation of transponder and objects and earth station. Satellite communication systems typically operate with very large power budgets, link margins and bandwidths suitable for broadcast applications.

The role of IoT integrated terrestrial coverage offers the next generation technology for navigation, global information systems, control and access of information using the Internet protocol and databases that give accurate time sensitive data pooled from close and accessible locations anywhere in network access. In this sense, IoT really offers a locally optimal and globally distributed solution to intelligently fill gaps in communication as well as communicate essential information from end-systems using the power of AI. In this way the IC and CI functionalities in IoT act in co-operative mode and this covers both static and mobile end-systems in the network. In the physical layer, which utilizes a subset of the communication stack, IoT provides short-to-medium range link which is stable and offers data rates with high QoS [5]. As cited earlier, the use of TDMA (Time Division Multiple Access) methods is necessary for improving the efficiency of service requests in multi-access multi-user environment. The CI role is effectively covered with real-time coverage and message passing to allow both deep learning and user visualization of this data via real-time interfaces. The function of IC also associates assessing needs for communication of end-users using parameters [11, 15] like user-density, activity rate, minimum span of hop, link data, mobility and demand prediction that is vital in deep learning architecture to intelligently manage and operate the network plane. In the next section we discuss the role of AI in twin modes of CI and IC for IoT-enabled application.

2.6 IoT Integrated with AI

The role of communicating intelligence in IoT system aims to offer real-time support for data-access in the vehicular network. The hierarchical features or parameters useful in the training of various layers of RNN (Recurrent Neural Network) are derived from various features depicting the traffic pattern [4, 6].

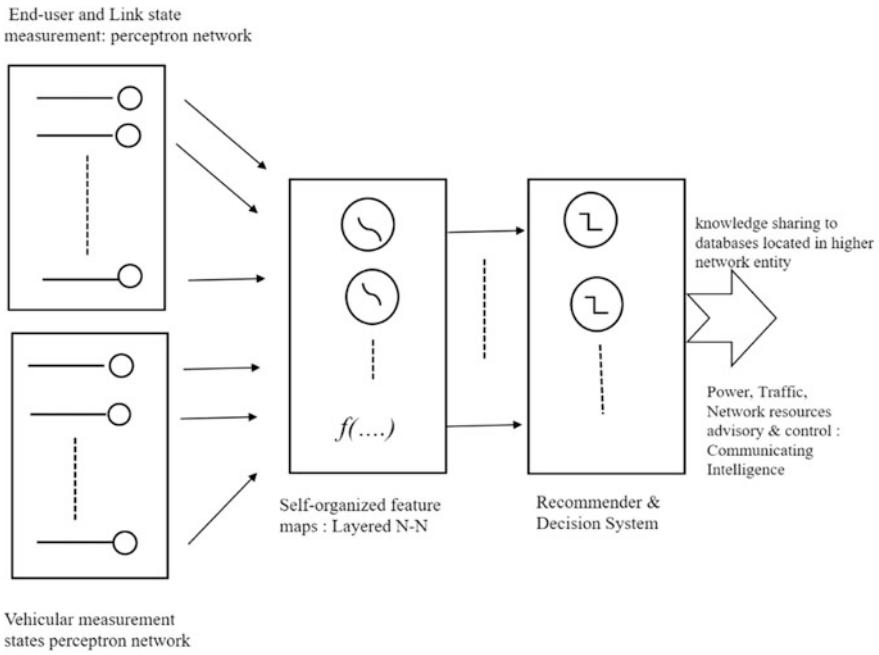


Fig. 2.6 Multi-layered deep learning for CI functionality

We refer to Fig. 2.6 which depicts a schematic of the layers of RNN arranged in parallel-tiers for learning of vehicular traffic, radio traffic and similarly other parameters. The processing of sensed data for useful features aids to train time-sensitive recurrent artificial neural networks that generate feature-maps with neurons to provide important recommendations for resource allocation and control actions. The AI system integrated for IoT-enabled data network provides autonomous set-up, allocation and management of network resources relevant for achieving IC role.

The CI system is a feedforward deep learning network that accumulates data for predictive control. Infact AI transfers cognitive capabilities to the IoT cellular network [9]. As mentioned somewhere earlier, the channel parameters and signal design required for mobile vehicular traffic can substantially vary in space-time. Often practical cellular solutions for wireless communication reveals that this leads to many hot-spots or holes in terms of QoS and signal coverage in several dense clutters that are busy intersections or portions with dense traffic flow profiles. From a long time, mobile network design has optimized with respect to bandwidth or data-rate and energy variables, however, not much attention has been paid in terms of practically improving coverage. In the past, solutions for extending coverage were in the form of repeaters or boosters that amplify and forward radio signal but the solution also increases interference and energy needs. There exist cellular planning methods such as cell-splitting the physical coverage of areas and sectoring

into smaller nano or pico cells with an umbrella structure of overlaid and underlaid cells. This is claimed to improve throughput with grade of service, provide coverage in dense-user cells and provide energy efficient reuse of resources [9]. However, this has to be managed by a central switch and requires dynamic measurements of complex data and control in the physical cell coverage. Apart from the uncertainties in selecting the channel model, energy and resources; the typical wireless network suffers from losses due to interference, poor directionality from weak control of physical and link layers at most nodes. The IoT network provides an alternate system that overcomes this by providing short hops and hop distances with directed paths from source to destination inside urban limits. The use of dynamic power management can improve QoS in wireless networks but it has other serious concerns such as high radiation power claimed to adversely reflect on short-term and long-term health of humans [3]. In light of this, IoT offers low power solution to extend mobile coverage with mobile co-operative relays and SCUs. The creation of additional logical paths with IoT-enabled end systems utilizes IP suite to share and support from active network resources that enhance the quality of services. As mentioned earlier, vantage point is in the use of AI to perform real-time policing and manage the supply versus demand profile for the network.

We cite some more examples where communication systems tend to fail with high drop rates and poor QoS. An example for this is adverse environmental conditions entailing fog, rain or extreme climatic effects. Other situation which may warrant step-by-step fall-out of regular communication network is location with accrued congestion and high density of vehicular traffic. It may be noted that the problem set for IC relies on the detection of parameters of mobile traffic and related environment. The graphical model with parameters relevant to traffic routes and connectivity can be very effective to train LTSM (Long Term Short Memory) type deep learning network [20] that can retain and forget the state knowledge at various nodes and routes in accordance to its criticality on traffic states [15]. Recommender systems utilizing reinforcement learning can be used to manage traffic light timings, create alternate path or diversions for effective route maps and assist in the co-operative role of IoT-enabled cellular communications network.

2.6.1 IoT Activation and Tagging

The integration of IoT active systems or tags on vehicles can aid in direct mapping and management of traffic. The tag refers to physical device set-up enabling IoT functions on any stationary or mobile application that includes the required processor, peripherals and communication protocols built on OSI stack. The use of tag assists in estimating user or end-system movement along with data, which is crucial in fast and real-time tracking for managing vehicular and radio networks. The tracking of vehicular movement can help driver assistance and rapid learning of traffic scenarios. We also recall that the binary divide used for viewing telecommunication services and mobile users; expected movements and area-wise

data-access needs can also provide vital statistics to the network management plane. Let us consider a case where early motion detection of vehicle and users can impact resources in both vehicular and data traffic. The IoT-enabled vehicle is live port that communicates to and forth through in IoT-network to manage both vehicular network and data network. The learning systems are alerted and convey the vitals of the movement so that data-access and traffic systems can be alerted for quantum of traffic in the present and immediate states. Additionally, drivers can get aid on optimal route and advisory from the external systems via IoT alerts. The built-up of human and machine activated roles entails that the application layer of the stack on user-side must be kept minimal. A minimal user-interface denotes a useful space of web contents that is easy to resolve query when continuously populated from distributed databases typical of IoT system [5]. The front-end or user interface can include search categories populated based on user criteria with secure access for user log-in. Such authentication process can help in human tagging and securing the exchange of information and services to enhance security in select applications. A user login process is also helpful in mapping and learning the pattern of services utilized by users.

Typical issues in processing of real-time updates and managing the databases is use of innovative web ontology for human or machine users for access or control in easy, reliable and secure manner. Whereas OWL (Web Ontology Language) is generally regarded useful in mapping of contents for web-pages using languages like HTML, content based semantic metadata can be used to describe the entities within document. Generic ontologies and hybrid formats are more useful to depict data and relationships that represent knowledge base and related actions. We feel that relational big-databases such as Hive can be used at backend with deep learning principles for efficient knowledge discovery, layering and retrieval.

2.7 IoT and Environment

The role of IoT-enabled ecosystem can cover many domains and here we consider another aspect related to application in measurement and monitoring of natural and man-made environment indicators [7, 11]. Multiple environmental factors can be investigated so that routine impacts and assessment of environmental data can be made on various life forms and of course for humans. This can be estimated using IoT-enabled sensing to evaluate environmental audit and compliances pertaining to routine physical variables such as—temperature, wind-rate, moisture, sunlight, mixture of gases, humidity, rainfall, street-lighting and many others. There can be several other variables pertaining to environmental factors that include variables to be recorded over larger span and rate like—pollution and presence of harmful gases in the environment, detecting or assessing phenomena that may occur for brief and intermittent intervals like earthquake, fire detection system that must function to gather data on minor and major preventive disaster and such other hypothesis that may be crucial to certain areas and specific installations to warranty such

installations. We feel that public safety is an essential factor and IoT systems can be integrated for smart sensing of conditions governing safety in the day-to-day human space. The IoT sensory-panel comprising of various long-term and short-term phenomena is clustered into panels based on logical addresses of panels distributed over the region of influence for sensing and control using data communication which is atypical CI role. In order to simplify, it is suggested that the panels can be networked and located in the vicinity with the SCU or close to access points distributed over IoT cellular network. A set of panels can be marked and served by the same SCUs in direct mode or indirectly with the help of access points which is SCU marked for the explicit purpose of relaying data to the main SCU. The collective data pertains to various devices on IoT panel and identification of data streams in serial data is made using ports and pre-allocated markers of data streams for various physical variables. The bulk data as such can be dumped to SCUs using the IoT drone set-up via routine measurement updates conducted periodically over some intervals as per command sent to the panels from higher level nodes. It is well known that many statutory studies of environment are approximate and done by slow and tedious trials and samples collected physically by humans. In fact, though we have attributed a small portion in this article to environment sensing and monitoring, interestingly the direct and indirect effects of new policies and practices in human society desires the power of IoT-enabled system in the study of long-term and short-term effects. It is therefore not far-off goal when international agencies and forums will make it mandatory for nations to share live-data reports on environmental norms, practices and compliances evidenced by standard real-time sensing and measurement network. The theme of IoT powered sensing of environmental parameters emerges as one-point solution which is not only fast and effective but also of immense help in synthesis of real-time data, mapping evidence from automated learning of states that denote changes in the graphical urban landscape and its distributed impact.

2.8 IoT in Extreme Communication

We consider an extreme use case of IoT based system in a novel role of communication for emergency and disaster situations [3]. Let us consider the physical parameters of environment such as wind velocity, rainfall density, gas precipitation or any accident related and scalable issues that can lead to disaster [1]. The CI functionality of IoT sensory system is relevant for early detection of extreme situations. In such situations we propose the IoT system with available satellite link can offer limited yet useful support for broad-area narrowband and energy limited terrestrial communication. An advantage of IoT system is its open location in elevated areas somewhat distant from radio occluding clutter such as trees, buildings or other tall installations. The energy and resource needs of IoT setup are limited and there is support from renewable supply besides regular power line. The SCUs can operate as mini-base stations to network the communication needs of IoT

devices and end users in vicinity with the novel use of drones in the radio environment. The coverage and access of services may be limited owing to energy constraints rather than bandwidth which is easily available. In this manner the IoT-enabled network can provide an alternate low energy cellular communication for multi-cast and broadcast in times of emergency within reach of vehicular system and also stationary users in close areas.

2.9 IoT Enabled Energy System: Set-up and Performance

Somewhere in prior sections we have introduced classification of services and network resources using a binary divide into static and mobile. This was done for the purpose of effectively mapping the demand side and evolving solution based on twin roles of communicating intelligence and intelligent communication in theme of IoT. We apply similar principles of classification to energy distribution networks. The advent of smart grid [3] has led to integration of energy monitoring with smart roles like managing user access, policing rights to services and data on demand in the power line network. Smart grid is another Intelligent system which incorporates algorithms and hardware to bring fairness and accountability between service providers and end-users, in this case for energy services. We refer Fig. 2.7 that shows a digital divide by classifying the energy transmission-distribution system into two components—(i) conventional smart grid which comprises of the power line network and measurement of active utilization and energy activity in the distribution network at various nodes or junctions with the aid of IoT system, marked as IoT sense, (ii) the natural smart grid has elements that aid in sensing and running renewable sources in

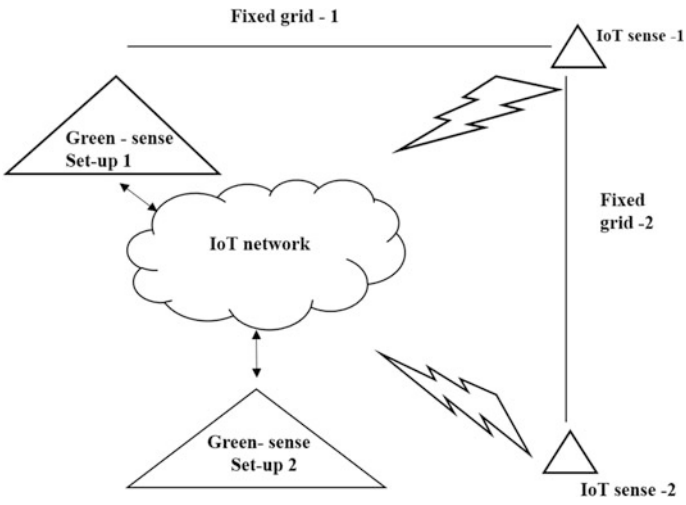


Fig. 2.7 IoT enabled energy system of smart power-line and green-grid

environment. With the help of green-sense units, IoT solution can monitor and act with data to build real-time physical environment of green energy like—solar, wind, vibration, thermal and other renewable energy. Based on forecasts [3] it has become necessary to establish green grid and to develop such capabilities in the urban planning and infrastructure specific to creating sustainable and renewable energy resources to meet mobile needs of small to medium energy loads [21].

The reason for increased interest in this form of energy is based on the inequity of demand w.r.t supply of energy, depletion of natural sources like coal, increase in the energy demands and, largely also due to mobility and adhoc needs of energy for various smart applications that make use of mobile electronics and active systems in establishing and maintaining IoT ecosystem. As seen in Fig. 2.7 the set-ups for green energy are identified using IoT network which also provides data on the generation and maintenance of green energy systems for commercial usage. The feature of energy harvesting with IoT can create a green energy grid for loads such as street lights, traffic lights and other types of mobile adhoc loads. Moreover, load balancing and learning based on feedback of live databases can be integrated to power AI for the IoT-energy ecosystem. Energy audit is vital in terms of learning profiles related to access and consumption of heavy loads such as Industry and other dense urban load units. Here again IoT network can actively provide micro-level and macro-level map for fixed and green energy grids, thereby realizing a more effective form of universal smart energy grid with fairness and ubiquitous connect.

As mentioned here, IoT ecosystem has continuous energy needs that are integral to reliable and successful operation of services in the system. The energy generation by renewable sources and energy demands from load side are both stochastic. The performance of IoT ecosystem is governed by its role as machine data network both in the case of CI (sensing and control) and IC (enhancing the communication suite) roles. We therefore feel it is vital to discuss performance models related to energy capacity with relevance to communication needs of IoT powered nodes. The ensuing discussion engages discussion on communication and energy models for signals that are stochastic in nature. This mainly covers the qualitative relationships in the green-energy generation and utilization to support IoT-enabled system. New generation IoT systems comprise of computationally complex processes that place significant demands on energy efficiency of various sub-systems and mobile nodes. A limited battery-life and charging facility proves to be challenging with growing demand of energy intensive computational loads like sensor networks, laptops, mobile phones. A potential solution to reduce this dependence is by adopting Energy Harvesting (EH) system that employs multiple transducers for diverse green or renewable energy sources available in the environment in order to meet the increasing demands of electrical load [22].

A deterministic parameter like conversion efficiency and sensitivity reflect transducer's ability to convert input energy into useful electrical output. As an example, efficiency of transducer system is typically given by the output power per unit of the input power times effective area and physical characteristics of the transducer [22]. Such indices are not fully reliable in selecting sensor for dynamic applications with stochastic input-output. The issue here is that systems like EH

operate with random energy signatures at the input side and output load, so deterministic performance indices like those cited earlier may not be effective or relevant to describe the energy supply—IoT load system. There has been increase in the use of EH for IoT applications [7, 8, 11].

Authors in [23] have depicted circuit and system elements for EH using heat from battery. Authors [24] have shown throughput-based schemes to improve EH ability of node so that it has greater residual energy. Authors in [21] have shown prediction model to statistically forecast EH supply and demand for random sources like wind and solar energy. It has also shown stochastic model to realistically denote the energy variables in EH system. Authors in [25–27] have shown performance index denoted by capacity of EH system. To the best of our knowledge not much prior work has been done on performance models based on the electrical and physical dynamic parameters governing source and load for formulating the capacity index of this energy conversion. Figure 2.8 shows functional schematic for energy harvesting of IoT node that consumes input arrived energy T_k from an infinite buffer to encode its data θ_k that is sent on a noisy communication link given by N_k. The signal recovery is processed at decoder whose quality depends on many losses over the channel including AWGN noise [28]. The ambient energy available at sensor's output is regarded as infinitely available and distributed as piecewise stationary or periodic ergodic process characterized by E_k. The node replenishes energy by an amount Y_k at iteration of time unit k, with available energy at node denoted as E_k stored in an infinite buffer. In order to encode symbol θ_k the node uses energy T_k at iteration 'k' with condition, $T_k \leq E_k$, and the energy update is denoted by, $E_{k+1} = (E_k - T_k) + Y_k$. Harvesting capacity is formulated under causal knowledge of energy arrivals at the encoder or transmitter. They include variations in ambient energy modelled as slow fading with multiplicative random variable. Finally, leakage at battery or storage and energy consumed at sensor node itself is treated as AWGN (additive white Gaussian sequence) denoting noise interference

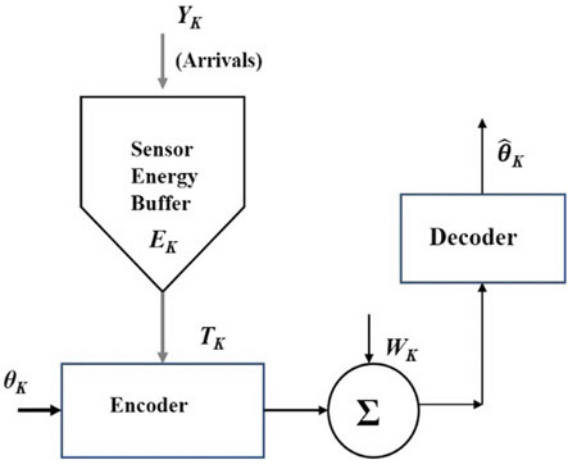


Fig. 2.8 IoT enabled energy generation-utilization model

in the communication channel. This model shows a formulation for communication capacity of transmit sensor node emphasizing energy needed for reliable transmission under arrivals using infinite buffer. The assumption of infinite energy buffer is mostly impractical, moreover, another drawback of this model is that it is limited to the role of capacity of communicating node employing harvesting than the conversion capacity of energy variable for the EH system. We mainly review the physics in the formulation and refer interested readers to [25] for more details and proof. Their work has also considered practical view on status of processor in two actuation modes—wake and sleep modes for driving the closed form expression of capacity. The capacity of queue as formulated in [25] is also used by considering both data and energy arrivals as discrete queues under energy penalties of processing and service times. In [26] authors have formulated energy capacity of single node—single sink system with causal knowledge of energy arrivals at both transmitter and receiver. This work considers the conversion channel as state dependent (memory) channel based on knowledge of energy arrivals. Once the transmitter sends symbol, battery again refreshes its energy depending on energy arrival process thus channel noise is dependent on variations of ambient arrivals conditioned with battery needs. This work shows that achievability of rate is only dependent on current battery level and causal knowledge of energy arrivals. In [27] authors simplify the conditions to give more practical results on capacity of conversion channel for finite battery. The battery energy is fixed and the work considers two operating regimes referred to as higher and lower threshold with respect to battery threshold. The results in these regimes are intuitive—firstly, they show dependence of capacity on the mean of harvesting energy and independent of time-varying harvesting energy in the case if battery is much larger than harvesting energy. Secondly, in the regime when battery need is smaller than maximum harvesting energy then capacity depends both on the stochastic of load and battery. We summarize some weaknesses in prior work formulating conversion capacity of harvesting systems. Firstly, the battery and capacity are considered theoretically infinite in [25–27]. For practical signals and sensors stand-point, this makes no practical use. Secondly, the system model utilized by most prior works mainly delves on harvesting with communication role that covers link and receiver rather than source and sensor or conversion. In the ensuing section we propose an alternate information theoretic formulation based on [25, 27] that gives a practically useful architecture of EH sensory system and a more practically useful conversion capacity based on Shannon theory [29, 30].

Figure 2.9 depicts a simplified view of EH system showing energy arrivals from finite countable set of ambient sources $S_1, S_2, \ldots, S_k$ collected in capacitive sink. The central capacitive storage harvests energy that can be simultaneously drained to supply for the charging of battery unit and cater needs of load unit in the form of computational load akin to most electronic systems involving smart processors, software and intelligent functions with stochastic demand. In the role of learning the environment for energy harvesting and initial planning of green energy network, IoT system is setup for measurement of this adhoc energy with stochastic nature from multiple ambient sources of energy. Let $S(t), L(t), B(t)$ denote the stationary

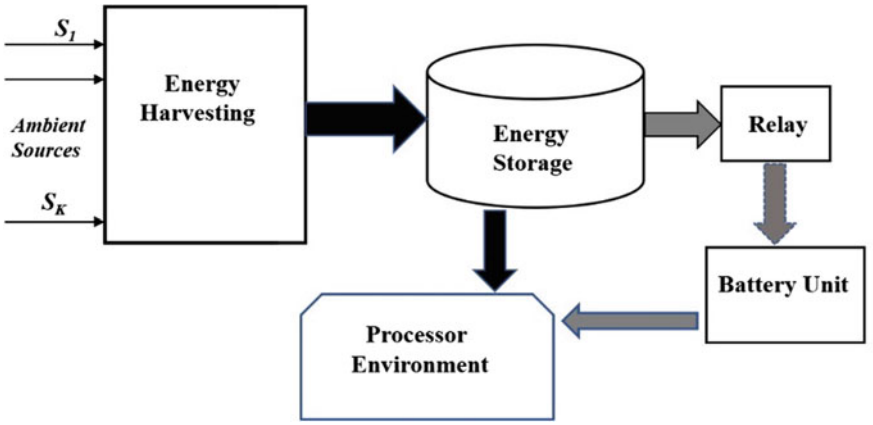


Fig. 2.9 Energy processes and harvesting system at IoT node

stochastic processes for source, load and battery charging. The Fourier transform of their autocorrelation function will denote the energy of these stochastic processes [29–31]. We assume the signals respectively satisfy wide-sense stationarity condition for some time period denoted by τ_s, τ_l, τ_b respectively for source, battery charging and load conditions. The inverse of the stationarity time-periods denotes the stationary spectrum and frequency window which depicts the coherence spectrum of the stochastic processes. This arises in decomposition of power spectrum using frequency domain representation with co-efficients projected in an orthogonal basis. Based on the considerations of supply meets demand an inequality as given below can be used to illustrate the average power flow from supply to load.

$$P_s \geq P_l + P_b \tag{2.5}$$

In terms of energy and rate, substituting power in terms of energy-rate, we can rewrite the above inequality as:

$$E_s.R_s \geq E_l.R_l + E_b.R_b \tag{2.6}$$

The conditions governing transfer of average power, involve both average energy and average rate and note that Eqs. (2.5)–(2.6) are satisfied only if the source can drive load conditions. Given the stochastic nature of demand plane in terms of the rates of charging and load, the source rate or capacity can be formulated as minimum rate given by $\overbrace{R}_s \geq R_s$ for which the Eq. (2.6) is satisfied [30]. It is important to note that empirically stated, the minimum rate is a point for which the energy is minimum on average. Normally when source energy is high then the power spectrum comprises of dominant high frequency terms, simply because both the energy and rate terms are product factors of power signal. Application of the law of conservation of energy-rate for EH system and power flow under stochastic

input-output leads to this basic formulation on energy-rate of source side which on average at least fulfil the sum of energy-rates of the load and battery units. If the energy variable of the source side falls below the total energy of the demand plane then the source rate must be higher to compensate for the low energy such that the Eq. (2.6) is satisfied. Thus energy-rate capacity of the EH system is the minimum source side energy-rate condition on average which satisfies the reliability criteria as follows—

$$Pr(\text{energy} - \text{rate of source} \geq \text{energy} - \text{rate of load}) \leq 1 - \varepsilon; \varepsilon \to 0.$$

Whereas the error event is given by a lower bound on probability—

$$Pr(\text{energy} - \text{rate of source} < \text{energy} - \text{rate of load}) \geq \varepsilon; \varepsilon \geq 0$$

Consider, $Pr(P_s \geq P_l) = \Pr((P_s - P_l) \geq \alpha) \leq E(P_\epsilon)/\alpha$; where P_ϵ denotes the discrepancy between source and load to give a bound simply using Markov inequality [29, 31]. We show a formulation for harvesting capacity by using binary-hypothesis as the flip-flop channels depicted by the binary hypothesis $(P_S \geq P_L)$ and $(P_S < P_L)$ and where X denotes the source side with random variable subscripts S and L denoting source and load side. The former condition leads to no error and latter leads to error event, both events are observed on the side Y denoting receiver side. We are interested in formulating the capacity denoted as C_{EH} based on mutual information between the transmit and receive side variables such that $C_{EH} = \max I(X;Y)$.

We refer Fig. 2.10 to show a unary valued input alphabet split into binary channels denoting the conditions on source and load power. The resultant symbol on receiver side may be correct or erroneous depending on the path traversed. We formulate the mutual information between X and Y as:

$$\begin{aligned} I(X;Y) &\triangleq h(X) - h\left(\frac{X}{Y}\right) \\ &\approx h(X) - [\Pr(P_S \geq P_L).H(1-\varepsilon) + \Pr(P_S < P_L).H(\varepsilon)] \\ C_{EH} &= \max I(X;Y) = \max[h(X)] - [(1-\varepsilon).H(1-\varepsilon) + \varepsilon.H(\varepsilon)] \end{aligned} \tag{2.7}$$

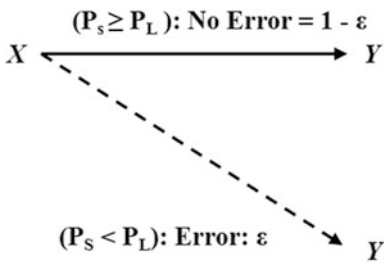


Fig. 2.10 Binary channel for energy harvesting

The source is denoted by differential entropy of Gaussian random variable which arises from application of limit theorem to combination of ambient source signals. The conditions used to formulate a noisy channel are interesting as these can lead to bound the error probability [31]. The use of Gaussian distribution to model source gives the maximum entropy condition to achieve the supremum of mutual information [29] in formulating harvesting capacity C_{EH} as given by Eq. (2.7).

2.9.1 Energy-Efficient Communication in IoT Network

The elements in IoT architecture for communication comprise of SCUs that operate between base station units and IoT end systems. We can view grouping mechanism of the SCUs based on distance, number of hops criteria or coverage map to form SCUs into clusters. The use of energy efficient routing and protocols has been widely known in some of the earlier adhoc networks divided into clusters using protocols denoted by LEACH (Low Energy Adaptive Clustering Hierarchy) [32]. There are many versions of the LEACH protocol, however these mainly use two criteria to optimize the energy utilization for communication of data packets—firstly, it defines sequence of hops for routing based on the energy utilization of intermediate nodes for the duration of activity and secondly, it iteratively reassigns such paths after some time duration based on the residual battery status and proposed activity at various nodes or SCUs as in this case. Interestingly, such protocols can also be used to check the battery status of several devices in the network for advisory and availing alternate forms of green energy. There are some techniques that have shown use of variable flow rate management with lazy scheduling of packets and datagrams [33] to maintain an energy-rate profile that achieves energy efficient communication. Afterall, it is clear that not all data streams comprising intelligence from IoT sensor systems demand high data rate, energy, error-handling or cross-layer functionalities and this can be used to minimize the energy consumption with greedy algorithms [10]. The IoT sensor network can utilize energy from harvesting and in such scenario, energy optimizing algorithms may be required to routinely update residual battery, energy demand along with harvested energy in the iterations. There are techniques for efficient data transfer like prioritizing different flows, storage and management of data queues involving data retrieval and storage. The physical layer can make use of modulation based on time-compressed near ultra-wide band pulse coding such as pulse position modulation [34]. A larger bandwidth naturally provides immunity against both multipath and deep fading thereby improving the signal propagation even with stronger error floor and lower energy per transmitted bit [9]. Measurement updates of real-time channel states assist in choosing adequate value of pulse energy in order to maintain the desired receiver sensitivity and keeping with regulatory policies to control harmful effects of high energy-bandwidth emission. An application of this signaling scheme can be effective during set-up phase, as IoT end systems register themselves with all nearby SCUs. The IoT set-up phase aims to identify and early detect all

new systems that advertise themselves using the on-board processors and basic protocols. These include pilot signals that exchange device identification number which is the electronic key to map the device based on criteria like its features registered priori in IoT system. As request is made to multiple SCUs, final allocation of SCUs is based on signal strength, loading and allocation of SCUs based on service or query stack in the IoT system. After successful round of PACK (positive acknowledgement) for registration request, SCU finally assigns a universal code to identify the IoT end-system for global mobility in the network. This type of local and global address mapping helps optimally utilize the criteria of classifying networks into static and mobile end systems and users.

2.10 Conclusion

In this article we have investigated a data theoretic architecture of IoT-enabled ecosystem with functional roles of measurement, monitoring and controlling of real-time parameters associated with vehicular traffic, data traffic, environment and energy; central to sustainability and utilization for smart resources. The twin roles of intelligent communication and communicating intelligence are shown for IoT ecosystem in various problem domains. The use of IoT active drones as mobile sensing and relay units enhances real-time acquisition, coverage and reliable communication of data both for end-users and network entities in the classes introduced as vehicular and fixed traffic areas. The distributed framework employs divide and conquer approach with IoT for managing issues in dense urban cells, remote areas and hotspots in network. In fact, traffic solution is viewed using graphical model and the solution as such can be generalized to other problem domains. The studies on drone platform suggest that prior training of object classes and channel states must be employed to minimize recognition errors in real-time object and event detection. Infact towards higher order nodes, the interactive features converge web activity driven by various databases, autonomous search directed AI for training SCUs and other IoT end systems. This provides a novel use case to web databases that can be used in evolving a neural-net based web ontology. The IoT sub systems make use of efficient bulk data access protocol towards bulk data access based on UDP/IP in the last mile between SCU and BS. We show cloud databases in vicinity of IoT systems to allow the required Edge computing roles.

Our framework of IoT ecosystem allows effective utilization of network protocols for efficient scalable adhoc systems with global connectivity of several autonomous data connected IoT elements. In energy sensing mode, the network shows hybrid ability to manage renewable energy panel along with the conventional smart power grid. We briefly review and formulate the capacity of an energy limited IoT node that performs energy harvesting. Finally, the article shows important applications supporting IoT limited communication in disaster like situation.

Acknowledgements In writing of the chapter gratitude is due to suggestions of the Editors of this volume. This article treats communication theory at graduate level showcasing bits of logic, architecture and switching methods that can be useful in IoT-enabled solution. Sincere thanks are due to Professor R G. Gallager for unmatched insights and inspirational work in data and communication sciences. Author thanks learning in ecosystems over the years with Communication Sciences Institute USC; GCATT, Georgia Tech. and EE & Statistics, UC Riverside. Author sincerely acknowledges the generous help of Er. Ravindra Prakash Bhatnagar in the preparing of manuscript.

References

1. Sorensen, A., Okata, J. (eds.): Megacities: Urban form, pp. 1–418. Governance and Sustainability, Springer Verlag (2011)
2. Drakakis-Smith, D.: Third world cities: Sustainable urban development, part 3. Basic Needs Hum. Rights, Urban Stud. **34**(5–6), 797–823 (1997)
3. Brennan, E., Lo, F.C., Chamie, J., Uitto, J.I., Fuchs, R.: Mega-city Growth and the Future, pp. 1–392. United Nations University Press, Japan (1996)
4. Goodfellow, I., Bengio, Y., Cournville, A., Bach, F.: Deep learning—adaptive computation and machine learning series. MIT Press, Cambridge, Massachusetts (2017)
5. Guo, K., Lu, Y., Gao, H., Cao, R.: Artificial intelligence-based semantic internet of things in a user-centric smart city. Sensors (Basel) **18**(5), 1341–1355 (2018)
6. Nilsson, N.: The quest for artificial intelligence: a history of ideas and achievements. Cambridge University Press, Massachusetts (2009)
7. Ray, P.P.: A survey on internet of things architectures. Comput. Inf. Sci. J. Sci. Direct **30**(3), 291–319 (2018)
8. Mulay, A.: Sustaining Moore's Law—Uncertainty Leading to Certainty of IoT Revolution. Morgan and Claypool Publishers (2016)
9. Goldsmith, A.: Wireless Communications. Cambridge University Press (2012)
10. Berteskas, D., Gallager, R.G.: Data networks. Pearson Press (1992)
11. Hejazi, H., Rajab, H., Cinkler, T., Lengyel, L.: Survey of platforms for massive IoT. IEEE Proc. in Future of IoT Technologies. Hungary, pp. 1–8 (2018)
12. Pop, M.-D., Proştean, O.: Comparison between smart city approaches in road traffic management. In: Proceeding of 14th International Symposium on Management. Elsevier Procedia of Social Behavioural sciences, vol. 238, pp. 29–36 (2018)
13. Kanungo, A., Sharma, A., Singhla, C.: Smart traffic lights switching and traffic density calculation using video processing. Proc. of IEEE RAECS 1–5 (2014)
14. Bommes, M., Fazekas, A., Volkenhoff, T., Oeser, M.: Video based intelligent transportation systems—state of the art and future development. Elsevier Procedia Transp. Res. **14**, 4495–4504 (2016)
15. Easley, D., Kleinberg, J.: Networks, Crowds, and Markets: Reasoning about a Highly Connected World. Cambridge University Press (2010)
16. Gallager, R.G.: Discrete Stochastic Processes. Springer Science Press (1996)
17. Zhu, P., Wen, L., Bian, X., Ling, H., Hu, Q.: Vision Meets Drones: A Challenge, pp. 104–109. Proc.of IEEE CVPR, Salt lake City (2018)
18. Everingham, M., Eslami, S.M.A., Gool, L.J.V., Williams, C.K.I., Winn, J.M., Zisserman, A.: The pascal visual object classes challenge: a retrospective. Int'l J. Comput. Vis. **111**, 98–136 (2015)
19. Deng, J., Dong, W., Socher, R., Li, L., Li, K., Li, F.: Imagenet: a large-scale hierarchical image database. Proc. of IEEE CVPR, 248–255 (2009)
20. Hochreiter, S., Schmidhuber, J.: Long short-term memory. Neural Comput. **9**(8), 1735–1770 (1997)

21. Cammarano, A., Petrioli, C., Spenza, D.: Online energy harvesting prediction in environmentally powered wireless sensor networks. IEEE Sens. J. **16**(17), 6793–6804 (2016)
22. Hepsbali, A.: A key review of exergetic analysis and assessment of renewable energy sources for a sustainable future. J. Renew. Sustain. Energy Rev. 593–661 (2008)
23. Cesarini, D., Jelicic, C., Kuri, M.: Experimental validation of energy harvesting-system availability improvement through battery heating. IEEE Sens. J. **17**(11), 3497–3506 (2017)
24. Ammar, A.M.A., Fallah, Y.P., Reynolds, D.: Throughput in an energy harvesting wireless uplink. IEEE Sens. J. **6**(18), 2616–2627 (2018)
25. Rajesh, R., Sharma. V., Vishwanath, P.: Information capacity of energy harvesting sensor nodes. Proc. of IEEE ISIT 2363–2367 (2011)
26. Ozel, O., Tutuncuoglu, K., Ulukus, S., Yener, A.: Capacity of the energy harvesting channel with energy arrival information at the receiver. Proc. of IEEE ITW, pp. 332–336 (2014)
27. Shaviv, D., Nguyen, P.-M., Özgür, A.: Capacity of the energy-harvesting channel with a finite battery. IEEE Transac. Inf. Theory **62**(11), 6436–6458 (2016)
28. Shannon, C.E.: A mathematical theory of communication. J. Bell Syst. Tech. **27**, 379–423 (1948)
29. Verdu, S., McLaughlin, S.W. (eds.): Information Theory: 50 years of Discovery. IEEE Press, New Jersey (2000)
30. Cover, T.M., Thomas, J.A.: Elements of Information Theory, Wiley press (2006)
31. Papoulis, A., Pillai, S.U.: Probability, Random Variables, and Stochastic Processes. 4th ed., Tata McGraw-Hill (2008)
32. Brachman, A.: Simulation comparison of LEACH-based routing protocols for wireless sensor networks. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) Computer Networks. Communications in Computer and Information Science, vol. 370. Springer, Berlin, Heidelberg (2013)
33. Uysal-Biyikoglu, E., Prabhakar, B., El Gamal, A.: Energy-efficient packet transmission over a wireless link. IEEE/ACM Trans. Networking **10**, 487–499 (2002)
34. Reed, J.H.: An Introduction to Ultra-Wide Band Communication Systems, Prentice Hall (2005)

Chapter 3
Paradigms for Intelligent IOT Architecture

T. Joshva Devadas and R. Raja Subramanian

Abstract Recent researches in IOT bring out smartness with the basis of machine learning techniques. IOT architecture describes the gateways or fog, an analysis engine and an insight layer. These layers are embedded between the cloud and the edge devices. The insight layer employs various learning modules onto the data in the cloud. The fog layer is the most significant layer that improves the efficiency of IOT architecture. Cloud computing and Fog computing is mutually operated. Fog based application should address the issue of the data to be kept in the fog device and to identify the data present in the nearest fog device with the relevant search query. Learning helps to identify the data that are referred frequently and predict the data requirements of the near future. Agents are introduced in the IOT architecture which reacts intelligently using its learning capability and its characteristics improve the system performance.

Keywords IOT · Cloud computing · Fog computing · Edge computing · Agents · Multi-agents

3.1 Introduction

In the recent computing technological research, Internet of Things gains the momentum in which the devices often handled by everyone, hardware/software/firmware and the sensors are used to build, connect and communicate with the objects/devices for exchanging of data/information/knowledge via networks. To understand the functionalities of IOT, discussion on various IOT architectures were brought in the subsequent sections along with cloud and fog computing architectures.

T. Joshva Devadas (✉) · R. Raja Subramanian (✉)
Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Virudhunagar, India
e-mail: joshvadevadas@gmail.com

R. Raja Subramanian
e-mail: rajasubramanian.r@klu.ac.in

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_3

Comparison of cloud, edge computing with distributed search architecture categorizes its features. Agents are intelligent software programs that are introduced in the IOT architecture to improve the performance of the whole system. Agent characteristics, communication protocols, its basic architectures, Multi-Agent Architecture along with the design principles of Multi-Agent Systems are discussed in this chapter. Agent based IOT, Multi-agent architectures for WSN, Cloud and IOT-Edge computing bring the significance of agent deployment and its roles. This chapter concludes with a case study on Health care application and the benefits of fog layer in smart systems.

3.1.1 Introduction to IOT Architecture

In 1999 Kevin Ashton introduced the term "Internet of Things" which connects the physical objects that exists in the world to the internet through sensors. Human beings are prone to have tiredness and they think of making the machines to work on their behalf. As technology grows, Internet technology paves a platform for the human beings to relax further with the help of Machine-to-Machine Communication that helps the humans to take smart decisions.

Internet Architecture Board (IAB) defines IOT as networking of smart objects. This means that large number of devices communicate intelligently using internet protocols, which cannot be operated directly by the human being but exists as a functional component in the environment. Further, smart objects have constraints in bandwidth, power and accessibility to process among smart objects. Use of internet for IOT lend a hand to connect with the IOT objects to work from anywhere, any time and anything using the four key technology enablers. The four key technology enablers are RFID, Sensors, Nano technology and Smart technology and those are used for Tagging, Sensing, Shrinking and Thinking respectively.

In the recent times, range of technology emerged to a greater extent that the domain of Internet of things includes everything by means of considering stateless to stateful, constrained to unconstrained and from hard real time to soft real time. Architecture is nothing but the framework that narrates on the physical component of the network, its configuration, procedures, and operation principles along with the data formats.

3.1.2 Conceptual Framework

Conceptually IOT was built based on Identifying, Interacting and Communicating with the smart objects. These three are used to interconnect the objects to disseminate the characteristics of Internet of Things at system level. In other words the conceptual framework of the IOT may be derived through the following expression:

$$\text{IOT} = \text{Services} + \text{Data} + \text{Networks} + \text{Sensors}$$

IOT can be viewed in different levels namely system level, service level and users level of the system. These levels are categorized to carry out the dynamic distribution of smart objects present in network systems, the functionalities of integrated Intelligent Objects and to establish end-user communication services respectively.

3.2 Multi Layer IOT Architectures

Many researchers conventionally device, IOT architecture has perception layer, network layer and application layer as depicted in Fig. 3.1. Few researchers identified a layer termed as support layer that comprises of fog computing, intelligent computing and cloud computing. The placement of this support layer ideologically differs with the researchers by placing this support layer either between application and network layer or perception and network layer.

In the IOT conventional architecture, perception layer is kept at the bottom and it is used to recognize objects, collect useful information and transform the information in a digital setup. This layer acts as the brain of conventional IOT architecture by owning the responsibility to secure data transmission between perception and application layer. In many applications this layer collects and forwards the information to the next layer. Perception layer represents the object layer that is intended to collect data from heterogeneous devices, process it and digitized the data. Also, it transfers the processed data to the object abstraction layer for further processing.

Researchers in the domain of communication technologies focus more on communication services in the network layer. The design of this layer aims to provide relevant procedural information, data processing capabilities, assigning

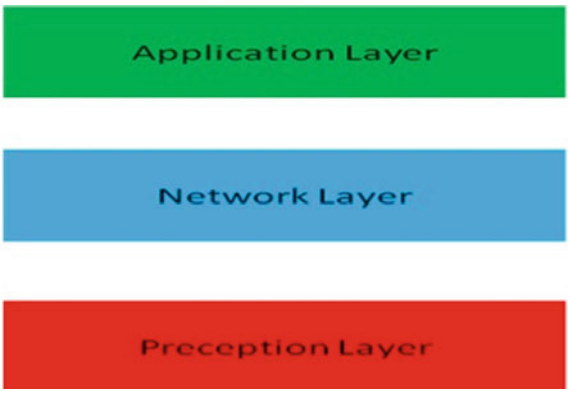


Fig. 3.1 Three-layer IOT architecture

addresses with routing capabilities to the devices present in the system. To provide these communication services contribution of wireless, wired and satellite technologies were deployed effectively.

Network layer or Object Abstraction layer lies between the Service Management Layer and the Object as mediator. Third generation communication technologies, RFID and WIFI are used in object abstraction.

Application layer offer personalized services and its responsibility is to bridge the gap between the user and the application. This layer combines the features and attains higher level intelligent applications such as monitoring health, disaster monitoring, transposition, fortune medical and ecological environment and handles global management relevant to the application.

To offer more functionality, application layer is decomposed into three sub layers namely service management, application and business layer as shown in Fig. 3.2. Service management layer facilitate to process the information, making decision and controlling of pairing requestor. Based on the pre-request received, a Smart high-quality facility is offered by the application layer. Business layer receive data and business model from application layer.

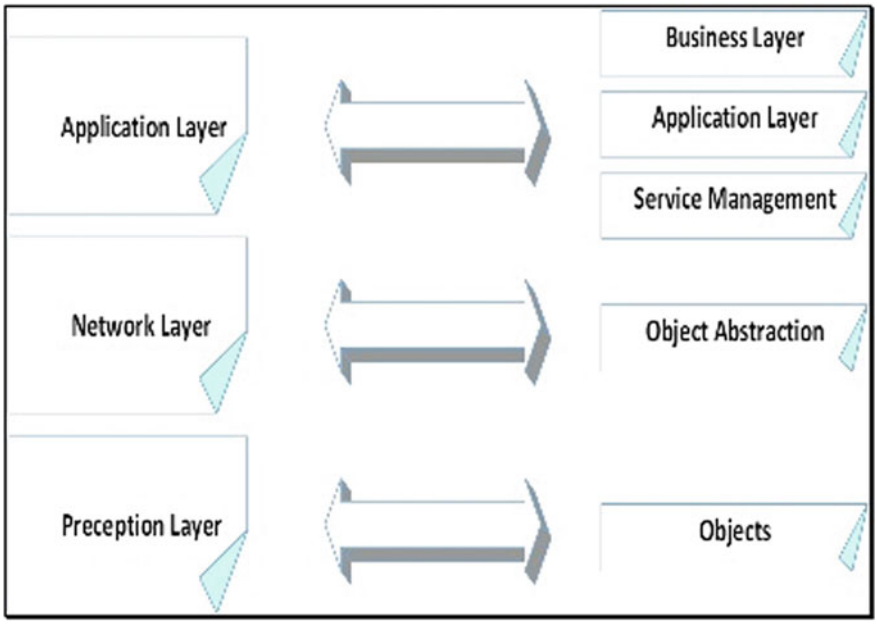


Fig. 3.2 Five layer IOT architecture

3.3 Overview of Various IOT Architectures

Progressive growth in the design of architecture and its framework [1, 2] endorse heterogeneous connection between the devices of IOT and IOT systems. Service Oriented Architecture favors the loosely coupled systems to minimize the integration problem by the use/reuse of IOT Services at the middleware layer. An intelligent framework in API layer is introduced to overcome the deficiencies incurred during the integration of IOT systems and related service routines. Figure 3.3 depicts the basic IOT architecture.

3.3.1 Edge Computing Architecture and System Design

In order to strengthen the network, Beatriz Lorenzo et al. have proposed architecture for dynamic edge network that collects the resources that are unused. To diminish network congestion, Multi-agent based flexible edge computing architecture [3] deal with the "stiffness" issue raised in the design of traditional edge computing architectures. To improve the system performance, Design of Multiple Collaborative Microcontroller for edge computing gateway of Industrial IOT is implemented through distributed collaborative computing. Bowen Du et al., [4] proposed an edge cloud computing architecture to work with edge servers to achieve 'traffic data' as services. To facilitate cloud gaming Yiling Xu et al., developed a transparent gamming cloud system with an objective to reduce the cost effectively by comparing cloud gaming technologies. IOT information retrieval architecture, shown in Fig. 3.4, uses query interface that has components to collect, store and retrieve information from repository. The search intension is precisely understood by decomposing the given query into sub queries and they are matched with appropriate component index for retrieving the data. Based on the data

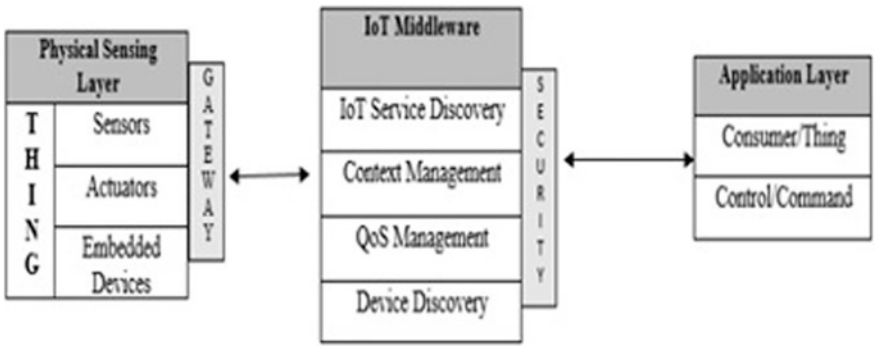


Fig. 3.3 IOT basic architecture

collected, the information may further be categorized as sensor and senor related data. Sensor data includes values generated by sensors and sensor related data corresponds to other observed or training data.

Data is extracted based on four basic query models and for rapid retrieval, these four query models are appropriately designed to associate with four unique indexes namely SID, OID, PROPERTY and OBSERVATION. SID represents sensor identifier and the Data observing and retrieving properties of sensor are carried out by PROPERTY AND OBSERVATON index.

To bring out the realism, the distributed search architecture (Fig. 3.5) proposes Live Data Buffer (LDB) and a resource resolver (RR). The former will collect live data from the entire device and later resolves the data service of an appropriate resource at a particular moment. LDB are nodes of Network that are distributed in wide area network and are responsible for collecting resource live data associated with the same network. When the RR receives a query, a service query in turn queries to the local LDB to ensure resource live data. Depends upon the availability of resource, the resource information is returned through local buffer to the resource resolver. Though these arbitrary searches may deploy several analytical functions in live data buffer it is sufficient to deploy the needy functions in accordance with the query. Query filter introduced in the architecture identifies the data associated with the query. Query translator creates the query filter with an objective of creating multiple search algorithms and distributes a query filter to live data buffer as downloaded application. The search area is minimized with the use of metadata that provides live data buffer and device information.

While gathering the resource, Live Data Buffer pushes or actively pulls the nearest/specific LDB to the resources live data. Data collected about each resource

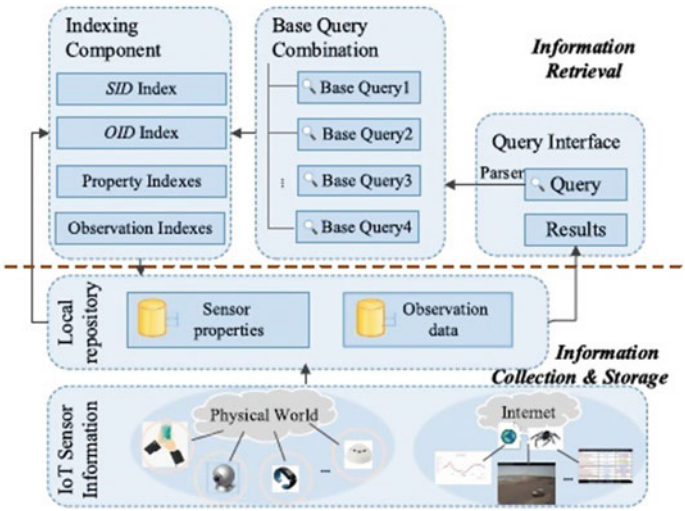


Fig. 3.4 Information retrieval architecture for IOT

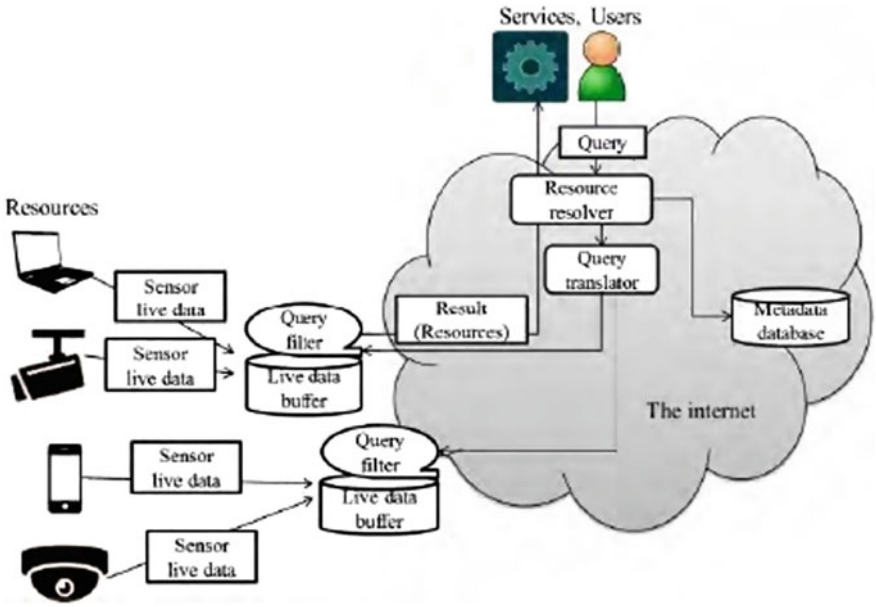


Fig. 3.5 Distributed search architecture

is carried out with a dynamic value 'n' between the time span of t_i and t_{iCn} and discard the expired *t* data. The architecture limits the time window to search live data quickly by making the targeted data smaller as stated in Fig. 3.6. Edge and Fog computing models [5] compute the processing at the edge of the network rather than

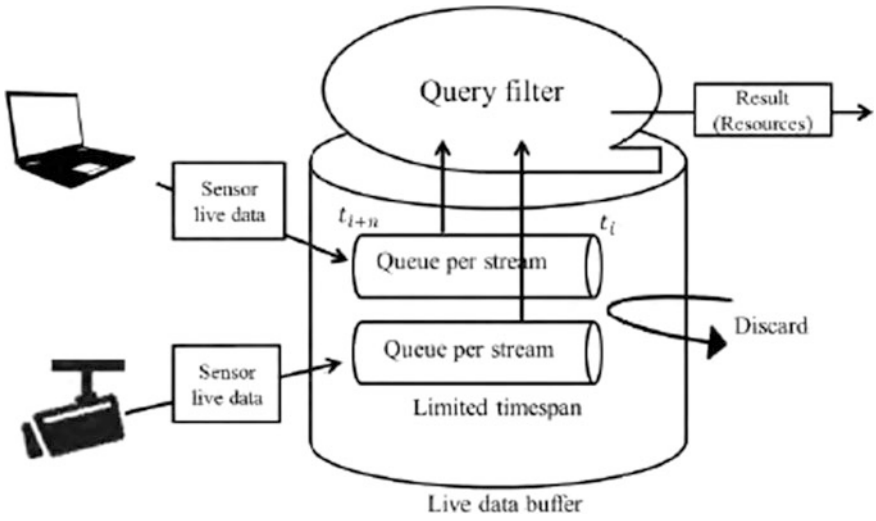


Fig. 3.6 Structure of live data buffer

focusing on cloud. Since these models are adaptable to LDB, employing the edge server in the local network as LDB becomes easier.

3.3.2 Generalized Cloud-Based Architecture

IOT architecture usually composes of five phases: Data capturing, Data preprocessing, Data Analysis, Data Storage and Retrieval, Application. The data capturing activities are taken care by IOT sensors or wearable devices. The sharing of data between the devices are usually through Bluetooth, WiFi, NDF, etc., which serve as a primary connectivity between the devices. The wearable devices sense the data regularly depending on the application and send them to the corresponding devices for processing. The sensing frequencies are fixed and the energy consumption based sources are not used, when the data load is less than the usual. The second preprocessing phase is required to filter the information obtained from the sensor. The data need to be orchestrated to suit the needs of the application in hand. Preprocessing involves elimination of outliers and noises in the data, trimming of low interest data items, etc. Each of the task require a considerable amount of time and processing power, as outlier detection or interest point detections are complex tasks. The crucial of all the phases in the cloud architecture is the analytics phase. A typical IOT application [1] is usually intended to be intelligent. To incorporate the intelligence into the underlying IOT application, the analytical phase, are aptly called as IOT insight layer, should use effectively learn the data. Various learning algorithms play a vital role in analyzing the data. The analyzed data will be provided to the application layer, where it is intended to provide the desired operation required for the user, using the IOT application. The data storage layer, in cloud based architecture, will have many servers and data centers. A resource manager serves as a mediator between the end devices and the servers.

The resource manager keeps track of the schedule, availability and dependency between the resources. Server is composed of many virtual instances or virtual machines (VM). The VM has access to the resources of the server and also encapsulate system configuration settings, memory, processor power and storage capacity. Centralized cloud based architecture is depicted in Fig. 3.7.

3.3.3 Fog-Based Architecture

Fog based computing applications are intended to consist of many networking devices called Fog nodes [6]. These fog nodes can be viewed as a minor replica of the virtual machines (VM) in the server of cloud-based architecture. Hence the fog can perform computation, storage and analytic tasks. These fog nodes, unlike cloud VMs, are not placed closer to data center. They are located close to the edge devices that actually require the computed and analytic data out from the data center. Since

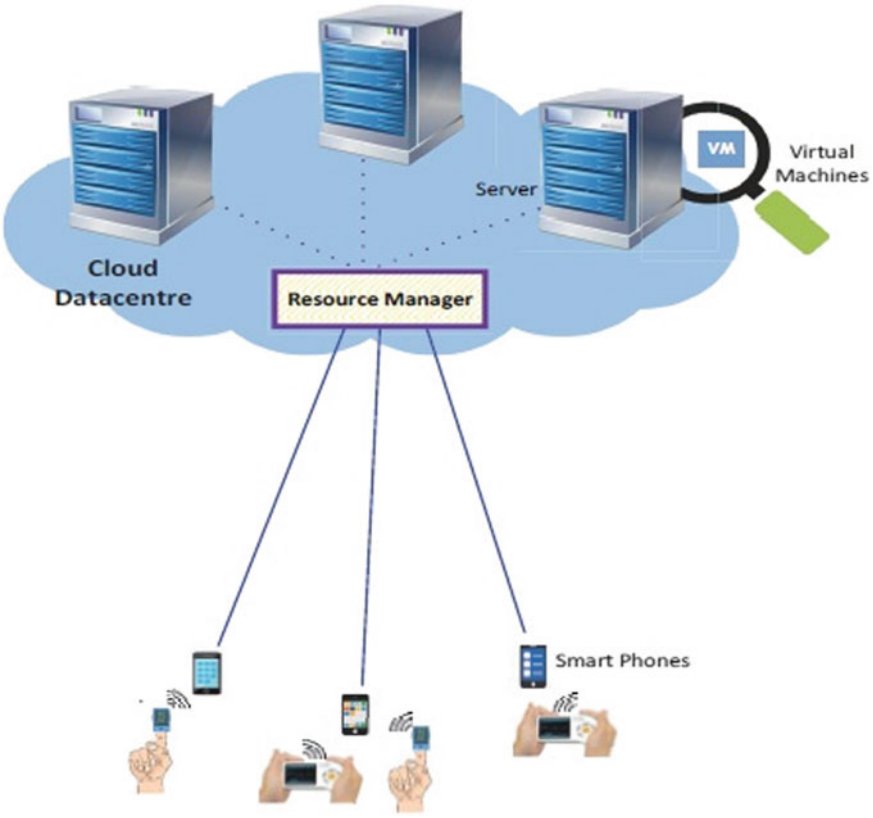


Fig. 3.7 Generalized cloud-based IOT architecture

VMs act as instances of server in cloud architecture, the fog nodes are considered as micro instances of the local compatible server. These micro instances have a memory, processor power and resources required to perform computation in the data obtained from particular or similar edge devices.

In the fog based computing environment, where computation is performed close to the edge devices, the fog nodes are not made active always. They are triggered to perform operation only on demand. That is when the data load is less, the fog nodes can be turned off, thus preserving energy. This is not a case in cloud based computing environment, where the VMs are always available for requests from edge devices. This is required to ensure reliability and availability of the underlying application. With fog based systems, such centralized control can be substituted by a distributed environment. Hence, instead of a central servers, performing all computation and storage, the local gateways or fog nodes close to the edge devices, carry out the computation task.

In this distributed environment, the data obtainable from the edge devices are categorized based on the computation requirements. Fog nodes are set up in

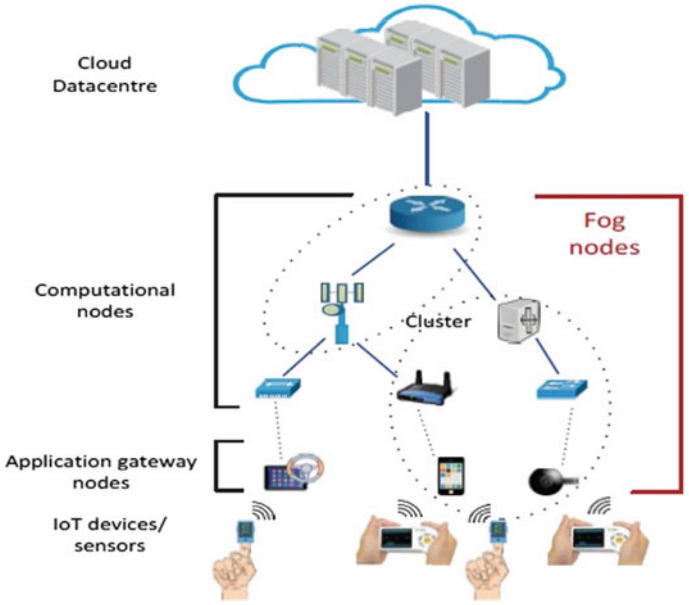


Fig. 3.8 Generalized Fog architecture

sufficient numbers and the fog nodes performing similar or particular computation can be grouped into clusters with required network bandwidth [7, 8]. In each cluster, some fog nodes are intended to perform application level processes and others are nominated to perform database hosting, computations, maintaining communication with other clusters, among others. Each cluster will consist of one fog node acting as a cluster head. The cluster head acts as a resource manager and scheduler. The cluster head equally distributes the computation among its slave nodes. Such parallelization of computation, results in improved response rate. The nodes that are not assigned jobs are turned off by the cluster head, preserving unused energy. If any slave node has disrupted its operation, then its tasks are distributed to other node, in order to maintain normal operation of the application. If the cluster head fails, then another idle node in the cluster, takes its control and configurations. This ensures reliability of the fog based computing environment. The generalized fog architecture for IOT applications is presented in Fig. 3.8.

3.3.4 Distributed Search Architecture Versus Cloud and Edge Computing Features

Distributed Search architecture and Edge computing [5, 9, 10] has lesser traffic in determining the devices and data than cloud computing. Cloud computing and distributed search architecture uses numerous kinds of request than edge

Table 3.1 Comparison of features of various architectures

Features	Cloud computing	Edge computing	Distributed search architecture
Network traffic	Bad	Good	Good
Query variation	Good	Bad	Good
Performance guarantee for multiple processing	Sufficient (has ample computing resources)	Sufficient (can estimate the maximum load)	Difficult (common computers)
Performance guarantee for hardware dependent processing	Sufficient (special computer)	Sufficient (common computer)	Difficult (common computer)
Other concern	Nothing	Nothing	Processing time and network traffic of query filter distribution processing

computing. There are quite a lot of tradeoffs between the features of distributed search architecture with cloud and edge computing, which are presented in Table 3.1.

Instead of using dedicated computers, shared computers are used as live data buffers to support various query filtering process simultaneously. In order to compute the processing load in advance, edge computing estimate its processing load by computing the load through preinstalled applications whereas cloud computing uses shared computing resources from multiple locations to compute the processing load. Distributed search architecture apply resource management tool namely Open Stack to indicate the size of the CPU and memory. Moreover, Open stack linked with CPU pinning function can handle multiple query filter executions will detect and notify when there is no free resource. Distributed search architecture reduce the distribution cost of the query filter by distributing the search request for reducing the total search time and communication traffic.

3.3.5 Fog Versus Cloud Based Architecture

The proposed fog based architecture consists of many advantageous characteristics. The characteristics of fog based architecture compared to cloud based architecture are depicted below:

(i) Fog mode consists of many servers with minimal required power, instead of few servers under direct control of data centers in cloud based architecture. With many servers with specialized functionalities and locality, fog based architecture provides quick response to the requests of the edge devices with minimal processing power. Whereas in cloud based architecture, in order to overwhelm the data transfer time, computation cost is minimized with high

processing power servers, resulting in high usage of energy and cost. Though such configurations are suitable for sensitive applications, fog based architecture can provide better performance with minimal resources, energy and cost.

(ii) Fog based architecture can be configured for a plug and play mode for servers. When a new server need to be added to the application, for improved performance or to provide a new use case in the application, the fog layer provides a provision to enable servers locally, with some configuration settings at the respective gateway or cluster. The similar mode becomes a tedious operation in cloud based architecture, where all the servers are centrally configured. Modifying server settings disrupts the entire model architecture.

(iii) Rather than a centralized orchestration of nodes in cloud based architecture, fog provides a distributed environment among the nodes. Centralized configuration is usually preferred to take care of security, authentication, reliability and storage centrally. Hence these can be handled easily at a central level. Fog, as stated above, makes use of a cluster mode of network to handle secure data transfer and reliability of data and nodes. Through this fog nodes, response time, energy and cost are preserved at a greater rate than with the centralized cloud, where, energy and cost need to be sacrificed in terms of full time active servers with high processing power, or better response time.

(iv) Fog provides a replication of data and configuration for each cluster heads. Hence when a node is failed, the tasks of the node are transferred to a new idle node. When a cluster head fails, a prior replica of the cluster node that is already defined will act as a new cluster. Hence fog based architecture is highly fault tolerant. On the other hand, if a VM or a server fails in cloud based architecture, it results in service disruption. Replication of servers is also possible at a cloud level, but the substantial cost and energy required duplicating a cloud VM or clouding server, than to duplicate a fog MI or fog cluster head.

(v) The communication and data transfer path in fog based architecture is provided with high band width and network capacity. But the path is not fixed; it is dynamic and varies with respect to traffic and cluster availability. Since in cloud based architecture, the centralized server manages all computation and data, the communication to that server is via a static path. In fog based architecture, the edge devices get connected to the fog nodes that are nearer to it. In mobility based applications, the fog node or cluster head are set up at various locations with substantial data and computations required for the application. Hence each time the nearest fog node to the edge device gets a request. All requests and responses are communicated among the nodes of the cluster, in order to maintain consistency. Due to the variable micro instances or fog nodes used by the edge devices, the communication path is always dynamic in fog based architecture.

(vi) The amount of energy used by fog is substantially less when compared to cloud. As fog based architecture turns on its fog nodes only when it is required, unlike cloud server or VMs, that are always active, it consumes less energy. Also fog does not require high end processors to perform computations. Each fog node is intended to perform a normal sub task provided by its cluster head. Hence the configuration of the fog nodes need not be high. Thus performing operations at a lower cost than cloud based architecture.

3.4 IOT Deployment Using Fog

Data plays a vital role in every IOT application. Data need to obtained from edge devices are stored in cloud. It is not all the gathered data reach cloud. With an involvement of suitable analytics engine or native projects algorithm, a normalized data is stored in cloud. But, the storage is still enormous with the Big data applications. Once data is stored, in cloud, several applications can use them to solve related problems. These applications require the data to be transferred from cloud to their environment. Hence data should again be transferred from cloud to the applications, crossing many interfaces. Many state-of-the-art models [1, 8, 11] exist for optimized storage and retrieval of data in cloud. The models lack, when a required data need to be retrieved from cloud after some analytics in a shorter time. Hence, there is an urge to retrieve required data from the wholesome data in cloud at faster rate.

Fog layer can be considered to be an important extension to cloud. It can be operated as a storage and computation medium for local data. Fog makes it possible for applications to access effective data efficiently. In OpenFog deployment model, significant numbers of nodes are structured between the cloud layer and fog layer. These nodes are used to bring the required data close to the computation at the node close to the underlying application. Thus, improve the responsiveness of the application. The major requirements of IOT based applications [6] include: Scalability, Interoperability, and Data quality, Responsiveness, Security, Location-awareness, Mobility and Reliability. Owing to the growth of Big Data and distribution of the connected devices, the computational node will face a higher burden of collecting the required data across these devices. Hence the IOT architecture, rather being focused on the centralized cloud model to organize the growing number of connected devices, requires a fog layer at the lower level. The fog layer can have nodes with different topologies to control the respective devices. Fog nodes can handle nodes widespread geographically, at varying degrees of density. Hence provide better scalability for the underlying IOT application.

Data collected from edge devices or sensors are highly heterogeneous. A typical IOT application will need to collect data from varying sensors, computing devices, storage mediums among others. The data obtained from each source is high dimensional and heterogeneous. The data need to be processed to pose the relation

among them and stored in cloud. Such a processing can be done at fog layer, with suitable fog nodes gathering data from particular sensors. The heterogeneity of the data is resolved with the varying data to handle them accordingly, which in turn are stored in cloud for effective retrieval. Such interoperability between the data providers can be possible with lower level fog nodes.

On top of being heterogenic, the data is also not highly dimensional. Since the data is collected from sensor, it produces multiple data. Of those data retrieved, relevant data for the application's computation need to be identified. The unwanted data can be called as noisy data. Hence there is a need to increase the quality of the data by removing the noises over the data. Data filtering, aggregation, normalization, compression comes into play to provide data quality. It will not be significant to do such operations after storing the data at cloud. Hence fog layer can act as an interface that could manipulate on the data and store only the quality data at cloud.

When quality data is stored in the cloud after being collected from geographically distributed edge devices, the data need to be retrieved back for computation, when the application requires it. The responsiveness of the application highly depends on the efficient computation algorithm. Before computation algorithm operates, it requires the data at its local device. The data transfer from cloud to device should not have much delay. Each time the devices prompt for data, taking it from cloud increases the delay. Hence the required data can be stored in a cloud representative node called fog, which is close to the edge device. Instead of moving computation close to the data in cloud architecture of IOT, fog architecture moves data close to computation. Hence responsiveness of the application increases with fog.

3.5 Ideal IOT Architecture for Smart Applications

It is comprehensive that all QOS parameters can be visualized only by effectively incorporating a fog layer, on top of the edge devices. This fog layer consisting of various fog nodes with minimal computation capacity is intended to process the requests at the gateway. The effectiveness of the fog layer can be improved by fitting the insight layer between the central cloud and the fog layer [12, 13]. The insight layer works out to minimize the hit rate in cloud for the requests from applications, making fog nodes suitable enough to handle the requests. An ideal IOT architecture for smart applications is depicted in Fig. 3.9.

3.5.1 Edge Layer

The edge layer includes various sensors fitted into the environment. Example: temperature sensors, pressure sensors fitted in patient body, as Body Area Networks, injecting sensors in on-board units of vehicles as Vehicular Adhoc

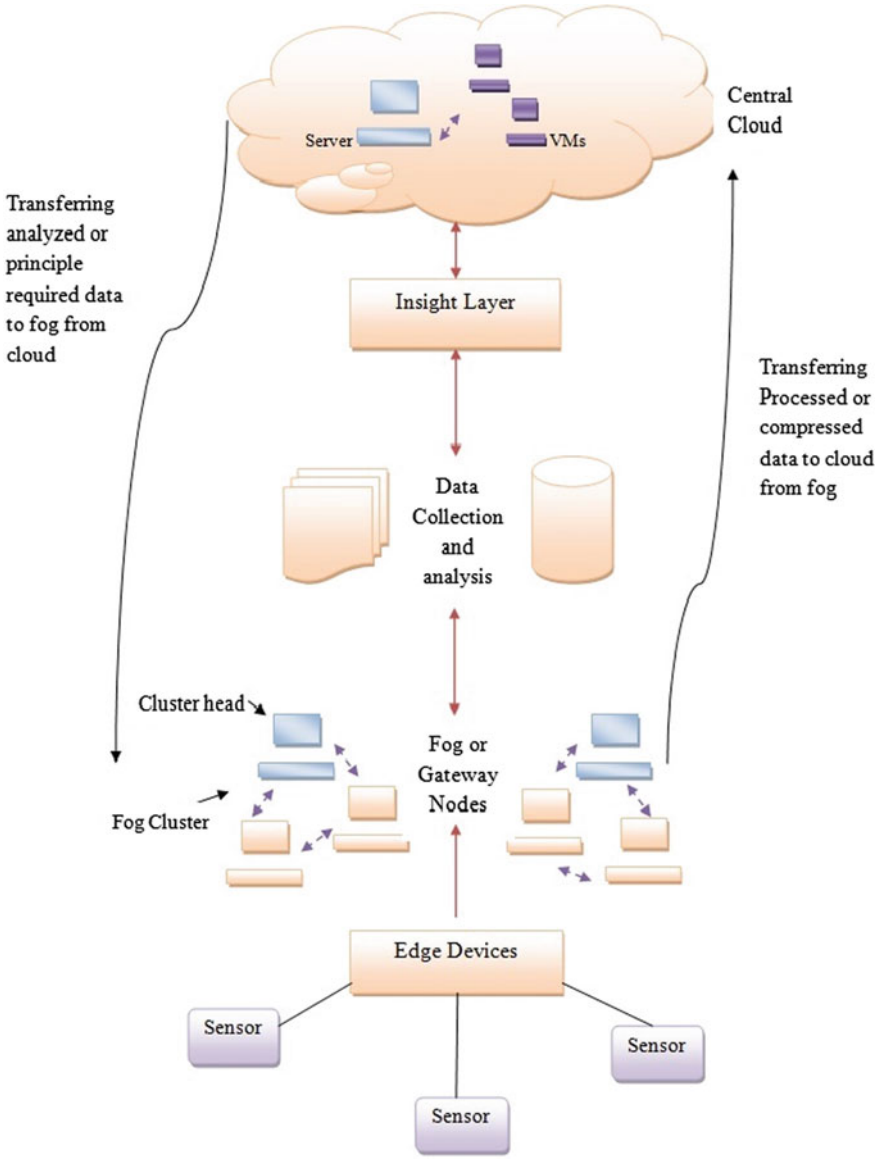


Fig. 3.9 Ideal IOT architecture for smart applications

Networks. The sensed information are gathered and hosted onto the nearest fog node. The sensed information may contain raw data with outliers and noise. The data requires preprocessing with significant analysis. Hence hosting the data

directly onto the cloud leads to excessive use of energy and cost of the underlying system. Hence the data is transferred onto the fog layer to preserve energy, cost and improve response time.

3.5.2 Fog Layer

The sensed data is stored in the fog node. The data is analyzed using the minimal computation power of the nearest fog node. Since, the computation is carried out in the fog node closer to the application and edge device, the application tend to experience better response times at minimal cost, compared to that in cloud architecture. The fog nodes are interconnected with high networking capacity. The reliability, consistency and fault tolerance of the fog nodes are taken care by the cluster head of the fog cluster. The fog cluster consists of group of similar fog nodes, one of which acts as a cluster head. The computed processed data from fog nodes are transferred to the higher layers of the architecture.

3.5.3 Data Collection and Analysis Layer

The processed data from the fog layer is collected and stored in this layer. The analysis engine is usually present in the fog layer itself to perform computations that can occur without the intervention of data and storage of central cloud server or virtual machines. The analysis engine helps in rendering the fog node to be more realistic. It can be modeled to predict the cloud data that would be required to process the future query of the application. Hence those data can be distributed in the fog layer at a lower dimension. Dimensionality of the data can be reduced using techniques like Principle Component Analysis, etc.

3.5.4 Insight Layer

The insight layer is the layer that is required to induce smartness onto the underlying application. The insight layer consists of many learning algorithms that performs many operations such as clustering of similar data, detecting outlier data, finding frequent item sets, finding closest pairs/items, predictions and validations. The insight layer can also use the learning algorithms to improve the security of the application. This can be done by updating the model with the knowledge of various attack patterns experienced by the device under test. It is also possible to render on-demand services to the underlying IOT applications. All learning algorithms require high computation and storage requirements, in order to deal with wholesome data. The error rate of learning algorithms decreases with the increased

training under benchmark and unbiased data sets. In order to efficiently perform such computations at minimal cost, distributed fog architecture can be used instead of a centrally orchestrated cloud environment.

3.5.5 Central Cloud Layer

At the top of the architecture, the central cloud covers the entire application. The cloud is intended to consist of a sophisticated data center, capable of storing huge volume, velocity and veracity of data. The data center is managed with cloud servers and virtual machines or instances of cloud servers. Both the cloud servers and virtual machines are high end systems with maximal computation capacity and storage. Hence they are of high cost and usually hired for cost from various cloud service providers. The cost invested in the huge centralized cloud server can be reduced by reducing the number of instances of cloud server by deploying a distributed fog environment. The fog environment consists of ordinary fog nodes that can perform computations at low cost compared to that of cloud.

3.6 Intelligent Agent Based Computing

Agents are software programs that perform a task on behalf of others using its characteristics. Based on the functionality agents are categorized into Human agent, Hardware Agent and Software Agents. Software agents are further categorized into Information Agent, Cooperation Agent and Intelligent Agent [14]. Agent characteristics determines its functionality such as autonomy, mobility, reactivity, goal-oriented and pro-actively. Autonomy ensures that without receiving commands from the environment the activity towards goals happen autonomously. Mobile agents are capable of wandering from one network to another to reduce network load, communication cost but raises issues in data security, privacy and management. Reactivity of an agent ensures reacting appropriately to influence or information from its environment through agents or human objects. Proactivity/ Goal Orientation ensure that an agent does not react to the changes to its environment but it takes an initiative under specific circumstance. In order to designate as agents, agents must have minimum degree of intelligence by learning or adapting to changes in the environment. Agent learns from the environment to update its knowledgebase by communicating, coordination and collaborating with other agents or others. Knowledge is directly proportional to Agents intelligent behavior. Knowledge grows results with reactive intelligent behavior [15]. Agent updates its knowledge by reacting with the environment applications, data, sensors, actuators and so on.

3.6.1 Agent Communication System

Agents communicate through procedure calls, blackboard systems or extended black board systems to communicate with others through simple dialogues or message passing, or using communication protocols. Procedure calls are the simplest communication method that uses request-reply protocol to establish communication between agents. Agents present in multi-agent system can share the information, data and knowledge through blackboard systems. Blackboards are used to read/access new information as depicted in Fig. 3.10. Since agents are task oriented, they read only the interested information. Moderator introduced in extended black board systems acts as a manager to publicize information on the black board by specifying the agent to which the message was sent. Dispatcher process and eliminate the agent's search when new information is arrived in the blackboard.

In a distributed system, individual agents are considered as a process and all agents present in the system are referred as concurrent process. Inter process communication is established to communicate with each agent present in the system. Agent use the 'broadcasting' mechanism to send and receive messages but the message is read by appropriate agent with the unique address assigned to it. A Dialogue is established to exchange several related messages. The Fig. 3.11 depicts a sample dialogue structure that involves three agents A, B and C.

The Knowledge and Query Manipulation Language (KQML) is developed by University of Maryland during the American Knowledge Sharing Efforts (KSE) Project was widely used protocol for establishing communication in Multi-Agent Systems. Every KQML message has the following basic structure

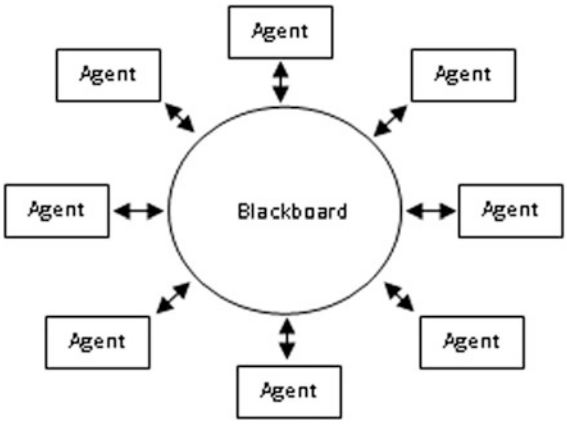


Fig. 3.10 Structure of black board system

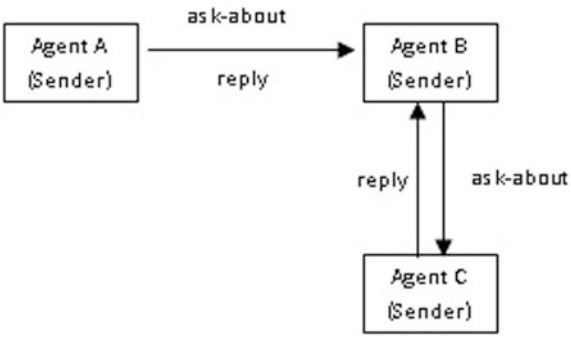


Fig. 3.11 Sample dialogue structure

(<Performative>

: Content <statement/speech act>
: Sender <Name>
: Receiver <Name>
: Language <Text>
: Ontology <Text>).

In KQML, dialogues are modeled to handle complex data structures rather than to handle simple questions/answer process as shown in Fig. 3.12a. Facilitators are introduced to bring together the agents who are fond of searching and providing information. Facilitator accepts the query and attempts to find an agent with the appropriate knowledge. The major difference between Fig. 3.12b and c is that the former uses facilitator as broker to obtain information while the latter uses recommend speech act to obtain the information. Facilitator present in Fig. 3.12c supplies address only to appropriate agent and the knowledge transfer takes place directly between the designated agents and not by the facilitator be the major difference with Fig. 3.12b.

3.6.2 Agent Architecture

This section presents the architectural components of intelligent agent and its various forms. Black Box system depicted in Fig. 3.13 with the minimum layer is considered as the basic architecture of agent. As the agent receives a range of inputs, it processes the input and produce initiated actions as output of the system. Since, the black box provides very minimal information; development of work process of an agent (as shown in Fig. 3.14) is used as basis for the development of concrete, task-specific modules and components. Interaction modules are used to establish communication and cooperation with the environment.

Agent uses interaction component as an interface to receive input from environment and initiate its own action. Information fusion component collect, integrate

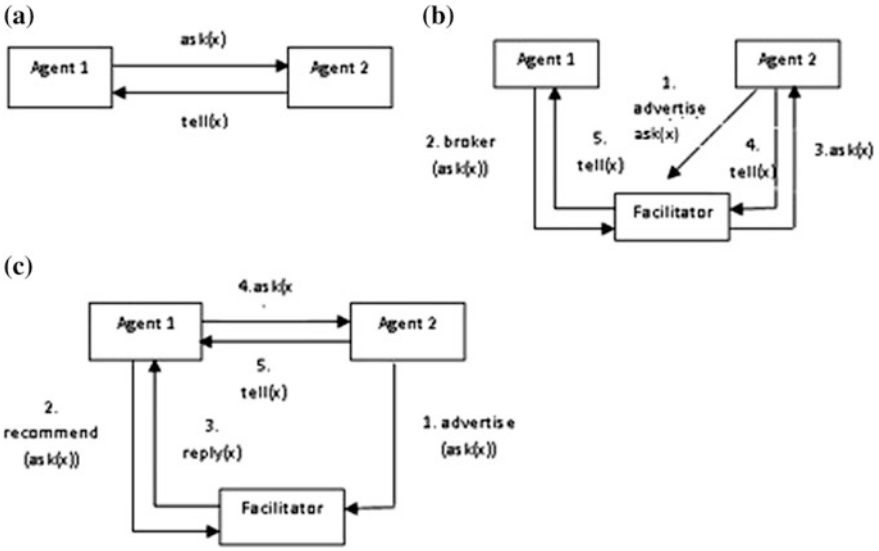


Fig. 3.12 Usages of facilitator and communication variant in KQML

Fig. 3.13 Agent as black box

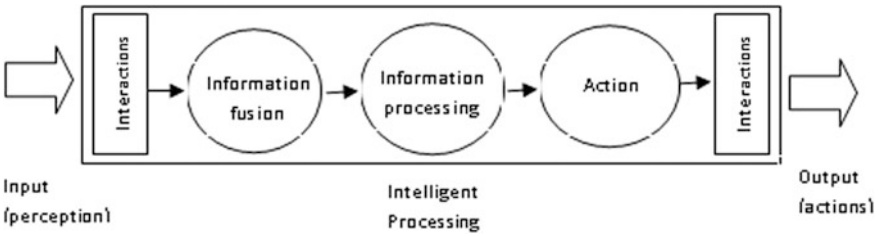


Fig. 3.14 Work process of intelligent agent

and store the information in the knowledgebase. Information component interpret the information to form specific plan to perform an action or reaction. Agent performs those actions that are considered as appropriate by the action module.

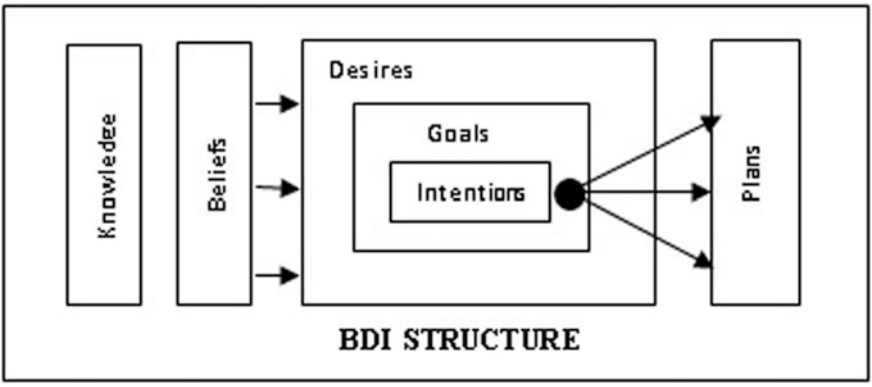


Fig. 3.15 BDI architecture

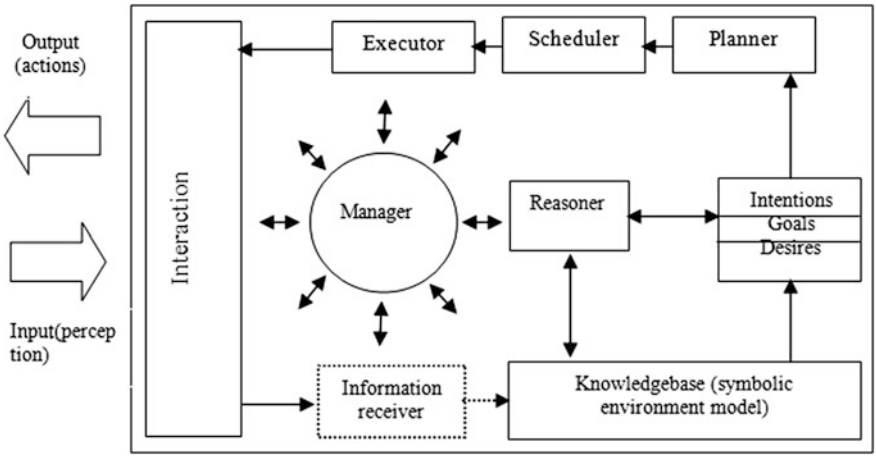


Fig. 3.16 Architecture of deliberative agent

Deliberative agents [3] involved in the decision making process make use its knowledgebase to modify its internal state or mental state which is composed of the basic components Belief, Desire and Goals are often referred as BDI (Belief, Desire, Intention) Agents (Fig. 3.15). Beliefs are the views, Desires are derived directly from the beliefs, Goals are the agent's desire and the Goals become an intention. The result of BDI model fulfils the requirements of architectural design of deliberative agent with Planner, Scheduler and Executor (Fig. 3.16). Planner combines the intensions into overall plans, scheduler receives the current plan from the planner and determines specific action to be made available for execution. Executer executes next outstanding action or terminates an action if it requires more time than the scheduled one.

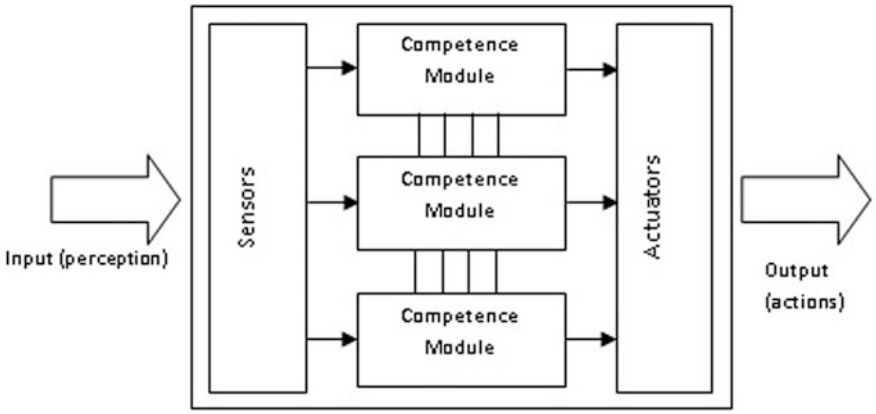


Fig. 3.17 Architecture of reactive agents

Reactive agents works based on stimulus/response basis by continuously monitoring the environment and initiate appropriate reaction. Sensors and actuators are used to forward task-specific information to competence modules and receive the reactions of the competence module (Fig. 3.17). Reactive agents normally do not possess any capabilities to create plans.

3.6.3 Multi-agent Systems

Agents introduced in the computing technologies manifest a new paradigm in addressing the common problems raised in several domains. Researchers of Artificial Intelligence introduce intelligent agents to solve complex issues using a group of software agents called Multi-Agent Systems (MAS) [3]. These multi-agents are capable working with each other by sharing the common resource to achieve the goals by interacting and communicating by exchanging messages. Multi-Agent System resolves the issues and provide solutions in situations where expertise is distributed. Performance of MAS is thus increased with concurrent computation of multi-agents present in the system. Cooperative processing among the agents is engaged when an agent has no knowledge to carry out a task; it may seek the advice of other agent or designate the task to others to complete the task. The major challenge in addressing the design of MAS relies in defining the language and protocol used for communication between agents, describing the behavior of each agent in making decisions and taking actions and recognizing, reconciling of disparate view points and conflicting intension among agents.

Since agents are task oriented, need of multi-agent systems to become mandatory to communicate and share the common resource in centralized systems to work better. Deploying multi-agent system will enhance the various dimensions of

performance such as increasing computational efficiency, reliability, extensibility, robustness, maintainability, responsiveness, flexibility and reusability. Increase in number of agents raises in addressing the challenges in defining, describing, decomposing and allocating the responsibilities among the available agents. Moreover to interact and communicate with other agents defining a language and respective protocols gains the focus in the design process. Describing the agent behavior in making decision, taking actions and formulating the coordination, state of the coordination, process associated with action, plans and knowledge are considered as some of the important issues. Recognizing and reconciling of disparate viewpoints and conflicting intention among a collection of agents which are trying to coordinate in their action.

3.6.4 Design Principles of MAS

In MAS, agents are distributed and connected via links and their dependencies are increased as number of agents present in the system increases. To establish a link between agents the concept of components and connectors introduced in the software architecture are used to reduce the structural dependencies between the agents this leads to the following principles of architecture-centric design.

Multi-agent Structure consists of agents having roles of components and connectors

In Multi-Agent system, a set of independent agents functioning autonomously with identical roles are identified in the design phase of MAS. Considering an agent as an abstract agent class and agents can be directly implemented without restructuring the object oriented model. This leads to the second principle of architecture-centric object oriented design.

An agent is a primitive building block in the design of MAS

Reusability is the core strength of object oriented paradigm. Agent uses this construct to inherit the abstract components to design the multi-agent architecture but MAS discourage this mechanism because inheritance brings knowledge component associated with one agent to other agent and this leads to create greater ambiguity among agents. However the behavior pattern and general system structure can be reused from successfully designed architecture. This leads to the third principle architecture-centric object oriented design and is derived to accommodate reuse in the design of MAS.

Architecture-centric design favors pattern-based mechanism over inheritance

The principles discussed above are not enough to design complete MAS and the architecture-centric principle needs to include some other general principles namely model selection, expressing the model at different levels and connecting the models to reality.

3.6.5 *Multi-agent Learning Design Process*

Learning process is classified according to the functionality of the agents present in the system. Learning agent [16] obeys user's likes and dislikes and interacts with the components by exchanging information. Agent improves its performance using the possessed knowledge and the experience in categorizing the information. Agent intelligence is determined by the size of the knowledgebase present in it. Knowledge base and intelligence are directly proportional to each other. Agent makes use of one or more learning algorithm to update its knowledgebase. Learning can be classified into centralized or distributed in Multi-Agent Systems. Learning done by a single agent on its own is referred as centralized or isolated learning. Distributed learning is done by agents as groups by exchanging knowledge or observes the other agents. When learning properties are introduced in Multi-Agent system, incorporation of skill management and the policy related acquisition arises more issues. Agents present in Multi-Agent system are capable of learning by themselves; it is feasible to allow every agent to use the computational resources at the same time in the learning process. Machine learning techniques and its related tools are used to establish the learning activity. Many agent based applications use machine learning techniques to recognize, classify and categorize the given information. To design learning system machine learning chooses the training experience, a target function and an algorithm for learning target function from training examples.

3.7 Agents and IOT

IOT establish communication by connecting things with other things for exchanging of information/data via Sensors, Network, Wireless Sensor Network, Internet, etc., Sensors play significant role in transmitting and receiving data in a WSN. A node in WSN is more active leads to shorter lifetime. Hence, making a WSN node to put to sleep as much as possible is a way to increasing its lifetime but the node that is asleep cannot receive sensory data. There are few more issues in WSN need to be addressed are: delay between the time the values are sensed and the time the base station receives them, commands issued from the base station to outlying node could potentially take an unacceptable amount of time to reach their target and power consumption of the multiple hops when relaying the sensed values back to be base station for processing. To overcome these issues it is evident that WSN could benefit a great deal from the distributed, intelligent decision making process offered by the agents.

3.7.1 Agent Based IOT

Agents are introduced and added to a product act as linking pin to the internet. The device becomes smart with the addition of agents and is termed as Internet of Smart Things (IoST). Agents are introduced in a product during the design and manufacturing process is capable of guiding a product along with the production cells and collect manufacturing data. Finally the agent will embed itself in the product hardware. Agents incorporated can monitor the sensors and collect information such as temperature, pressure, shock etc.

Agents are deployed in IOT are capable of performing knowledge management and Discovery process to create, modify, update and retrieve the knowledge for making decisions from knowledgebase or other objects. In WSN agents uses its adaptability and mobility characteristics to route the queries and carry/deliver data in networks. The Mobile Agent (MA) is a special kind of software which visits the network either periodically or on demand and performs data processing autonomously while migrating from node to node. Mobile agents are self-contained and identifiable pieces of code that can be executed independently, and presenting mobility in distributed computational devices. In a WSN scenario mobile agents can offer a suitable implementation method in terms of Intelligence, less bandwidth, Cooperative, Autonomy, Mobility and Low power. Mobile agents are deployed in the real time applications such as Traffic flow management, Volcano monitoring, Climate Data Management systems and Target Tracking Sensor Network data management in mobile Ad hoc Network.

3.7.2 Multi-agent Architecture for WSN

The architecture of a single agent results in carrying out the deploying of Individual agent's responsibilities at micro-level. Individual agents may use reactive, deliberative, collaborative or distributed and Hybrid architecture to respond external stimuli, use symbolic knowledge, cooperate to solve problems respectively. A multi-agent architecture is a framework that describes the relationship between the agents present in the system, to exchange information and distribute its capabilities to solve problems in a collaborative manner. Architectures are categorized into Hierarchical, Flat, Subsumption and Modular. Hierarchical architecture is used to retrieve the knowledge of local database. In Flat Architecture any agent may contact another agent arbitrarily. Subsumption Architecture is completely controlled by the containing agents and Modular architecture sub divide the modules into Multi-Agent Systems.

The Multi-Agent Architecture for WSN, shown in Fig. 3.18, has Interface Agent, Regional Agent, Cluster Agent and Query Agent. Interface Agent receives

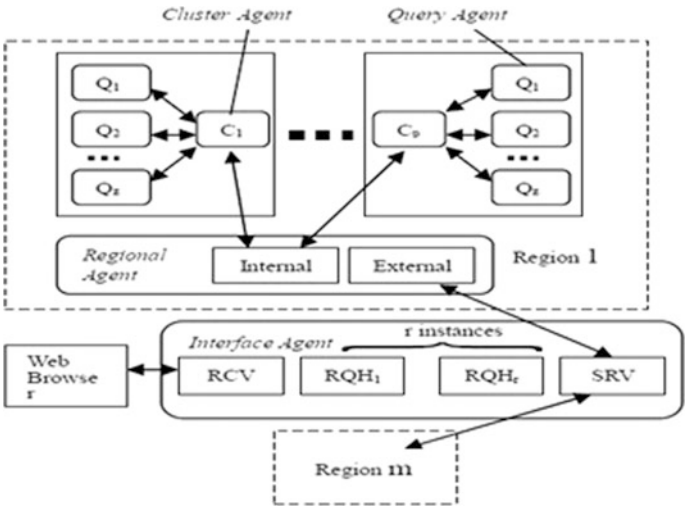


Fig. 3.18 Multi-agent architecture for WSN

the queries from end user and returns back the processed results. Regional Agents send the query packets to the cluster agents and in turn they broadcast the query into the network for processing. Finally Query Agents process the query in the sensor node.

3.7.3 Agent Based Cloud Computing Architecture

Cloud computing uses computing resources delivered as a service over a network/ Internet. Any parallel and distributed system comprises of a collection of inter-connected virtualized computers that are dynamically provisioned and viewed as one or more unified computing resources that adheres to service-level agreements established through negotiation between the cloud service provider (CSP) and its users. Agent based cloud computing architecture (Fig. 3.19) is formed with a two layer architecture namely cloud server- side and cloud client- side. Agents present in the cloud client side have agents namely Cloud Service Provider Agent (CSPA) and Cloud Data Integrity Backup Agent (CDIBA). CSPA offer security services by creating and sending alarms based on security report and monitoring the activity of a cloud user. CDIBA make use of SQL for backup. Agent-based cloud computing mainly focuses on the design and development of software agents for bolstering cloud services.

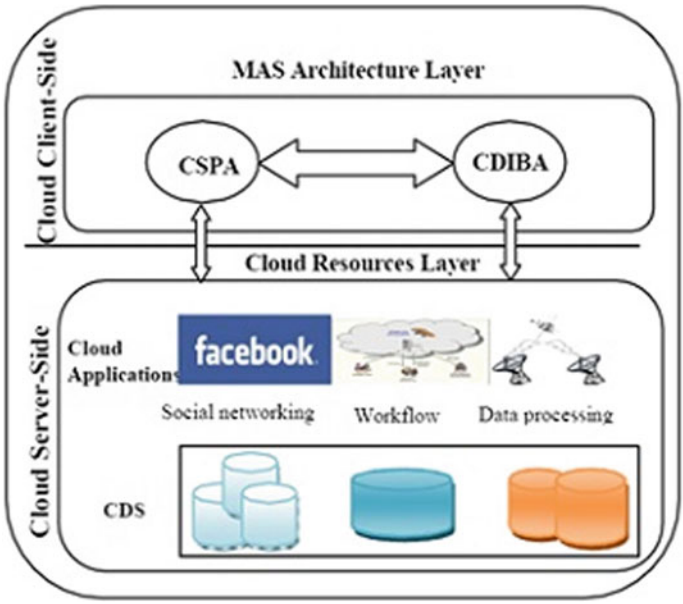


Fig. 3.19 Agent based cloud computing architecture

3.7.4 Multi-agent Based Architecture for Flexible IOT-Edge Computing

In a MAS, Agents are deployed in an application can be sub divided into number of sub tasks and are assign to cloud or edges or unique agent to perform the assigned responsibility. IOT based application can be sub divided into number of tasks that are assigned to cloud or edges. In MAS, the sub divided tasks of an application are autonomously distributed and assigned to unique agent to perform the task. To carry out the responsibility agents can either move from cloud to edges or one edge to another. Such mobility resolves one of the major problems raised during the processing. To determine the behavior of the entire system, the data collected from cloud need to execute the optimization and control functions in cloud. Since the information is dispersed throughout the system it's hard for an agent to control the whole system. Agent's collaborative characteristic is used to assist those agents present in cloud as well as edge for optimizing and balancing their work load. Multi-agent based Architecture of Flexible IOT-EC is depicted in Fig. 3.20 overcomes the challenges of IOT Edge Computing. Agents communicate with different edge agents in its vicinity or cloud may interact with other clouds by establishing collaborative and cooperative process between the edges or clouds.

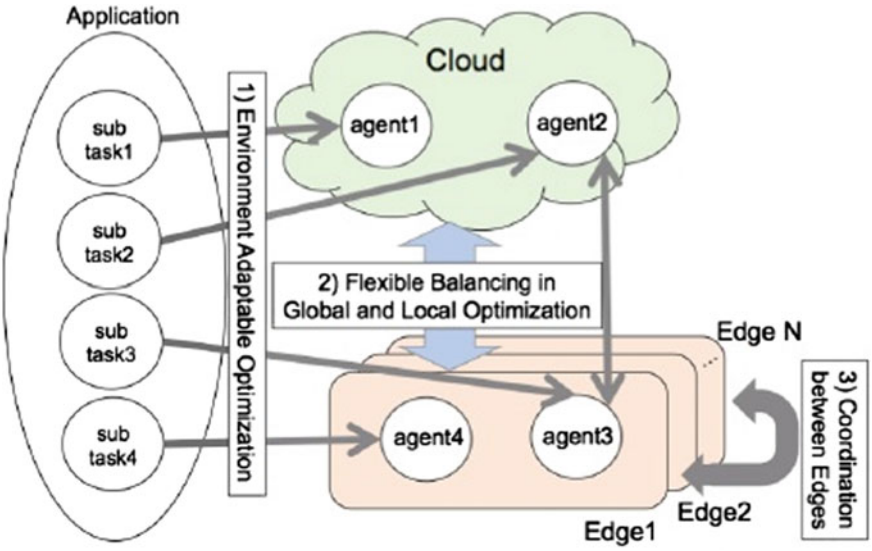


Fig. 3.20 Multi-agent based architecture of flexible IOT-EC

3.8 Cloud-Fog Interoperable Architecture in Healthcare Application—Case Study

In a health care application, data such as symptoms, diagnosis results (sugar, pressure. temperature, among others) are usually benchmarked in cloud for reference [11, 17]. The benchmarked data consist of various analytics incorporated into it, specifying the diseases for various symptoms and diagnostic results. Predictive mechanisms, indulged into the virtual machines of the server, will have many predictions for various combinations of input parameters. The inputs being the underlying symptoms and diagnosis results retrieved out from the patients through sensors. The actuation process for this type of applications need to completed in a rapid sense, as they are very sensitive and time-prone.

As fog is known for its reliable and rapid responses to the underlying applications, a group of fog nodes can be integrated to a cloud VM to make the task efficient. The fog nodes tend to have a minimal processing capability. The primary requirement is to bring the necessary data from cloud on to the fog nodes, based on the application demand. Hence if the required part analyzed data present in the cloud is brought into the fog node, then the fog node that is closer to the application, can perform further analysis and perform the actuation to the application that raised the query. Analysis to be performed in fog node does not require any notable computing powers or storage. This is because the fog is going to deal only with the sensed data obtained from the edge device and the corresponding analyzed benchmark data from cloud. This is essentially not a big data with huge volume or velocity or veracity.

In order to bring the required data alone to the fog, there need to be an insight layer that provides such a service. The insight layer needs to identify the principle data, among the wholesome data, required to analyze the sensed data at the local fog node. One more criterion is the storage of data in cloud. It is not possible for the fog node to store all the collected data in cloud. In typical healthcare applications, ECG data can cover around some gigabytes. Storing the ECG data of all the persons in cloud is a time and energy consuming task. It introduces a considerable delay in the application.

Tailor-made fog architecture for a smart Health care application is depicted in Fig. 3.21. The architecture consists of Data Collection and Data Analysis phase at the top. Bottom of the architecture is the Medical devices and Applications. Between the architecture fog includes various services, security and privacy mechanisms and configurations. The notable advancement in this fog enabled smart health care architecture is the local fog node is enabled with its capability to perform data analysis and provide services. These analysis and services are normally handled by a central cloud server or VM in various state-of-the-art IOT enabled Health care systems. The micro computing interfaces present in the fog nodes try to take some computational load of the cloud VM. Hence the data sensed from the patients either through Wireless Body Area Networks (WBANs) or Wearable Medical Sensors (WMS), is first collected and analyzed at the local fog node. Performing analysis at the fog nodes has various advantages:

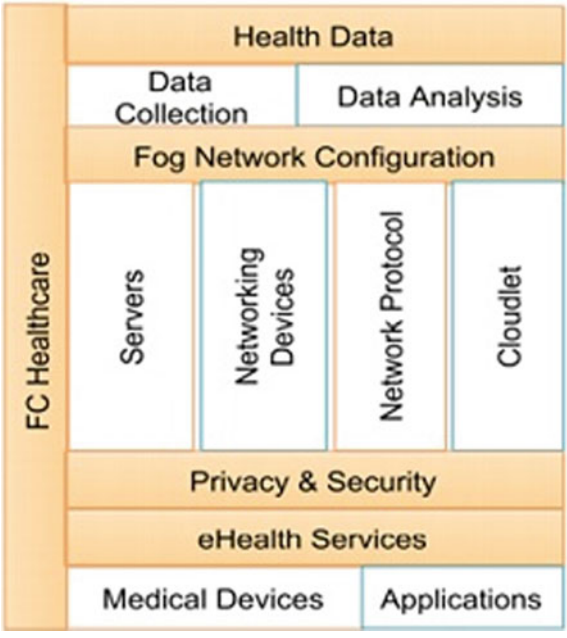


Fig. 3.21 Fog architecture for a smart health care application

(i) The delay generated in sending the data to cloud is subsequently reduced. If the raw sensed data is processed at the fog node itself, having the necessary computational resources, then these data need not be traversed to the cloud. The need for maintaining consistency among the data in each fog nodes can be ensured using various algorithms like gossip based algorithms [18] or genetic algorithms, suitable for communicating the data from each node to the other and finally sending the processed data to cloud. The sensed ECG or temperature data is immediately processed at the fog layer, and the corresponding medical diagnostic report is actuated to the application. The processed data, that is required to improve the learning curve of the analysis engine, is sent to the cloud for storing at the data center.

(ii) Minimal processing power is required at the fog level for analyzing the sensed data. If the same analysis is performed at the cloud server, then enormous computation and storage power is required. This is because, cloud server is directly connected to cloud data center, which consists of maximum storage capacity, depending on the application. This storage capacity is required for enabling the server and VMs to accumulate all the data at a reliable and consistent manner. On the other hand, the fog nodes consist of micro computing interfaces (MCIs), which consist of minimal storage and processing capacity. These MCIs analyses the data obtained from the incorporated sensors, analyses them locally at the fog node and stores only the compact and processed data in the cloud. This can be visualized as a proper divide and conquer strategy, wherein the both the data storage and computation of the cloud is divided into that of the MCIs at the fog layer. The resultant data are stored in the cloud and computed information is actuated towards the application. The former reduces the storage requirements at the cloud and the latter reduces the time taken to resolve the request of the underlying application, hence providing better response time at the application layer. Since health care application usually deals with sensitive requests, responses need to be as better as possible. Hence fog is an essential requirement for smart health care applications.

(iii) Privacy and security parameters are very sensitive in Health care based applications. This is because, patients are very conscious that their medical data need to be secure and not be leaked outside. This privacy constraint is very tedious to get implemented in the centralized cloud architecture. This is because, in cloud architecture, the sensed data from an edge device need to traverse various layers, before being stored at the cloud data center. Hence data leaks or privacy loss is a serious issue. In fog based systems, the data are usually processed at the local node; hence the privacy requirements are satisfied at the local node. Hence reducing the cost of preserving sensitive data. The cost of securing the data is also reduced considerably. The sensed data are encrypted into ciphers, before being transmitted to the cloud layer. In fog based architecture, it is not required to encrypt all the data, only the processed data need to encrypted and sent. The processed data consist of all principle factors, required to visualize the dimensions of the new data.

Storing these principle components in the central cloud datacenter reduces storage and transportation cost.

(iv) The fog network is configured to consist of servers, called fog clusters, networking devices, network protocol and cloudlets. The fog cluster can be visualized as a resource manager in cloud environment. The fog cluster is responsible for load balancing, resource allocation, task scheduling and maintaining consistency of the processed data. The fog nodes and cluster is provided with sophisticated bandwidth to ensure effective network connectivity. Cloudlets are responsible for connecting the fog cluster with the cloud VM. The processed data are transferred between cloud and fog via the cloudlets. The above stated responsibilities of the fog can effectively and efficiently be carried out, than when orchestrated in cloud environment. This is because, at the fog level, the data, computation and task seems to be simple than compared to those at cloud level.

3.8.1 Benefits of Deploying a Fog Layer in Smart Health Care Systems

Fog computing can be useful to work with heterogenic devices and process real-time data without any delay. With the integration of smart gateways/fog nodes, data analytic engine and real time response service at the edge, fog can improve the smartness of various state-of-the-art IOT based health care applications. Extracting features from ECG helps in diagnosing various diseases affecting heart. The PR, QT, RR intervals extracted out from the ECG, along with P wave and pulse train can be effectively used for diagnosis. These signals are extracted and using dynamic time wrapping (DTW) approach. The extraction is done on MIT, Beth Israel Hospital database. The dimensionality of the data is reduced for finding the principle components. DTW is an efficient algorithm for analyzing time series data. The DTW is used to discriminate the different time series data, irrespective of phase differences.

The ECG database is stored onto a fog node. The principle task is to extract the QRS complexes from the ECG data. The QRS represents the vertical depolarization of the ECG. The widening of the QRS duration requires serious notification to the physician. This QRS extraction can effectively be done at the local fog node. Once the complexes are extracted, the ECG files are compressed and stored in cloud data centre for futuristic purposes. Figure 3.22 represents the increase in the percentage of compression with the use of fog computing. The compression helps in processing the ECG files at a rapid rate. More than 90% efficiency of bandwidth with a real time response is obtained with the help of fog computing close to the network.

The typical layout of smart health care application incorporating interoperable cloud-fog architecture is depicted in Fig. 3.23. It can be visualized that fog and cloud are orchestrated in a similar fashion. Both cloud and fog consists of

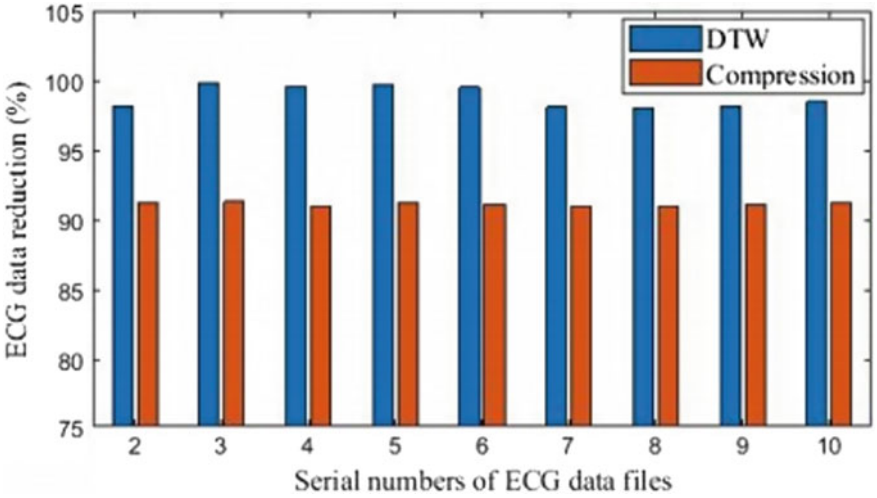


Fig. 3.22 Comparison of ECG data compression using fog computing

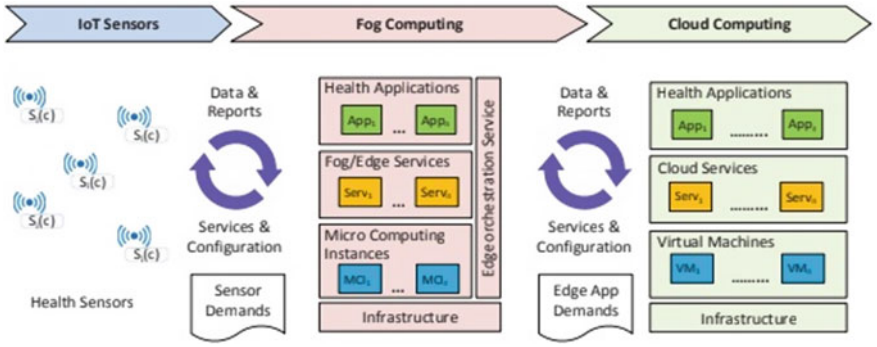


Fig. 3.23 Cloud-fog interoperable iot health care application layout

Application interfaces, services, computing interfaces (MCIs in fog and VMs in fog). This kind of layout signifies the fact that fog tries to represent the cloud in a confined manner with minimal storage and computation requirements. The optimizations used in fog includes: distributed computation of tasks at various fog nodes, storage of processed and compressed data at cloud, maintaining maximum hit rates at the fog, from the application and minimizing the number of data requests from fog to cloud.

Maximization of hit rates at the fog level is possible only when the data requested by the application is available at the fog node. This requires two tasks: the gateway need to predict the pattern of data that will be requested by the application and maintaining consistency of data among the fog nodes through clusters. The

prediction of requests requires learning the parameters from the dataset that are used for previous requests. Using these parameters, dataset can be clustered using various clustering mechanisms like k-means or k-medoids clustering. Hence it is learnt that if a parameters from a cluster is requested from cloud for a particular application request, then the future requests from the application can require the parameters of the corresponding cluster. Hence these parameters are transferred to the local fog to be available for those future requests. Dimensionality reduction techniques such as Principle Component Analysis (PCA) can be applied to the data prior to clustering in order to avoid clustering of data components of less significance. This prevents storage of less significant data at the fog node.

3.9 Conclusion

This chapter begins with the introduction of IOT and Multi-layer architectures for IOT, Edge computing, distributed search architecture, Cloud computing and Fog computing. Comparison of various multi-layer architectures gives a clear idea to distinguish and understand the concept. Moreover an ideal architecture of smart applications helps to understand the functionalities of the layers present in the system. Agents are intelligent systems whose characteristics, communication schemes, protocols, multi-agent system, illustrate the capabilities and performance of agents. The design of multi-agents and learning enumerates the behavior of the agents. The deployment of agents and IOT is illustrated in detail with WSN, cloud and IOT-Edge computing. A case study on Health care system with the interoperable architecture with cloud and fog computing is presented and discussed along with the benefits of deploying fog layer in health care applications.

References

1. Barik, R., Dubey, H., Misra, C., Borthakur, D., Constant, N., Sasane, S., Lenka, R., Mishra, B., Das, H., Mankodiya, K.: Fog assisted cloud computing in era of big data and internet-of-things: systems, architectures and applications. In: Cloud Computing for Optimization: Foundations, Applications, Challenges. Springer, Berlin (2018)
2. Onoriode, U., Gerald, K.: IoT architectural framework: connection and integration framework for iot systems. In: First Workshop on Architectures, Languages and Paradigms for IoT EPTCS, vol. 264, pp. 1–17 (2018)
3. Tadashi, O., Shinji, K., Takuo, S., Norio, S.: A multi-agent based flexible IoT edge computing architecture harmonizing its control with cloud computing. Int. J. Networking Comput. **8**, 218–239 (2018)
4. Bowen, D., Runhe, H., Xie, Z., Jianhua, M., Weifeng, L.: KID model driven things-edge-cloud computing paradigm for traffic data as a service. IEEE Network **32**, 34–41 (2018)
5. Ju, R., Yi, P., Andrzej, G., Beyah, R.A.: Edge computing for the internet of things. IEEE Network 6–7 (2018)

6. Paolo, B., Javier, B., Antonio, C., Sajal, D., Luca, F., Alessandro, Z.: A survey on fog computing for the internet of things. J. Pervasive Mobile Comput. **52**, 71–99 (2019)
7. Deng, R., Lu, R., Lai, C., Luan, T.H., Liang, H.: Optimal workload allocation in fog-cloud computing towards balanced delay and power consumption. IEEE Internet Things J. 1171–1181 (2016)
8. Flavio, B., Rodolfo, M., Jiang, Z., Sateesh, A.: Fog computing and its role in the internet of things. In: ACM MCC, pp. 13–15 (2012)
9. Xu, Z., Hao, C., Yangchao, Z., Zhan, M., Yiling, X., Haojun, H., Hao, Y., Dapeng, O.: improving cloud gaming experience through mobile edge computing. IEEE Wireless Commun. 1–6 (2019)
10. Hirofumi, N., Tatsuya, D., Misao, K., Yoji, Y.: Distributed search architecture for object tracking in the internet of things. IEEE Access **99**, 60152–60159 (2018)
11. Redowan, M., Fernando, L.K., Rajkumar, B.: Cloud-fog interoperability in IoT-enabled healthcare solutions. In: Proceedings of Distributed Computing and Networking Conference, pp. 1–10 (2018)
12. Debanjan, B., Harishchandra, D., Nicholas, C., Leslie, M., Kunal, M.: Smart Fog: Fog computing framework for unsupervised clustering analytics in wearable internet of things. In: 5th IEEE Global Conference on Signal and Information Processing, pp. 472–476 (2017)
13. Lorenzo, B., Garcia-Rois, J., Li, X., Gonzalez-Castano, J., Fang, Y.: A robust dynamic edge network architecture for the internet-of-things. J. IEEE Network 8–15 (2017)
14. Sardinaha, J., Milidiu, R.L., Lucena, C., Paranhos, P.: An object oriented framework for building intelligence and learning properties in software agents. J. Object Technol. **2**, 85–97 (2003)
15. Gerhard, W.: Multi Agent Systems—A Modern Approach to Distributed Artificial Intelligence. The MIT Press, Cambridge (1999)
16. Mitchell, T.M.: Machine Learning. McGrawHill, New York (2018)
17. Mingliu, L., Deshi, L., Gimei, C., Jixuan, Z., Kaitao, M.,, Song, Z.: Sensor Information retrieval from internet of things: representation and indexing. IEEE. Transl. Content Mining IEEE Access 36509–36521 (2018)
18. Herve, B., Pierre, F., Hovhannes, H., Remide, V.: The worst case behavior of randomized gossip protocols. J. Theor. Comput. Sci. **560**, 108–120 (2014)

Part II
IoT Integration with Sensors and Cloud

Chapter 4
Semantics and Clustering Techniques for IoT Sensor Data Analysis: A Comprehensive Survey

Sivadi Balakrishna and M. Thirumaran

Abstract Semantics is used to exchange information from one place to another place in a meaningful way. The data is generated from various heterogeneous devices, communication protocols, and data formats that are enormous in nature. This is a significant problem for Internet of Things (IoT) application developers to make the IoT generated data interoperable. In the existing approaches, there is a lack of well-defined standards and established tools to solve the semantic interoperability problem in IoT smart city applications. Smart cities are much popular these days. Currently, smart city applications are facing a problem with a lack of semantic interoperable standards. At present, there is no unified interoperable methodology to redeploy and reuse the IoT smart data for smart city applications. Having the smart city become interoperable in nature, there is a need to focus on architecture, framework, work progress of IoT smart data, semantic interoperable services and applications, and provide security to smart city applications. In this chapter, firstly, exposes the all-applicable semantic interoperable standards in smart city applications to become a semantic web of things in comprehensive survey manner. Secondly, the unsupervised clustering mechanisms are discussed for performing analysis on IoT sensor data and highlight with much more attention towards the issues, challenges, and current research directions. Finally, this chapter concludes with proposed semantic reasoning mechanism for unified accessible resources in IoT smart city applications.

Keywords Semantics · IoT · Smart city · Clustering · Research directions

S. Balakrishna (✉) · M. Thirumaran
Department of Computer Science and Engineering, Pondicherry Engineering College, Pondicherry, India
e-mail: balakrishna.sivadi@pec.edu

M. Thirumaran
e-mail: thirumaran@pec.edu

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_4

4.1 Introduction

The buzzword IoT is used to connect the things to the internet and is a combination of IoT devices- sensors, actuators, Radio Frequency Identification (RFID) tags, smoothly distributed smart IoT objects having the sensing abilities, actuating capabilities, and embedding with IoT technology. IoT mainly addresses scalability, accessibility, visibility and controllability of the sensing smart objects and things. In the future, physical objects and digital objects have to be embedded and inter-communicated to obtain more domain-specific applications [1–3]. The IoT is concentrating on transforming the real-time objects into sensible smart objects with communicative and controllable environmental physical objects. RFID is the technology used to capturing of objects, people and living and non-living things. Electronic Product Codes (EPC) are embedded RFID tags to be used for tacking IoT smart things. Cloud and Big data technologies are the finest technologies that are useful for storage and performing analysis of IoT data. The IoT has the mid-range list of applications to be supportably suitable for smart city environments. The applications like Environmental monitoring [4], Smart homes [5], Healthcare applications [6], Production and inventory management [7], Supply chain management of food [8], Smart cities [9], Fire station systems [10], Aerial vehicle data [11], VANETS [12], Semantic real-time traffic management [13, 14], Smart home [15, 16], and Industry 4.0 are used under IoT domains.

Clustering is used to find the hidden pattern information and form a group of clusters of the same category in the whole dataset. In this, IoT and Cyber-Physical-Systems (CPS) digital era, a massive amount of sensor data has generated. In order to perform data analysis and integration of IoT sensor data, the semantics and clustering algorithms play a major role. To process and analyze sensor data is a big challenging task. In earlier days, so many traditional algorithms are proposed and implemented for IoT cluster analysis. The traditional clustering algorithms are only dealt with static and spherical data. However, when dealing with huge volume and variety of dynamic data originate from IoT sensor devices is a challenging problem. The traditional clustering approaches are downfalls in two points: (1) it occupies more memory when the large-sized data sets are loaded into the model: (2) if the data is varying irregular and dynamically coming from blogs, tweets, streamed data, online transactions, etc. then that particular point of the time faces a huge overhead and computational time issue.

Therefore, to perform analysis and dealing with dynamic data, in this chapter proposed a new and innovative approach named as CFS (Clustering by Fast Search) using Incremental Clustering.

Figure 4.1 shows the comparison between the connected IoT devices in billions versus the years starting from 2015 to 2025. In this 10 years span of time, the connected devices are a 5-fold increase from 15 to 75 billion devices with 2015–2025 respectively.

The raw data is generating from the IoT devices i.e. the first layer data called as a data acquisition layer. Next, it goes to the processing layer where data is structured

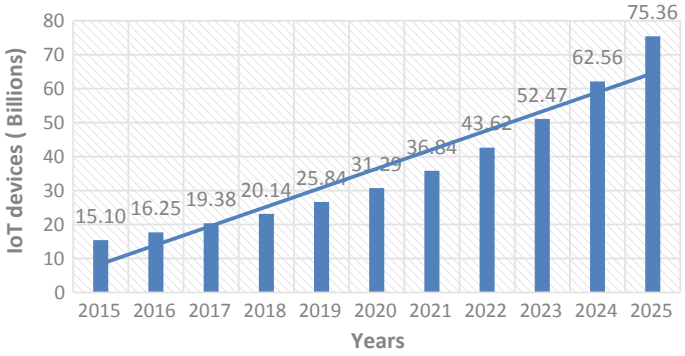


Fig. 4.1 Estimation of IoT connected devices year wise. *Source* statista

data format represented for processing. The perception data is next categorical data contains the cluster, concept, and context for performing analysis. The topmost layer contains the executive data, which performs the predictions and actions to the user. The entire IoT sensor data hierarchy has been depicted in Fig. 4.2.

Machine learning and semantics are solving the problem of IoT sensor data integration and analysis. These approaches may also support integrating, acquiring, unifying the sensors generated smart data. The smart cities are much popular these days. Currently, smart city applications are facing a problem with a lack of semantic interoperable standards [1–3, 13–16] (Balakrishna et al. 2018). At present, there is

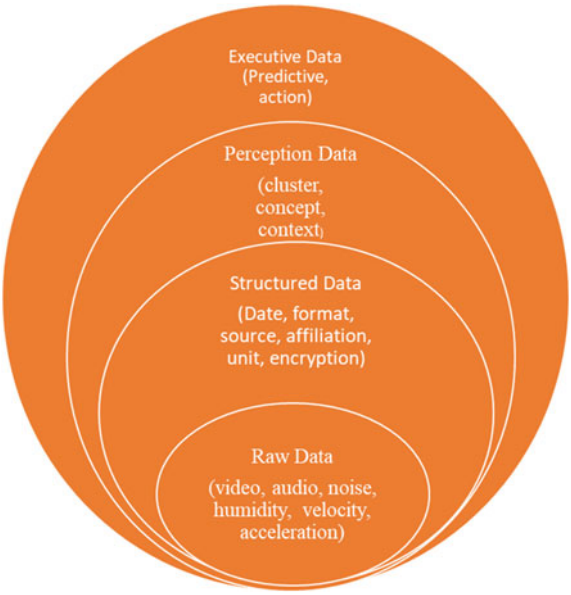


Fig. 4.2 IoT sensor data hierarchy

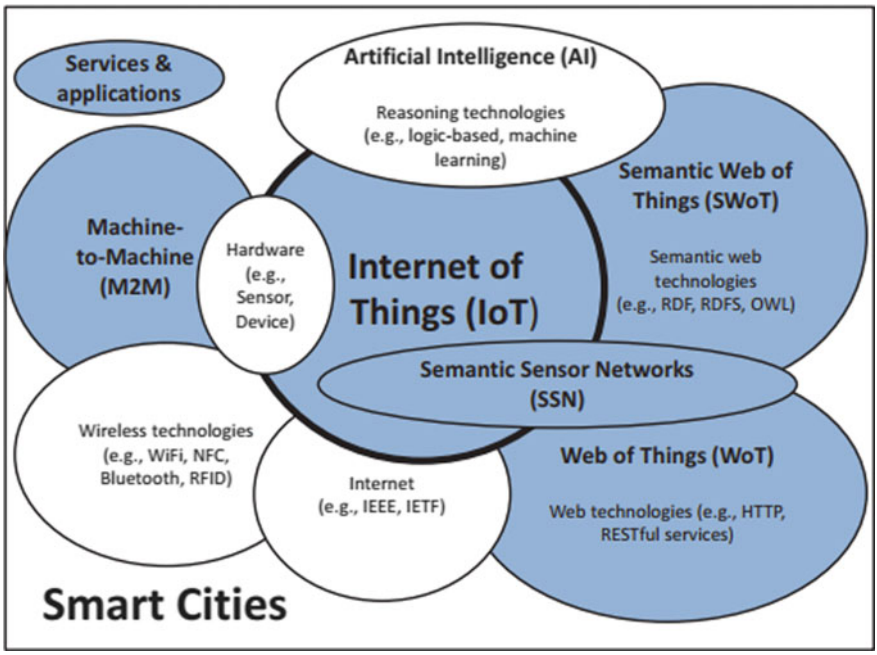


Fig. 4.3 Smart cities with supportable technologies

no unified interoperable methodology available to redeploy and reuse the IoT smart data for smart city applications. Having the smart city become interoperable in nature, there is a need to focus on architecture, framework, work progress of IoT smart data, semantic interoperable services and applications, and provide security to smart city applications [1–3]. Figure 4.3 shows that how the various types of approaches like Artificial Intelligence (AI), SWoT, SSN, WoT, IoT, WT, services and applications, and Machine-to-Machine (M2M) are integrated with each other for building the future smart city applications with semantics and machine learning approaches.

The main contribution of the proposed work is as follows

1. To survey the related semantic approaches for IoT sensor data integration and analysis.
2. To review the unsupervised clustering approaches for IoT data analysis.
3. To expose the challenges faced for IoT data analysis.
4. To highlight the main research directions to achieve the IoT sensor data analysis in smart city applications.

The next coming sections of the proposed chapter is structured as follows: The related work of semantic technologies survey is discussed in Sect. 4.2. Section 4.3 gives an overall survey of semantic technologies for IoT sensor data analysis in detail. The machine learning based unsupervised clustering approaches discussed in

Sect. 4.4. The challenges and current research directions are illustrated in Sect. 4.5. Finally, Sect. 4.6 concludes this chapter and stretch the future enhancements of this work.

4.2 Related Work

In this section, the authors surveyed the recent existing works related to the Internet of Things and semantic technologies. Atzori et al. [17] surveyed on Internet of Things and presented their views on communications, protocols, challenges, and security issues. Zeng et al. [18] surveyed on a semantic web of things and described their intention on sensor discovery and reasoning, ontology matching, frameworks and architectural elements, and security and privacy issues highlighted. Petrolo et al. [19] focused the smart city based cloud things applications and presented a survey related to the existing smart city vision and its paradigms for smart cities. Aggarwal et al. [20] surveyed the data-centric approach on semantic web technologies and Internet web of Things to focused the semantic data, communication protocols data etc. Perera et al. [21] analyzed the context-aware applications are needed to propagate the sensor semantic data for machine-to-machine interactions. Raul Garcia-Castro and Gomez-Perez [22] given a roadmap on data interoperability in smart cities to generate energy-efficient protocols and systems. Ganz et al. [23] discussed the information processing and gathered sensed data on the Internet of Things in a practical evaluation approach. They presented and implemented the semantic annotation problem in IoT-based smart home resources using RESTful URI's. The smart home and lighting concept using semantic technologies.

4.3 Semantic Techniques

In this section, the authors surveyed the semantic techniques for supporting IoT sensor data integration and analysis.

The semantic technologies include Ontologies, RDF, RDF Schema, OWL, SPARQL, semantic annotations, and semantic reasoning to interoperable IoT smart data. It also supports integrating, acquiring, unifying the sensors generated smart sensor data. The smart cities are much popular these days. Currently, smart city applications are facing a problem with a lack of semantic interoperable standards. At present, there is no unified interoperable methodology available to redeploy and reuse the IoT sensor data for smart city applications. Having the sensor data become interoperable in nature, there is a need to focus on architecture, framework, work progress of IoT smart data, semantic interoperable services and applications, and provide security to smart city applications.

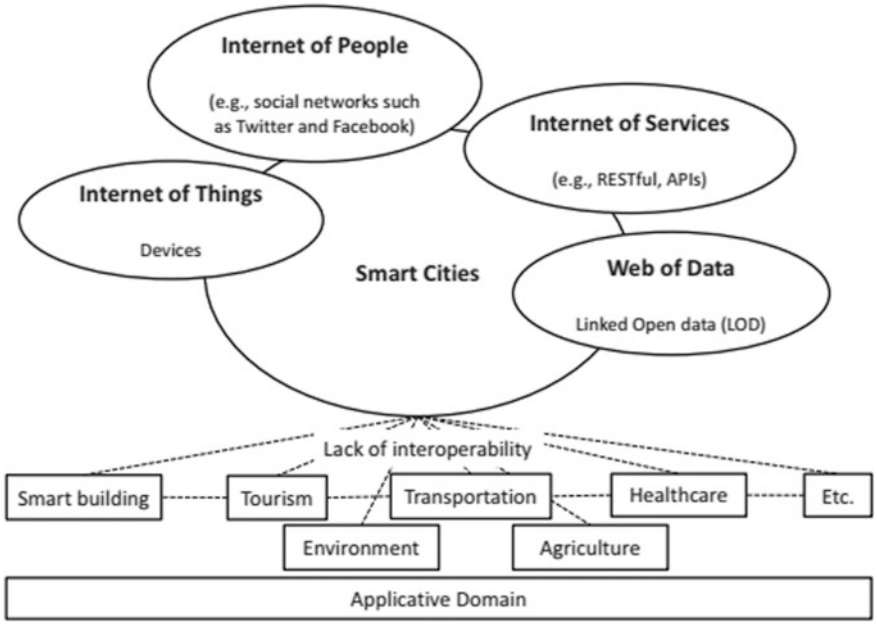


Fig. 4.4 Smart cities applications with lack of semantics

Figure 4.4 shows that the various IoT smart city applications like smart home, smart traffic, healthcare, tourism, environment, etc., are facing the interoperability problem with lack of semantics and machine learning approaches. The smart cities are merged into the integration of IoT, Internet of Services, Web-linked data, and Internet of people to become the more accessible and scalability to the users.

In Fig. 4.5, picture the overview of semantic technologies supported for data analysis and integration in an efficient and meaningful way. These semantic approaches include reasoning with machine learning, reasoning with logic based rules, reasoning wit recommender system, reasoning with SPARQL, and some semantic constraints like SPIN, RIF, and CONSTRUCT, etc. at top-level layer. The subsequent layer shows that the ontologies/vocabulary, knowledge graphs, model to be used for predictions, and finally the lowermost layer deals with a description of the content used in different formats. The most popular supporting formats for semantic approaches to perform analysis in IoT sensor data includes—RDF, RDFa, Turtle, and N-triple. On the right side of Fig. 4.5 showing the security and privacy features like cryptography, authentication etc. needed for semantic approaches in all the layers mentioned.

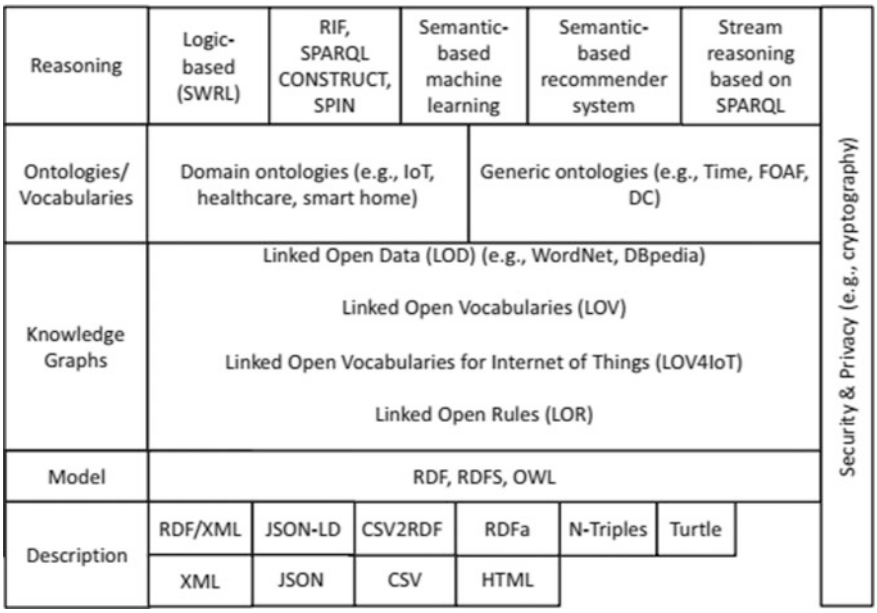


Fig. 4.5 Semantics complete overview

4.3.1 Ontology

Ontology is the core concept in semantic technologies. It is used to describe the single religious community relations and concepts. The relation is applied between any two types of things or services or applications. The concept is representing the type of thing i.e. a person, home, animal, or the state of activity like shopping, listening, and towards work etc. Ontology predominantly contains four forms; those are classes, attributes, objects, and relationships. Classes can describe something related to someone. The classes also describe subclasses called as children are used to propagate the inner information. It has the attributes to represent the information of properties and features. The objects are the instance of the classes. The relations make the things and components associated together. The vocabularies are supported by ontologies to provide meaningful information between the machine-to-machine communications. As per the author concerns, an ontology 'Ontl' be made up of the Co denoted as the central Ontology of the knowledge representation, the term Ax denoted as the axioms, the keyword KnBase denoted as the knowledge base, and the symbol Lx represented as the lexicon and is predominantly categorized by exhausting 4-tuple as shown in Eq. 4.1.

$$\text{Ontl} := (\text{Co}, \text{Ax}, \text{KnBase}, \text{ and Lx}) \tag{4.1}$$

Subsequently, the central ontology Co of the knowledge representation is defined as 5-tuple as shown in Eq. 4.2.

$$\text{Co} := (\text{CLS}, <=\text{CLS}, \text{REL}, \sigma, <=\text{REL}) \tag{4.2}$$

The two central attributes namely CLS and REL are the concepts used to describe the inner principles. The 'clss' is classified as 'classes' and the intermediator relations should be depicted as 'rels', and renamed as properties, has to satisfies the conditions cl *ss* ∈ CLS, rels ∈ REL; The <=CLS and <=REL are two partial orders on CLS and REL and it has named as concept hierarchy and relation hierarchy. The σ = R-> CLS × CLS is a function where $\sigma(rels) = <domn(rels)$, rang (rels) > with *rels* ∈ REL, the domain rels is represented as domn (rels) and the range rels is represented as rang (rels).

Figure 4.6 shows that the department Ontology example and it contains the classes, objects, attributes, and relations. The department contains branches like EEE, CSE, and ECE. The professor and student is a human category. The professor contains research work and has classwork whereas a student has only classwork. In research work, has the publications and projects whereas class work has the subject and its associated timetable of periods. In the same manner, the healthcare sector also mapped with ontologies.

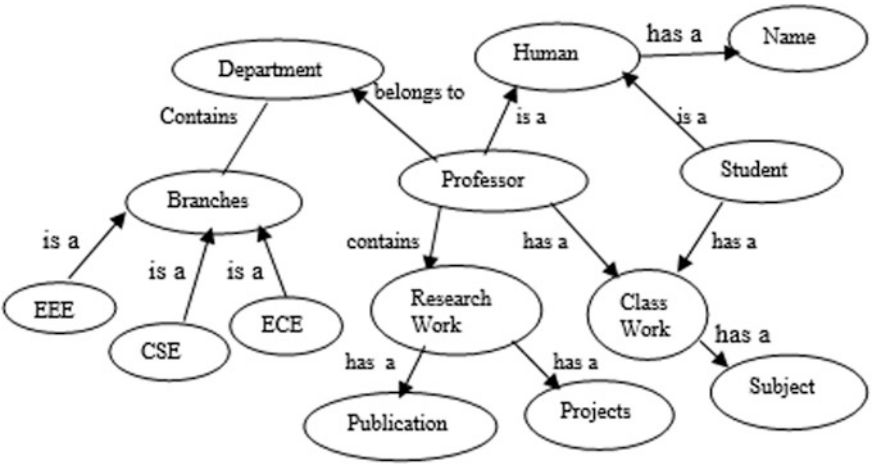


Fig. 4.6 Department ontology example

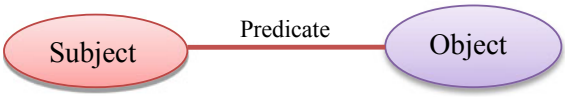


Fig. 4.7 RDF

4.3.2 RDF

The RDF stands for Resource Description Framework (RDF), developed and presented by World Wide Web Consortium (W3C) in early 1999 for providing the machine-readable and understandable data to the users. The RDF directly supports integration and analysis among the heterogeneous IoT applications that interchange machine-readable data on the Web. Figure 4.7 is the RDF in syntactical structural format and it consists of subject, predicate, and object view.

For example, consider the IoT resource sentence "sensor has type temperature". In this sentence, sensor is the subject, has type is the predicate, and temperature is the object. Like this, the RDF statements are generated with semantical meanings.

4.3.3 RDF Schema

Brickley and Guha [24] presented the RDF schema and it provides the data modeling vocabulary to the data supported by RDF. The RDF schema is a semantic extension of the data modelling RDF vocabulary and it illustrates the related descriptions and establishes the meaningful connections between resources.

Figure 4.8 depicts the RDF schema example, it has the domain, and range values are mentioned. The director contains a subclass called Famous director and the director can direct the movies.

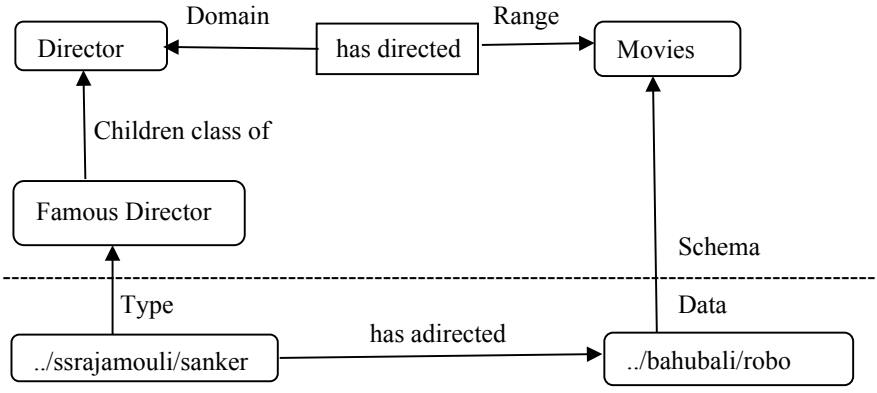


Fig. 4.8 RDF schema example

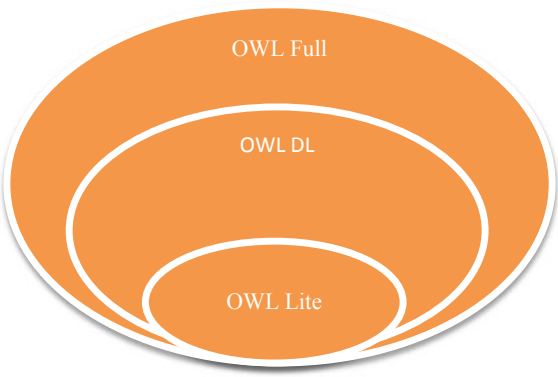


Fig. 4.9 OWL family

4.3.4 OWL

The OWL stands for Web Ontology Language (OWL) was developed by W3C. It is a semantic markup language used to exchange the ontology on the Web. The primary purpose for the creation of OWL is to extend the vocabularies of RDF data. The OWL family contains OWL Full, OWL DL (Description Logic), and OWL Lite. Figure 4.9 shows the complete OWL family structure.

4.3.4.1 OWL Full

It uses the all functionalities of the OWL language. Additionally, it takes the primitives of RDF and RDF Schema. This is fully upwards with RDF compatible in a semantic and syntactic way.

4.3.4.2 OWL DL

The OWL-DL denoted as Description Logic, is the subpart of OWL Full and takes limited primitives compared to OWL Full. The description logic is ensured to support semantic reasoning.

4.3.4.3 OWL Lite

This again some limited primitives has taken and applied compared to OWL DL (Description Logic). This is a restricted end not supported cardinalities, enum-classes, and disjoint operations. However, it is easy to understand the logic of primitives and implementations.

4.3.5 Semantic Reasoning

Semantic reasoning or Reasoning engine is used to infer logical consequences from a set of axioms, rules, and facts. Apache JENA, RDF Sharp, Prova, Flora-2, RACER are the widely used tools for semantic reasoning on IoT over sensors data. Figure 4.10 illustrates the semantic reasoning engine for unifying the IoT sensor data. It takes the openIoT dataset and makes the semantic IoT data with adding ontologies. The composition of data or unifying data is formed on combing the IoT raw data and Semantic IoT data. Thereafter, the unifying data is implemented on real-time projects like VITAL testbed and Smart Santander testbed. There are various types of IoT services available in the form of RESTful, SOAP, and APIs from users to model the unified language and describe the IoT data. The semantic query engine is used to querying and unifying the IoT data. The rule-based engine and machine-learning engine are developed for simple and complex data streams respectively. These two are high abstraction level principles to make semantic reasoning engine more powerful and efficient.

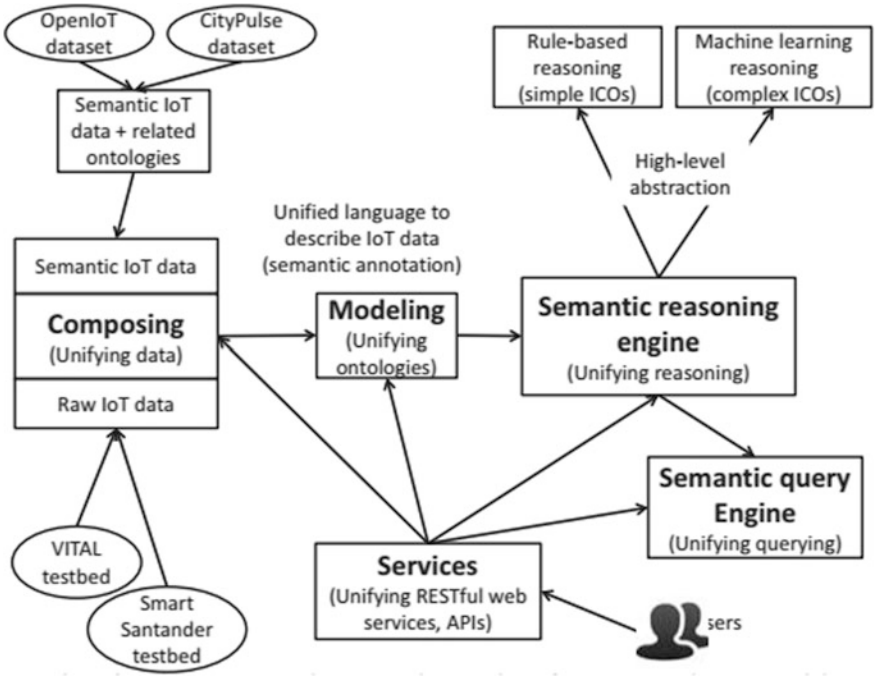


Fig. 4.10 Semantic reasoning engine for unifying the IoT sensor data

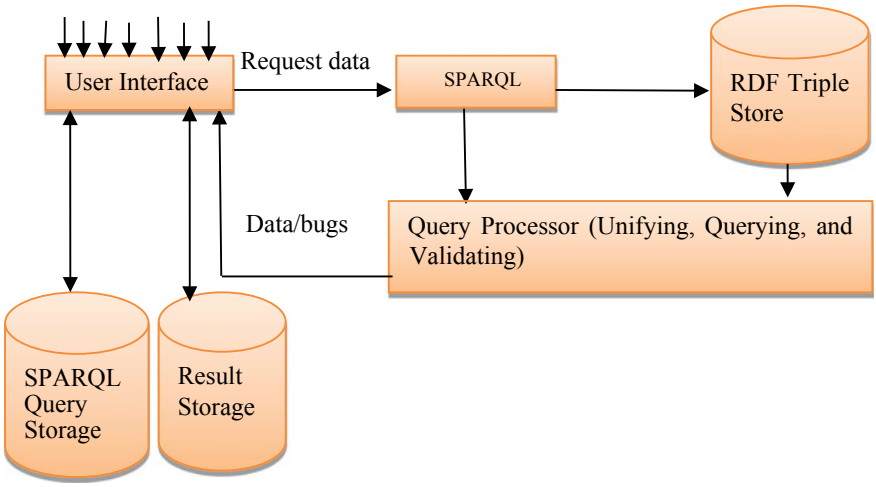


Fig. 4.11 SPARQL semantic execution framework

4.3.6 SPARQL

SPARQL stands **f**or **S**imple **P**rotocol **A**nd **R**DF **Q**uery **L**anguage and it was developed and presented by W3C. This is a directed graph with semantics for performing data on the Web. Figure 4.11 depicts the SPARQL semantic execution framework. The user interface takes the input from the user and stores the requested data in the RDF triple format using SPARQL. The query processor performs the data on unification, querying, and validation. It evaluated the big data processing mechanism for integrations IoT sensor data. Having an improved query response time for the proposed mechanisms the streaming data is processing with SPARQL queries.

4.3.7 Semantic Annotations

Semantic annotations have been originated from the text annotations. Adding semantic annotations to the resources is a big asset to solve the interoperability problem in IoT-based applications. This is a process of annotating the IoT resources with semantic metadata. To annotate the resources, first, identify the entity and then entity disambiguation and finally annotate the data to resources. Balakrishna et al. [1–3] surveyed the semantic technologies in clear-cut vision and presented a well-organized manner. As per the author views, the semantic annotations are efficient mechanisms for unifying the IoT sensor data.

4.4 Clustering Approaches

In this section, the authors will discuss how the huge amount of sensor data has been integrated and analyzed for future predictions. The machine learning techniques are predominantly categorized as supervised and unsupervised learning. The semi-supervised and reinforcement learning algorithms are does not mention here because those are out of the scope of this chapter. The supervised learning is sub-categorized into classification problems and regression problems along with dealt top most algorithms. Similarly, the unsupervised algorithms dealt with clustering and dimension reduction problems. Based on the type of the user requirement and the problem occurred in the sensor data along with corresponding algorithms has been chosen. The needful clustering algorithms for performing data analysis and integration in IoT sensor data are partitioned. For this point of research work, in machine learning techniques, unsupervised learning is suitable for integration and analysis of IoT data. The most popular clustering algorithms are used in this regard and will overview all types of clustering approaches next sub-section Clustering is an unsupervised approach. In this, the unlabelled data is grouped into similar kind of clusters. In general, clustering determines to discriminate the matching and un-matching sensor data.

Figure 4.12 shows that the heterogeneous data items are grouped and make the cluster merging. If the matched items are away from the cluster, means create a new cluster. It clearly indicates that three clusters are formed in a spherical structure.

Actually, there is no important to expose the data in the spherical format it can also depict the irregular format as shown in Fig. 4.13.

If the unlabelled data is grouped and perform analysis as well as predictions on the sensor data, then clustering is an ultimate and powerful solution in this regard. Dimensionality reduction, outlier detection, finding missed data, sensor fault detection and prevention are the popular problems occurred in the clustering. For every problem, there are different categories of algorithms are available for analysis and presented detail in the next section. Choosing the correct clustering algorithm for the appropriate problem is a big challenge.

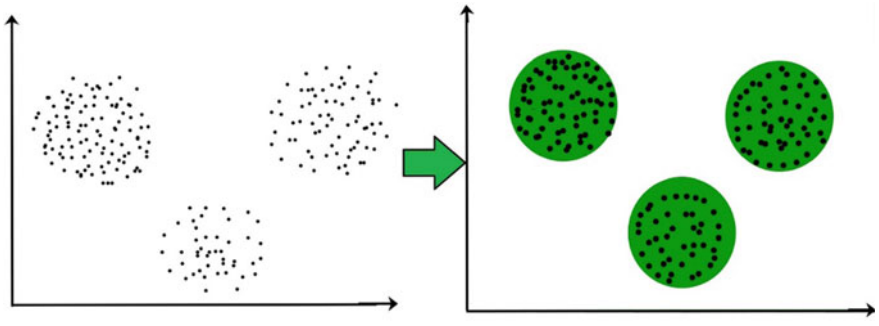


Fig. 4.12 Clustering in spherical

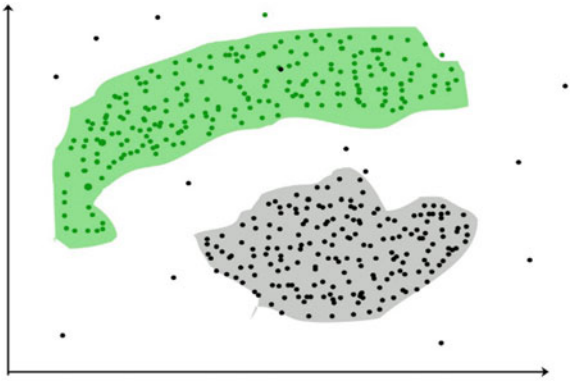


Fig. 4.13 Clustering in non-spherical

Table 4.1 Traditional clustering algorithms overview

S. No.	Clustering algorithm category	Example
1	Partition	K-means, fuzzy c-means, k-medoids, CLARANS, PAM, and CLARA etc.
2	Hierarchy	BIRCH, CURE, ROCK, and Chameleon etc.
3	Fuzzy	FCM, MM, and FCS etc.
4	Distribution	DBCLASD, EMA, and GMM etc.
5	Density	DBSCAN, Mean-shift, and OPTICS etc.
6	Graph theory	CLICK and MST etc.
7	Grid	STING and CLIQUE etc.
8	Fractal theory	FC
9	Model based	COBWEB, GMM, SOM, and ART etc.

4.4.1 Clustering Types

There are aforementioned clustering approaches are available for performing analysis and integrating the IoT sensor data. In that authors have been surveyed the most relevant and accurate clustering algorithms in this regard as shown in Table 4.1.

4.4.1.1 Distribution Based Mechanisms

In this type of clustering mechanism, the sensor generated data is fitted in probability-distributed manner [25]. The dynamic data is portrayed in the exact distribution. If this process is increased in irregular then the probability of the distribution is also gets maximum window size. Figure 4.14 shows the resultant of the dynamic data is distributed in this way.

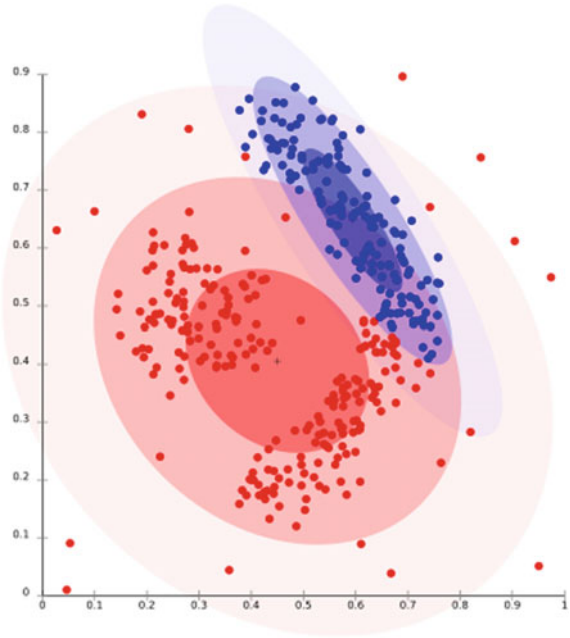


Fig. 4.14 Distribution based approach. **Pros**: 1. Good at synthetic healthcare data items. 2. Distinctly sized clusters. **Cons**: Sometimes constraints should not be categorized if the proposed model is complex in nature. **Example**: Expectation-Maximization Algorithm (EMA), etc.

4.4.1.2 Centroid-Based Mechanisms

Nowadays this type of clustering mechanisms are popular and these will follow the iterative approach. To accomplish this approach, first, need to find the centroid of the cluster. The centroid is called as the center of the cluster and find by measuring the Euclidean distance or mean of the dataset elements [26]. Figure 4.15 illustrates how the data represented in the centroid-based approach.

4.4.1.3 Connectivity-Based Mechanisms

This mechanism is somewhat similar to the centroid-based mechanism. To fix the number of clusters based on nearest of data items. If the dataset items are closer to the cluster compared to the dataset elements far in distance. If the dataset elements are closeness, means need to merge the cluster whereas the dataset items are far away from the cluster means need to create a new cluster for dynamic data points. The connectivity-based mechanism of the clustering resulted graph is depicted in Fig. 4.16.

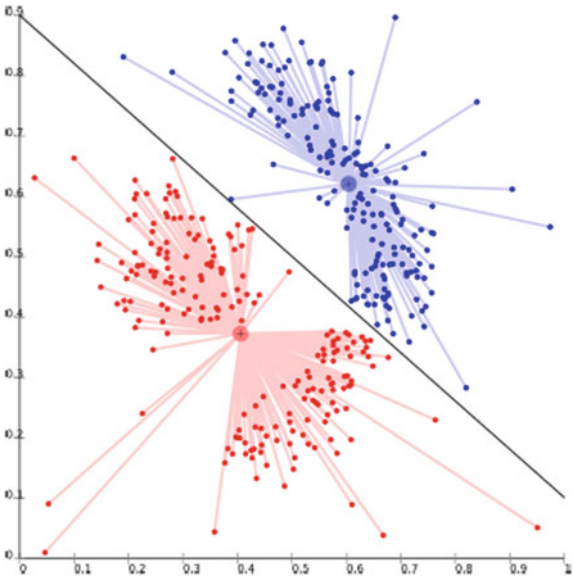


Fig. 4.15 Centroid-based approach. **Pros**: 1. Fast and simple for medium-sized datasets. 2. Accurate. **Cons**: 1. Need to fix the number of clusters in advance. 2. Not useful if the data set is too large. **Example**: K-means, Fuzzy c-means

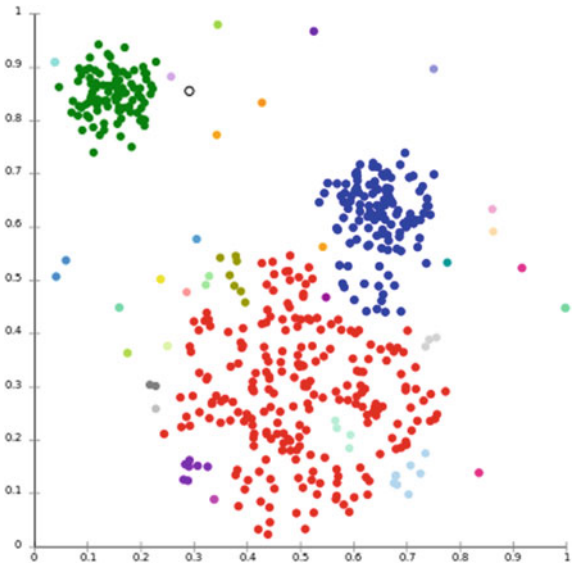


Fig. 4.16 Connectivity-based approach. **Pros**: very easy to implement. **Cons**: scalability. **Example**: ICFS (Incremental Clustering by Fast Search), and hierarchical algorithm, etc.

4.4.1.4 Density-Based Mechanisms

This clustering algorithm is much popular for finding the non-linear data space for the varying clusters based on density [27, 28]. This type of clustering mechanism able to find sensor fault detection and prevention in the healthcare sector and many more fields. Figure 4.17 showing that the resulted clustering of the non-linear data space in a density-based approach.

The following are a list of application areas to be supported for performing clustering and analysis in IoT sensor data.

- Online-Marking
- Biology
- Online-Libraries
- City planning
- Insurance
- Earthquake studies
- Bio-medical engineering
- Image processing
- IoT and WSN technologies
- Data mining and Data warehousing
- Artificial Intelligence
- Cloud Computing
- Big data and much more fields.

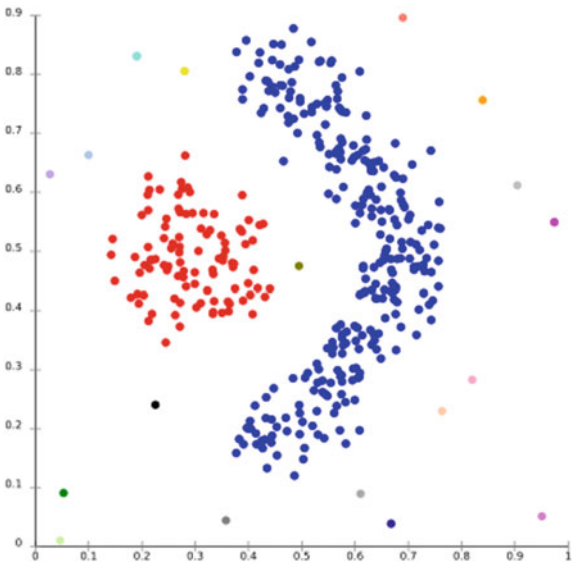


Fig. 4.17 Density based approach. **Pros**: 1. No need to specify the number of clusters in advance. 2. Able to perform the noise in the data. **Cons**: Fails if the dataset is too large. **Example**: OPTICS, and DBSCAN, etc.

4.4.2 Incremental Clustering

The incremental clustering (IC) algorithms are widely for dynamically IoT sensor data. The sensor data coming heterogeneous protocols, formats, and applications are enormous in demand. To process the data in an iterative manner for performing analysis and predictions, the IC algorithms are suitable. Most of the IC algorithms are deals with static and balanced data. The simplicity in implementation has added advantage of this type of clustering approaches in one end. In the other end, this type of algorithms consumes less time when compared to other approaches. Nevertheless, it is a failure in dealing with non-spherical and unbalanced data. Mean-Shift, Affinity Propagation (AP) [29], and DBSCAN are examples for this type of incremental approaches.

4.4.3 CFS Clustering

Clustering by Fast Search (CFS) [30] is mainly using the exemplars for identifying centers of clusters in an efficient way. In order to obtain the cluster centers of multiple representatives in dataset need to use the objective function '*Of*' is as shown in Eq. 4.3 as follows

$$Of = \sum_{i=1}^{n} p(obj_i, e_i) \tag{4.3}$$

Here $p(obj_i, e_i)$ depicts that distance among the object obj_i and the exemplar e_i is measured. The main motivation behind this CFS is to minimize the cluster centers objective function shown in Eq. 4.1. Therefore, to propagate this objective function, two of the other functions has to be calculated. The first one is local density ld_i and the second one is minimum distance δ_i is as shown in Eq. 4.4

$$ld_i = \sum_{i,j=1}^{n} q\left(dist_{i,j} - dist_c\right) \tag{4.4}$$

where $dist_{i,j}$ represents that the object obj_i and object obj_j distance. The $dist_c$ is any of the object in the dataset as shown in Eqs. (4.5)–(4.6).

$$\mathrm{q(obj)} = \begin{cases} 1 & \text{if obj} < 0 \\ 0 & \text{otherwise} \end{cases} \tag{4.5}$$

$$\delta_i = \min_{j=ld_i > ld_j} \left(dist_{i,j}\right) \tag{4.6}$$

If the object obj_i has achieves the peak density than it's md_i is measured as $\delta(i) = max_j(dist_{i,j})$.

$$\gamma_i = ld_i * \delta_i \tag{4.7}$$

The data objects contain the huge local density ld_i and the higher distance δ_i among the nearest representatives must select the centers of the clusters. Therefore, the large value γ_i has been calculated by using the Eq. 4.7.

As of now, discussed how to find the cluster centers to minimize the objective function with the help of local density and a minimum distance between neighboring data representatives. The cluster centers are required for new arriving objects are merged in the same cluster or create a new cluster based on the threshold function using Eq. 4.8.

$$Threshold\ Value = \frac{(new\ data - old\ data)}{(old\ data)} * 100 \tag{4.8}$$

The modern clustering algorithms are more powerful for integration and analysis of IoT sensor data. Those are listed as follows:

- Clustering on data streams
- Clustering on sequence data
- Clustering on spatial data
- Clustering for large-scale data
- Clustering based on density and distance
- Clustering on affinity propagation
- Clustering for spectral graph theory
- Clustering on quantum theory
- Clustering for swarm intelligence
- Clustering based on kernel
- Clustering for ensemble methods.

4.5 Challenges and Research Directions

In this section, discuss the challenges and research directions in IoT sensor data integration and analysis. The current research directions faced by the researchers dealing with dynamic data coming from IoT sensor devices, protocols, data formats, and heterogeneous resources, are list-out as follows:

- Scalability Issues
- Adding Semantic annotations to the sensor data with clustering analysis
- IoT data interoperability
- Automatic annotations for unifying the sensor data

- Extraction mechanism for IoT senor resources
- Reasoning over the data
- Clustering the dynamic data
- To find the hidden data is normal or abnormal etc.

Table 4.2 shows that the challenges faced for sensor data integration and analysis with semantics and clustering approaches. Ongoing with semantic web approaches, IoT approaches, and limitations are discussed. The Linked Open Data (LOD), Linked Open Vocabularies (LOV), Linked Open Rules (LOR) are under semantic web approaches. The same is extended with IoT, which make the LOD4IoT, LOV4IoT, S-LOR, ARM, and SWoT in intelligence manner. The limitations are specified with each category of the approach combinable with semantic web and IoT approaches.

These are the current challenges to achieve sensor data integration and analysis in heterogeneous IoT resources.

1. **IoT data unification**: The motivation behind data unification in IoT platforms is Linked Open Data (LOD). There is a need to develop the Linked Open Data for the Internet of Things (LOP4IoT) to solve the scalability and reliability of a high amount of big data real-time processing. The data coming from various heterogeneous data through IoT devices and protocols. Therefore, the huge sensor data is required complex event processing mechanisms for processing in real-time and unifying smart IoT data.

Table 4.2 Challenges as per domain specific

Challenges	Domain		
	Semantic Web approaches	Internet of Things (loT) approaches	Limitations
Unifying data	Linked open data (LOD)	Linked open data for internet of things (LOD4loT)	– Not adapted to real-time – To reuse and combine data
Unifying model/ vocabulary/ ontology	Linked Open vocabularies (LOV)	Linked Open vocabularies for internet of things (L0V4foT)	– Lack of best practices – To reuse, extract and combine ontologies – No ontology matching tools adapted to loT ontologies
Unifying reasoning	Linked open rules (LOR)	Sensor-based linked open rules (S-LOR)	– Need more approaches for interoperable reasoning and sharing and reusing-based approaches – S-LOR limited for complex ICOs
Unifying architecture	-	Architecture reference model (ARM)	-
Unifying service	Semantic web services	Semantic web of things (SWoT) gene rator	– Composition of services

2. **Querying of Model/Architecture/Framework for semantically annotating the IoT sensor data**: Semantic annotations are used to solve the interoperability problem in IoT domains. Adding the semantic annotations for querying the IoT smart data has become a crucial problem. Therefore, using SPARQL queries is one approach for the data is to be queried and enriched. The unification of the models, frameworks, and architectures to propagate the interoperability in IoT applications and that would enable the reusing, exchanging, and merging.
3. **Semantic reasoning on IoT data**: Semantic reasoning is also the important issues of semantic interoperability in IoT platforms. Adding rules/facts and real value of the data is offered by semantic reasoning mechanisms. Exchanging and reusing the sensors data is more adaptable for services and applications.
4. **The unification of services**: The service unification leads to the interoperability of the IoT data supports to service composition and discovery for two or more sophisticated applications. It also mitigates the refinement in annotations in services is making the smart city applications more intelligent and smart.
5. **Real-time processing and reliability of scalable big data analytics**: Some of the smart city applications contains the big data coming from the IoT sensor world. The real-time processing of that data requires more complex event algorithms to propagate the reasoning over the IoT data.

4.6 Conclusion and Future Work

In this chapter, the authors presented a decent survey on semantic technologies for IoT smart city applications and presented the semantic technologies like Ontologies, RDF, RDF Schema, OWL, SPARQL, semantic annotations and semantic reasoning mechanism was required to interoperable IoT smart data. Some of the real-time examples were taken and explained the semantic technologies for IoT domains. The unsupervised clustering mechanisms were discussed for performing analysis on IoT sensor data. The recent challenges and current research directions were mentioned in clear-cut vision. With this survey, the authors have been outlined that the semantic technologies were important for semantically interconnecting the heterogeneous IoT resources globally. Clustering approaches have taken into account and surveyed for performing analysis on IoT sensor data. In future, firstly, to survey more semantic technologies and more clustering algorithms, that was missed in this paper. Secondly, the presented current research directions are taken into account and will perform the implementations on IoT-based smart city applications like Smart home, Traffic management, Smart parking, Healthcare, Industry 4.0, and many more. As of now, the authors discussed only sensor data integration in IoT using semantics and machine learning approaches. In addition, in the future, the authors can progress the work as follows:

1. Sensor data integration in smart city domain both IoT and Machine Learning implementation using appropriate tools.
2. Data analysis is also considered as a major impact on the smart city sector whether the sensor data is syntactically correct or not.
3. The sensor data is stored in an intelligent IoT cloud platform, so providing security to the stored sensor data is a critical problem to be addressed.
4. Semantic analytics is also a major area to do more research for classification and clustering on IoT smart data.

References

1. Balakrishna, S., Thirumaran, M., Solanki, V.K.: A Framework for IoT sensor data acquisition and analysis. EAI Endorsed Trans. Internet Things **18**(1), 1–13 (2019). http://dx.doi.org/10.4108/eai.21-12-2018.159410
2. Balakrishna, S., Solanki, V.K., Gunjan, V.K., Thirumaran, M.: Performance analysis of linked stream big data processing mechanisms for unifying IoT smart data. In: Proceedings of International Conference on Intelligent Computing and Communication Technologies (ICICCT), pp. 680–688. Springer, Berlin (2019). https://doi.org/10.1007/978-981-13-8461-5_78
3. Balakrishna, S., Solanki, V.K., Gunjan, V.K., Thirumaran, M.: A survey on semantic approaches for IoT data integration in smart cities. In: Proceedings of International Conference on Intelligent Computing and Communication Technologies (ICICCT)pp. 827–835. Springer, Berlin (2019). https://doi.org/10.1007/978-981-13-8461-5_94
4. Xiao, G., Guo, J., Xu, L.D., Gong, Z.: User interoperability with heterogeneous IoT devices through transformation. IEEE Trans. Industr. Inf. **10**(2), 1486–1496 (2014)
5. Pavithra, D., Balakrishnan, R.: IoT based monitoring and control system for home automation. In: Proceedings of the Global Conference on Communication Technologies (GCCT'15), pp. 169–173. IEEE (2015)
6. Nugroho, B.R.: The architecture of an IoT-based healthcare monitoring system using smart e-health gateways in home/hospital domain. Bull. Inovasi ICT & Ilmu Komputer **2**(1), 1–6 (2015)
7. Agra, A., Christiansen, M., Ivarsøy, K.S., Solhaug, I.E., Tomasgard, A.: Combined ship routing and inventory management in the salmon farming industry. Ann. Oper. Res. 1–25 (2016)
8. Zhao, X., Fan, H., Zhu, H., Fu, Z., Fu, H.: The design of the internet of things solution for food supply chain. In: Proceedings of the International Conference on Education, Management, Information and Medicine, pp 1–8 (2015)
9. Misra, P., Rajaraman, V., Dhotrad, K., Warrior, J., Simmhan, Y.: An interoperable realization of smart cities with plug and play based device management, pp. 1–8 (2015). https://arxiv.org/abs/1503.00923
10. Aldabbas, O., Abuarqoub, A., Hammoudeh, M., Raza, U., Bounceur, A.: Unmanned ground vehicle for data collection in wireless sensor networks: mobility-aware sink selection. Open Autom. Control Syst. J. **8**(1), 35–46 (2016)
11. Grant, C.C., Jones, A., Hamins, A., Bryner, N.: Realizing the vision of smart firefighting. IEEE Potentials **34**(1), 35–40 (2015)
12. Santos, J., Rodrigues, J.J.P.C., Silva, B.M.C., Casal, J., Saleem, K., Denisov, V.: An IoT-based mobile gateway for intelligent personal assistants on mobile health environments. J. Netw. Comput. Appl. **71**, 194–204 (2016)

13. Balakrishna, S., Thirumaran, M.: Semantic interoperable traffic management framework for IoT smart city applications. EAI Endorsed Trans. Internet Things **4**(13), 1–17 (2018). https://doi.org/10.4108/eai.11-9-2018.15548
14. Balakrishna, S., Thirumaran, M.: A RESTful CoAP protocol for internet of things. In: Proceedings of 7th International Conference on Informatics Computing in Engineering Systems (ICICES), pp. 1–6. IEEE (2018)
15. Balakrishna, S., Thirumaran, M.: Towards an optimized semantic interoperability framework for IoT-based smart home applications. In: Balas, V., Solanki, V., Kumar, R., Khari, M. (eds.) Internet of Things and Big Data Analytics for Smart Generation. Intelligent Systems Reference Library, vol 154, pp. 185–211. Springer, Cham (2019)
16. Balakrishna, S., Thirumaran, M.: Programming pParadigms for IoT applications: an exploratory study. In: Solanki, V, Díaz, V., Davim, J. (ed.) Handbook of IoT and Big Data, pp. 23–57. CRC Press, Boca Raton (2019)
17. Atzori, L., Iera, A., Morabito, G.: the internet of things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
18. Zeng, D., Guo, S., Cheng, Z.: The web of things: a survey. J. Commun. **6**(6), 424–438 (2011)
19. Petrolo, R., Loscr's, V., Mitton, N.: Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms. IEEE Trans. Emerg. Telecommun. Technol. 1–14 (2015)
20. Aggarwal, C.C., Ashish, N., Sheth, A.: The internet of things: a survey from the data-centric perspective. In: Managing and Mining Sensor Data, pp. 383–428. Springer, Berlin (2013)
21. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Context aware computing for the internet of things: a survey. Commun. Surveys Tutor. IEEE **16**(1), 414–454 (2014)
22. Raul Garcia-Castro, O.C., Gomez-Perez, A.: Ready4smartcities: Ict roadmap and data interoperability for energy systems in smart cities. In: 2014 European Semantic Web Conference, pp 1–6 (2014)
23. Ganz, F., Puschmann, D., Barnaghi, P., Carrez, F.: A practical evaluation of information processing and abstraction techniques for the internet of things. IEEE Internet Things J. 1–18 (2015)
24. Brickley, D., Guha, R.V.: Resource description framework (RDF) schema specification 1.0 (2000). W3C Candidate Recommendation, 27 Mar. Available on http://www.w3.org/TR/rdf-schema/
25. Wang, Y., Chen, L., Mei, J.P.: Incremental fuzzy clustering with multiple medoids for large data. IEEE Trans. Fuzzy Syst. **22**(6), 1557–1568 (2014)
26. Zhao, L., Chen, Z., Yang, Z., Hu, Y., Obaidat, M.S.: Local similarity imputation based on fast clustering for incomplete data in cyber-physical systems. IEEE Syst. J. (2016). https://doi.org/10.1109/JSYST.2016.2576026
27. Singh, S., Awekar, A.: Incremental shared nearest neighbor density based clustering. In: Proceedings the 22nd ACM International Conference on Information & Knowledge Management, pp. 1533–1536. ACM (2013)
28. Bakr, A.M., Ghanem, N.M., Ismail, M.A.: Efficient incremental density-based algorithm for clustering large datasets. Alexandria Eng. J. **54**(4), 1147–1154 (2015)
29. Sun, L., Guo, C.: Incremental affinity propagation clustering based on message passing. IEEE Trans. Knowl. Data Eng. **26**(1), 2731–2744 (2014)
30. Rodriguez, A., Laio, A.: Clustering by fast search and find of density peaks. Science **344** (6191), 1492–1496 (2014)

Chapter 5
IoT Sensing Capabilities: Sensor Deployment and Node Discovery, Wearable Sensors, Wireless Body Area Network (WBAN), Data Acquisition

T. Poongodi, Anu Rathee, R. Indrakumari and P. Suresh

Abstract Internet of Things (IoT) is an emerging technological paradigm where the things can be connected from different fields through the Internet. The rapid advancement in communication technologies, actuators and low-cost sensing devices leads to extensive deployment of IoT devices. Such devices can be deployed in any public spaces provide detailed information about the behavior of individuals such as personalization, behavior change and personal health monitoring. IoT technology which is being deployed is specially designed to make it invisible, such that the technology does not manifest its presence to the users it is monitoring. For the IoT based healthcare applications, the Wireless Body Area Network (WBAN) is gaining much popularity as wearable devices spring into the marketplace. Multiple sensor nodes can be deployed on different locations of the human body to measure the heartbeat, body temperature distribution, and detect falls. In addition to medical signals, the sensor nodes can be placed to track environmental conditions around the human body as well. Hence, wearable sensor systems afford valuable information about the impact of human health. These systems are not only limited for personal use, can be fitted on animal, car, etc. to construct a wireless sensor network. According to previous estimation, healthcare IoT solutions lay down the platform for extremely accessible, personalized and on-time services that will attain $1 trillion by 2025 hopefully. Wearable systems have emerged as a prominent area in healthcare for managing cardiovascular,

T. Poongodi (✉) · R. Indrakumari · P. Suresh
School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India
e-mail: tpoongodi2730@gmail.com

R. Indrakumari
e-mail: indramurugesh25@gmail.com

P. Suresh
e-mail: psuresh2730@gmail.com

A. Rathee
Maharaja Agrasen Institute of Technology, New Delhi, India
e-mail: anujaglan@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_5

neurological diseases etc. These sensors are used on the body surface or inside the human body non-invasively, however it is distinct from invasive implantable devices. This system will be particularly helpful for sensing information inside the human body as the sensors are designed and supported by flexible technologies. The sensing device collects data which is transmitted through wireless communication protocols to a server that is responsible to gather the datasets available for further analysis. WBAN comprised of heterogeneous nodes fixed in and around the human body which is connected to the network. It is characterized by IEEE 802.15 communication standard; generating huge volume of data and gathering it play a vital role in electronic healthcare. Data residing in multiple wireless devices need to be collected and analyzed effectively. Within WBAN datasets may be fragmented across many nodes and if practitioner's node does not have the correct information then the quality of healthcare processing would be degraded. This chapter presents the overview of wearable sensors for tracking physiological and physical changes in daily life, their basics and applications. Wearable sensor based systems have enormous potentials to be completely explored and it is anticipated that advancement in technologies will afford the transformation how healthcare will be in future. It highlights the significance of localization in on-body area network and it gives an overview about evaluating the performance of localization systems. It also presents the several types of sensors and methodologies to fuse the data generated by sensors. Since we foreseen a future where the existence of miniature devices communicating through packet radio in both indoor and outdoor environments.

Keywords Sensors · Actuators · Deployment · Wearable devices · WBAN · Data acquisition · Localization

5.1 Introduction

IoT is an emerging technology which builds over the mobile and internet networks automatically expands the world's network even further. According to Gartner's Hype Cycle, it is anticipated that IoT will take next 5–10 years for market adoption. It consists of different technological layers that initiates a role from primarily connecting 'things' to building applications that declares a clear objective whether it is meant for industry grade IoT projects or consumer based applications [1–3]. Sensors are the significant building blocks of IoT and could be deployed everywhere, for instance, from military battlefield to agriculture farm fields, vineyards, golden gate bridge, redwoods etc. The sensors can be worn or implanted under human body skin, on a T-shirt or in a purse. IoT market has reached an exponential growth with immense range of IoT products in different areas such as people's private lives, enterprises, and controls huge industrial appliances. Basically, IoT exploits conventional standard networking technologies and protocols. However, the major protocols and various enabling technologies of IoT are low-energy radio protocols, low energy Bluetooth, low-energy wireless, RFID, NFC, WiFi-Direct

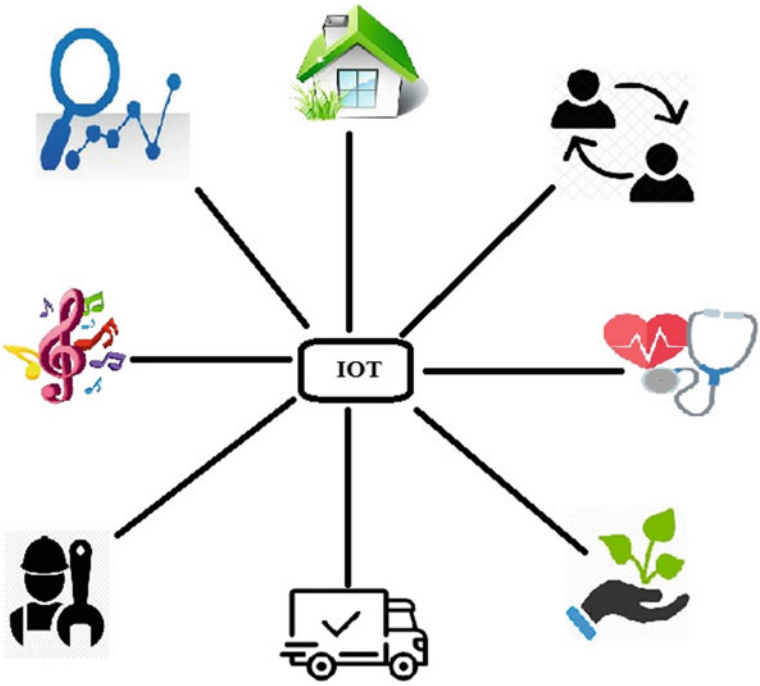


Fig. 5.1 Domains associated with Internet of Things

and LTE-A. The most significant factor of IoT makes anything "smart", means that it enriches people's life with the efficient data collection, processing and decision making [4–6]. Figure 5.1 tells about the domains where IoT is used to make life smarter and convenient. An efficient, scalable, secured, computing and storage resources are essential to realize the complete IoT vision.

The sensors and actuators in IoT blend seamlessly in the surroundings around us and the information is communicated across different platforms in order to construct a Common Operating Picture (COP). The recent adaptation of several enabling device technologies such as Near Field Communication (NFC), RFID tags and readers, transforms the internet into a most expecting next revolutionary technology.

5.1.1 IoT Technology Stack

IoT technology stack comprises of IoT devices, actuators, sensors and gateways in IoT platform and it is viewed as a three layered model.

(i) IoT devices: Accurate sensors, actuators and devices produce accurate data which is vital for IoT.
(ii) IoT gateway: It can be connected to the internet for transferring data using 3G/4G/GPRS modem, Wi-Fi, Ethernet. Non-GPRS network is preferable for internet connectivity and this level is deserved because which is strongly connected towards consumer and business applications and services.
(iii) IoT platform: It acts as an interface between business applications and services and the first two layers.

IoT bridges the gap among the physical and digital world with the use of IoT devices which are available in various forms and shapes [7]. IoT devices consist of transducers such as actuators, sensors, and myriad objects called 'intelligent'/'smart'. A connected object may have any number of sensors and transducers. In car, telemetric box can be fixed to know about the car insurance which has a few sensors and an oil rig has thousands of sensors. The device connectivity enables the link between the physical things and the controller via communication and processing units [8–10].

IoT sensors:

Sensors are acting as a digital backbone of IoT and it is a device that measures any specific quantity such as motion, heat, light, moisture, pressure by converting them into electrical pulses. A transducer converts the signal from one form to another form. In the context, IoT sensors are capable of sensing the environment or in and around IoT devices to which they are attached [11–13]. Sensors can detect the changes in the surroundings and events or changes of some specific parameters are communicated to the system for further analysis and action. Sensors can sense about the environmental factors, parameters, and events such as temperature, sound, humidity, light, presence of gases or chemical components etc. It plays a significant role among all IoT components because it is the starting point of data gathering that needs to be very accurate. Figure 5.2 shows several sensor types available nowadays and it can be bought separately or fixed with sensor boards where many sensors are fixed that are required in the scope of different IoT use-cases or projects. For example, sensors boards for different applications such as smart traffic, smart city air quality monitoring etc. are available. Sensor boards could also be customized by adding the required sensors or precise boards can be built.

IoT actuators:

Actuators are transducers that act and activate after receiving a signal sets in motion for action in an environment. In smart building, actuators can be fixed in a radiator, actuators get triggered if the temperature level is low and reports that the energy saved as a result as a decision. The role of actuator in IoT is expected to reach 5.4% CAGR until 2025. Figure 5.3 shows that how a signal is transmitting from sensors to the actuators. Initially a sensor node detects heat or some noise. After that this signal is transferred to the control center and then the control center is responsible for sending the signal to initiate the command for the devices. There are several types of sensors and actuators available in the market. Electrical actuators turn energy into mechanical torque and some actuators control valves, for example

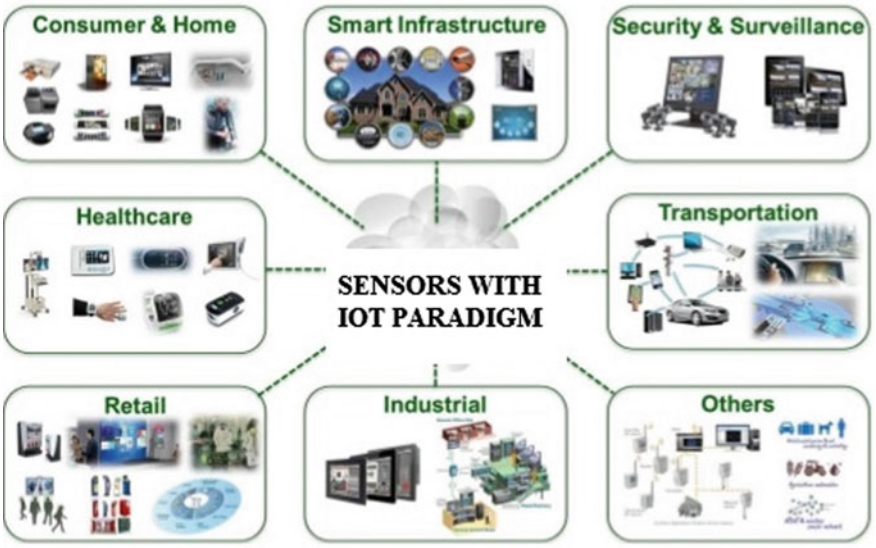


Fig. 5.2 Different types of IoT sensors based on application areas

Fig. 5.3 Data flow from sensor to actuators

water leakage. In robotics or industrial applications, the actuators are mainly used for grippers.

IoT Gateways:

It acts as an interface between devices and IoT platforms. It can be hardware, software or both and it is a separate layer provides more functionalities. It is a layer with multiple devices used for connectivity aggregation, encrypting and decrypting IoT data (to secure the data). Pre-processing can be accomplished in the gateway and the effective data analysis process is improved significantly.

IoT platform:

It is the third layer in IoT technology stack with various potential features [4, 5]. It is meant for gathering data and makes sense of data in order to provide the right services as the right time. IoT platform offers services such as connectivity support, device management, service enablement, application support.

5.2 IoT Technologies

The most widely used IoT technologies for the success of IoT products and services are [1, 2, 14]:

1. Radio Frequency Identification (RFID)
2. Wireless Sensor Networks (WSN)
3. Middleware
4. Cloud computing
5. IoT application software.

- Radio Frequency Identification RFID

RFID permits automatic identification and data captured using radio waves, a reader and a tag. The tag in RFID is capable of storing more data than conventional barcodes and it holds data in the form of Electronic Product Code (EPC) [3]. There are three types of tags commonly used:

(i) Passive tags: Passive RFID tags are not battery powered and it rely on radio frequency to obtain the energy for the tag.
(ii) Active tags: Active RFID tags can activate the communication with the reader and it has self-contained batteries. It also contains many external sensors to track pressure, chemicals, temperatures and some other conditions. These kinds of tags are mainly used in remote sensing, manufacturing and hospital laboratories.
(iii) Semi-passive tags: It is expensive than passive tags and use batteries to create energy.

According to International Data Corporation (IDC), IoT is anticipated to reach the Compound annual Growth Rate (CAGR) of 14.4% in the forecasted period 2017–2021 and it reaches $1 trillion in 2020 and $1.1 trillion in 2021. Figure 5.4 shows that no of devices connecting to internet are increasing rapidly at a very fast rate.

- Wireless Sensor Network (WSN): Sensor networks bridge the gap between the physical and computational world by providing reliable, scalable, fault tolerant and accurate monitoring of the physical phenomenon [15, 16]. A sensor network is composed of a large of sensor nodes that are densely deployed either inside the phenomenon or very close to it. The main task of the sensor networks can be categorized as: Sensing, Processing and Acting. After sensing the network, based on the query provided by the user, the sensor node may process the data, and sometimes may also aggregate the data sent to it by other nodes, and finally send it to the base station. It comprises of spatially distributed self autonomous sensor devices to monitor the environmental conditions and RFID systems are used to track the location, movement and temperature. WSN approaches multi hop

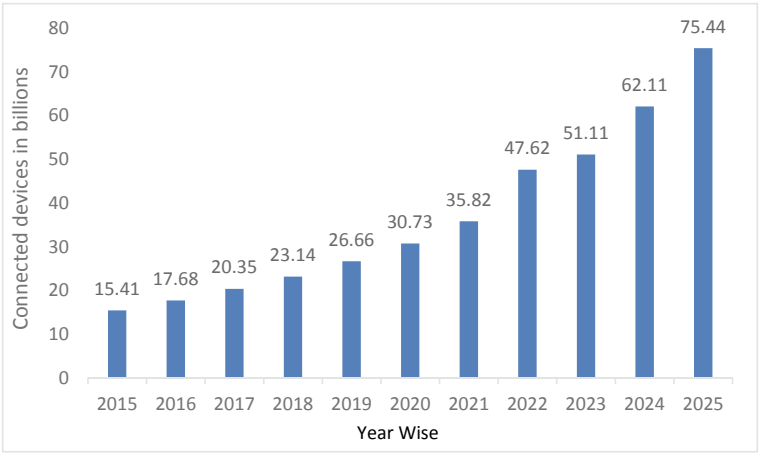


Fig. 5.4 No of devices connected to the internet

communication and different network topologies. The recent technological advancement in low power integrated circuits have made available low-cost, efficient, low power miniaturized devices to be utilized in WSN applications [17, 18]. WSN is primarily being preferable in logistics for efficient transportation of temperature sensitive products. It is also used for maintenance and tracking systems, for instance, General Electric (GE) deployed sensors in turbines, jet engines and wind farms. GE incurs less time and money by analyzing data in real time. Wireless Sensor Network (WSN) is the primary real-time application of ubiquitous computing and it bridges the gap between the physical and the digital world by offering scalable, reliable, accurate monitoring and fault tolerant of the physical phenomenon [14]. It is an intelligent distributed sensor network provides wide range of applications in both civilian as well as military domains linked via wireless links. WSN comprises of low-power, spatially distributed, low-cost and autonomous sensors with base stations to monitor the physical or environmental conditions such as temperature, pressure, motion or sound. The wireless sensor nodes are energy-constrained, battery powered. The sensed data would be communicated for assessing and self-organized after deploying. The sensor devices are low-powered consists of microcontroller for transforming the data, a microchip and senses ecological components such as light quality, dampness, heat range, etc. WSNs are useful in a great variety of application domains such as surveillance, intrusion detection, structural monitoring, ecosystem monitoring (e.g. for earthquake and fire prevention), localization of objects or animals, intelligence detection of ambient conditions such as weather or sea, medical monitoring and emergency operation like disaster relief.

- Middleware: It is a layer acts as an interface between software applications to perform input/output and communication process. The significant feature of this layer is hiding the technological details in order to provide software services that

are not directly relevant to any specific IoT application. It facilitates the new type of services in the distributed computing environment. The Global Sensor Network (GSN) is a sensor based open source middleware platform enables sensor services with zero programming effort. A service oriented approach is followed in IoT middleware architectures that support dynamic network topology.

- Cloud computing: It is an on-demand access model with the shared storage of configurable resources such as networks, server, computers, storage, applications, software, services, etc., that is provisioned as Software as a Service (SaaS) or Infrastructure as a Service (IaaS). The most significant outcome of IoT is the huge amount of data generated from the devices connected to the Internet. Several IoT applications are in need of enormous amount of data storage, processing speed which enables high-speed broadband networks for streaming audio, video, or data that paves a way for efficient real-time decision making [11, 12, 19, 20]. It is acting as a perfect back-end for handling massive data streams with unpredictable count of IoT devices in real time.
- IoT applications: It enables human-to-device and device-to-device communication in a reliable as well as robust manner. IoT devices facilitate the development of user specific applications and ensure the effective communication occurred in a timely manner. For instance, in transportation and logistics applications the condition of transported goods such as dairy products, meat, fresh-cut produce, and fruits are monitored. The conservation status such as humidity, temperature etc. are tracked continuously to take appropriate actions automatically in order to avoid spoilage if the condition is out of range. Sense Aware is used in FedEx to track the location, temperature, and other important signs such as whether the package is tampered or opened on the way. Human centered IoT applications present information in an intuitive way that allows smooth interaction for end users with the environment. Moreover, IoT devices with its intelligence track the environment continuously, identify problems, allows communication among users, and problems are resolved without any human intervention [21].

5.3 Wireless Body Area Network (WBAN) in IoT Paradigm

IoT is a fast growing technological paradigm which connects things from several fields through the internet. In IoT based healthcare applications, the Wireless Body Area Network (WBAN) gains popularity as wearable devices which turns attention of many users [10]. The multiple sensor nodes are deployed in different locations of the human body to measure the heartbeat, body temperature, distribution etc. Wearable sensor devices can be deployed to monitor the health condition around the human body such as in safety application. Wearable sensor systems could provide the useful

information about the impact on patient's health. The users' can gain a deep understanding of the local environment. A wearable system can be installed on a car, bicycle, and animal to build a wearable wireless sensor networks. For instance, a sensor node can be installed on a bicycle to track the environment. WBAN consists of heterogeneous nodes that can be attached to the human body in order to provide a variety of services. Body Area Network (BAN) is the network which handles immense amount of heterogeneous data with complex relationship. The sensor nodes attached to the human body that is connected to a local or wide area network for providing remote services to the users [10, 22–24].

WBAN is characterized by IEEE 802.15 communication standard for miniaturized devices attached to the human body. A WBAN interfaces communicate with the hubs using a local controller. Data gathered via BAN plays a significant role in the patient care process. It is mandatory to maintain the high standard quality data for efficient decision making. BAN generates massive amount of data, managing such a huge dataset is highly challenging. The sensing devices are subjected to hardware constraints and inherent communication including unreliable network links, limited power and interferences. The complete sensor readings in healthcare domain should be compulsorily validated in terms of reducing false alarm generation. The data available in multiple devices need to be gathered and analyzed effectively in a seamless fashion. In BAN, the most significant patient datasets could be fragmented across many laptops or PCs. If adequate patient related information is not available in medical practitioner's mobile device, then the quality will be automatically degraded in healthcare system. WBAN is a self-organizing network which consists of heterogeneous devices that are miniaturized, low-power, hardware constraint (limited storage capability and processing) and fixed (or implanted) to a human body. Sensors attached to the human body gather signals about the physiological signs (temperature, heartbeat), movement (orientation, acceleration), environment (toxic gases, temperature) [17, 25].

Wearable devices can be attached on the human body such as smart rings, watches, T-shirts, badges, pendants, glasses, bracelets, fitness trackers, and any other accessories as many users are gaining health benefits. A wearable device that is kept closer with the user is able to monitor the wellness, health of a person and collected data would be transmitted to the central hub station for analysis. Some of the wearable devices are shown in Fig. 5.5.

Wearable devices comprise of three main components such as sensor devices, computing architecture and display unit. The sensor devices gather data in an aggregate form about the particular user; the collected data is computed and displays the information that helps in making decision. The gadgets accomplish some basic functionality and provide various biological information to the users such as blood pressure, heart-rate, steps walked, and calories burned, and time- spent on exercising etc. The impact of such devices is quite extensive, powerful and gain more attraction in monitoring physical health. The main drawback of these wearable devices is regarding the potential of interpreting massive amount of information that is generated. Once the information generated is interpreted well, then the strength of wearable's becomes extremely effective.

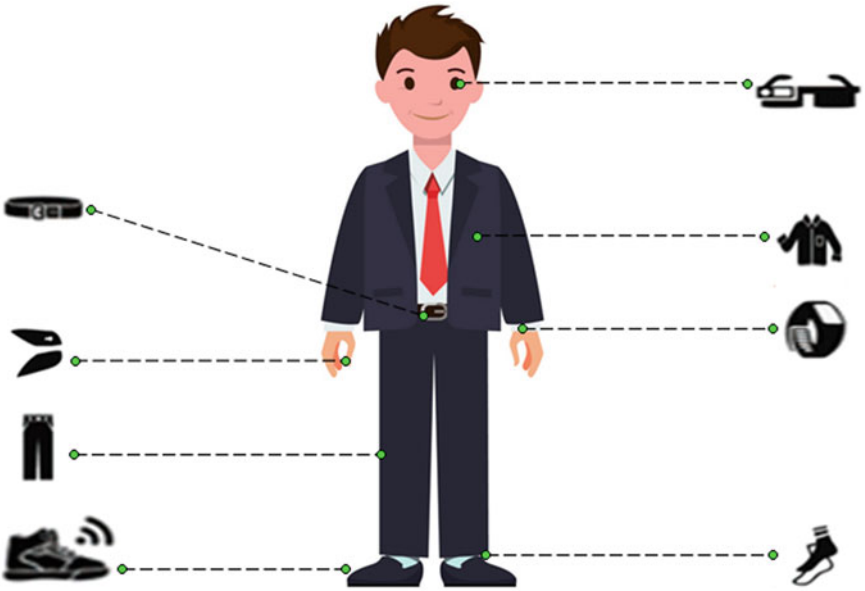


Fig. 5.5 Wearable devices

Wearable technology plays a significant role in several domains of daily life such as sports and fitness, augmented reality, healthcare (monitor the physiological signals), localization and many more. Wearable systems are envisioned for many potential applications such as rescue management as well as workers safety. It also plays a vital role in saving human lives and protecting valuable assets. Typically, wearable solutions are based on various standards such as Bluetooth (IEEE 802.15.1), Wi-Fi (IEEE 802.11a, IEEE 802.11b, IEEE 802.11 g), and zigbee (IEEE 802.15.4, IEEE 802.15.4a, IEEE 802.15.4j). IEEE 802.15.6 standard is designed specifically for wearable applications and their design requirements. To meet the design constraints of different applications, some of the below-mentioned key features of Medium Access Control (MAC) layer of IEEE 802.15.6 standard are focused for analysis.

- Reliability
- Quality-of-service
- Energy efficiency
- Data transmission rate.

5.3.1 History of Wearable Sensors

In the year 1960s, there is a need to check the astronaut health when they are in space. This paves the way to develop wearable sensors which transmits the data back to earth from space craft. In the late 80s, the general people came to know the importance of wearable sensors. In the year 1977, the Finnish National Cross-Country Ski team has developed a Wireless electrocardiogram (EKG) contributed by Prof. Seppo Säynäjäkangas to monitor the health of heart. The reach of this machine shed light on the production of wearable devices and the invention of Sport Tester PE2000, pulse oximeter is made. In the year 2002, Cygnus introduced GlucoWatch, which uses 2 gel pads over the skin [26]. Wearable Sensors are the devices used to sense or detect various physical quantities from the surroundings. The sensed input may be moisture, light, motion, heat, vibration, pressure etc. The output signal is send out through a network for further procedure. The sensors are classified depending upon the types of input. In this era, wearable sensors play a vital role in the form of smart wrist watch, medical patches, smart clothing etc. Wearable sensors can be categorized based on configuration, sensing method, power and data, sensing function and it is shown in Fig. 5.6.

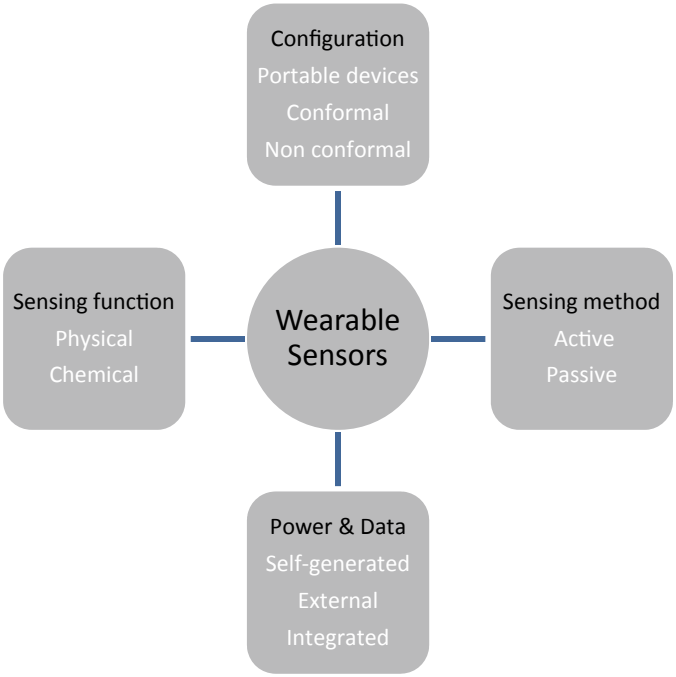


Fig. 5.6 Conceptual categorization of wearable sensors

5.3.2 Wearable Sensors in Healthcare

Physiological measurements include the respiratory rate, heart rate, muscle activity, blood oxygen saturation and blood pressure provides the indication of health status with diagnostic value. In the recent past, the continuous monitoring of physiological parameters is done in hospitals. In contrast to this, today with the help of technological advancement researchers has developed wearable sensors for accurate real time monitoring of physiological activities through signals.

5.3.2.1 Gyroscope and Accelerometer

Gyroscope measures angular velocity which is applicable for navigation purposes as it involves rotation and orientation. Accelerometer tracks human movement like inclination, tilt and overall orientation of the body. The accelerometer is often paired with gyroscope to produce 3D representation of movements involved during workout.

5.3.2.2 Altimeter

This type of indispensable sensors plays a major role in designing wearable devices required for mountain climbers to measure the altitude.

5.3.2.3 Proximity Sensor

Proximity sensor is used to find a particular nearby subject varies from non-living objects to human being. The designer should estimate the beam width or distance to design a wearable device. This sensor is used to detect obstacles or metal objects in the industrial setup.

5.3.2.4 Physical Sensors

Physical sensor is used to sense physical factors like pressure, strain and temperature. The factors monitored by the Physical sensor indicate the condition of blood pressure, skin and body temperature, skin strain and pulse rate.

5.3.2.5 Optical Sensors

Optical sensors convert light energy into electronic signals and it measures the physical quantity of light, transforms it into readable form by the instrument.

It works both in distributions of points and in single point. In distribution method, the sensor is reactive along single fiberoptic array or acts as a long series of sensors. In single point, a single change in phase is required to activate the sensor. Optical sensor proves its dominance in many applications ranging from medico technologies and remote sensing. Many types of optical sensors are available using novel manufacturing materials such as nano, micro and meta material. The advantages of optical sensors are electrical passiveness, high sensitivity, wide range dynamic, multiplexing capabilities and independent of Electromagnetic interference.

5.3.2.6 Temperature Sensors

A temperature sensor is a device that detects and measures hotness and coolness and converts it into an electrical signal. Temperature is the major parameter related to biological, chemical, physical, electronic and environmental systems. Wearable temperature sensors application ranges from food safety, electronic skins, environmental temperature measurement and human–machine interface and robot sensors [27–30]. Some of the temperature sensors are thermo resistance temperature sensors [31], thermocouple sensors [32], and thermal responsive field-effect transistor [33]. The global temperature increases rapidly and now it is necessary to choose the clothes to wear depending upon the climate change. These temperature sensors analyses the body temperature and inform the users what to wear. Wearable basal body thermometers act as fertility indicator by tracking the ovulation cycle of women with the aid of basal body temperature. This sensor can be integrated to a smart mobile phone app to indicate the chances of getting conceive.

5.3.2.7 Pressure Sensor

A pressure sensor is a device that senses pressure and converts it into an electric signal where the amount depends upon the pressure applied. In early days, a device called sphygmograph was dedicated to measure blood pressure. The later device is the cuff based diagnostic tool to monitor the blood pressure. However, these devices are used to measure the diastolic and systolic pressures only and it cannot monitor continuously. The materials used in making the pressure sensors are gold nanowires [34], polymer transistors [35] and piezoelectric materials [36]. Pressure sensors with light weight, high flexibility, good workability and high sensitivity are highly needed in health monitoring devices [37].

5.3.2.8 Force Sensors

Palo Alto Research Center, Impact Measurement and the Stanford Tae-kwondo Program has jointly developed a force sensor for martial arts sparring ring.

5.3.2.9 Humidity Sensor

A humidity sensor or hygrometer is a device that detects and measures water vapour. The ratio of air moisture to the highest amount of moisture at a particular air temperature is often called relative humidity. Humidity sensors work by detecting changes that alter electrical currents or temperature in the air. There are three basic types of humidity sensors, namely

1. Capacitive
2. Resistive
3. Thermal.

Humidity sensor is found as a part of air conditioning systems, home heating and ventilating system.

5.3.2.10 Piezoelectric Sensors

Sensors which follows the concept of piezoelectricity is called piezoelectric sensor, in which when mechanical stress is applied to a material it produces electricity. The types of piezoelectric sensors are Flow sensors, Level sensors and Accelerometers. Piezoelectric sensors play a vital role in wearable technology. The invention of piezoelectric pacemaker makes lot of notable changes in the heart health. It works by the rhythm of the heart beat thus eliminates the urge of complicated surgery to replace battery. Piezoelectric sensors can be placed under the vehicle seat of the driver to monitor the respiration and heart rate. Piezoelectric blood pressure cuffs monitor the blood pressure via phone app. Smart fabric is made by embedding piezoelectric sensors to monitor measure and harvest energy. Piezoelectric sensors are used in shoes to measure the step counts and pressure.

5.3.2.11 Wearable Electrodes

Human heart rate is read by electrodes using the electric pulses by sticking the electrodes directly onto the skin. An electrode in the wearable device is used in devices like Electrocardiogram (EKG), Electroencephalogram (EEG) and Electromyography (EMG). These electrodes can be embedded into clothes to measure various parameters and it can be washed without removing the sensors.

5.3.2.12 Biochemical Sensors

Biochemical Sensors in a wearable device converts chemicals into electric signal. It works on the principle of chemical resistive detection in a wearable configuration. In wearable devices these sensors monitors EtG (ethyl glucuronide) through human sweat to measure the metabolic rate. It is also used to find the amount of alcohol consumption.

5.4 Wearable Wireless Sensor Networks

Wireless Sensor Networks is a network with self-organizing capability. It accommodates smart devices with miniature hardware and low power constraint. Sensors are connected on the human body to collect movement and physiological signs. Wearable Wireless Sensor Networks has many applications in the field of sports, healthcare, ambient intelligence, fashion, augmented reality and localization. Wearable Wireless Sensor Networks standards are Bluetooth, Wifi and zigbee [38]. The designing of Wireless Sensor Networks should follow the designing strategies like quality-of-service, reliability, energy efficiency and data transmission rate. The application layer governs the communication stack which handles packet transmission rate, the traffic patterns and the network topology. Other important building blocks in the Wireless Sensor Networks designs are feasible medium access, selection of appropriate routing strategies, security, privacy and mobility modeling [18].

The requirements for different applications are data rate, traffic patterns, sensor devices and its types, miniaturization etc. In healthcare systems, vital sign, EEG or ECG and the coordinating node should be enough powerful to obtain an access to the nearby access point. In particular, for remote monitoring system, the coordinator node should be capable of supporting various standard and functionalities with less battery constraints. In terms of games, sports and fitness, few specific sensors such as heartbeat, gyroscope, sweat, accelerometer etc. are used that can operate stand-alone without any intervention of any external communications. Some critical applications require reliability, better QoS and adequate resources.

In some systems, on-body and off-body communications are essential that append various constraints and requirements. For instance, few sensors are generally used to track the orientation, health and movement of fire fighters. Some requirements which are common to many applications are shown in Table 5.1 with various parameters and their requirements. Table 5.2 shows the comparison of various IEEE standards of wearable wireless sensor network.

Table 5.1 Parameters and requirements for BAN applications

Parameters	Requirements
Devices used	Sensors, actuators, smart phones, base station
Sensor types	Vital signs: Breath rate/Heart beat, sweat, stress, oxygen saturation, temperature, blood pressure, glucose level Body movement: Fall detection, acceleration, orientation Environment: Humidity, heat, pressure, carbonic gases, light intensity
Traffic type	Audio, video, raw data, encoded data
Traffic pattern	Periodic, event driven, burst traffic
System co-ordination	Centralized (intra-BAN) Distributed (inter-BAN
Location awareness	Absolute/relative

Table 5.2 Comparison of IEEE standards for wearable WSN

	IEEE 802.11 a/b/g/n (Wi-Fi)	IEEE 802.15.1 (Bluetooth)	IEEE 802.15.1 (Bluetooth-LE)	IEEE 802.15.4 (Zigbee)	IEEE 802.15.6 (WBAN)
Modes of operation	Ad hoc	Ad hoc	Ad hoc	Ad hoc	Ad hoc
Power consumption	High	Medium	Low	Low	Ultra low
Network topology	Infrastructure based	Ad hoc (small networks)	Ad hoc (small networks)	Ad hoc, Peer-to-peer, Star, Mesh	Intra-BAN, Inter-BAN, ½-hop star
Target applications	Data networks	Voice links	Healthcare, fitness	Sensor network, home automation	Body-centric
BAN architectures	Off-body	On-body	On-body	On-body, Off-body	On-body

5.5 Global Wearable Sensors Market Share

The chart shows the global wearable sensors market share by 2020 and it is shown in Fig. 5.7.

5.5.1 Sensor Deployment Strategies

IoT along with WSN has made the major foundation for an incredible growth of smart and sustainable cities. The self organized distributed nature of WSN with low-power autonomous nodes has envisioned the formation of novel solutions which cover multi-disciplinary domains such as telecommunications, embedded computing architecture, industrial technologies and microelectronics [39, 40].

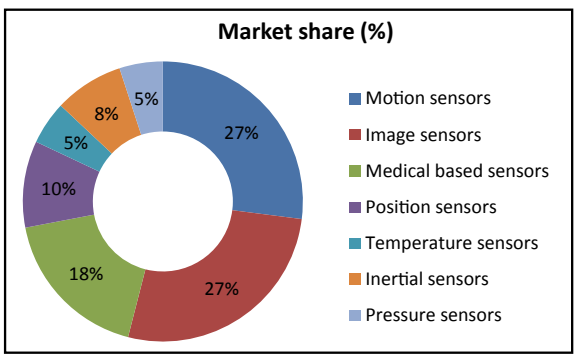


Fig. 5.7 Global wearable sensors market share, by Type, 2020 (%)

The system design optimization can be done in different contributions such as radio propagation, power awareness, sensor coverage, embedded software capabilities and hardware cost. The deployment techniques for WSN turn the researcher's attention towards random strategies in which uniform, non-uniform and grid distributions are converged with coverage optimization analysis in order to balance/maximize the network connectivity.

5.5.2 *Design Issues in Deployment Strategies*

The various design issues related to Wireless Sensor Networks have been addressed [41, 42].

Reliability:

The reliability can be checked out on the basis of packet/event and end-to-end/hop-to-hop level. Wireless medium is highly prone to error; the surety of solid exchange of information is not assured among sensor nodes. Packet dependability guarantees that all the packets transmit sensed information which is gathered from the sensor nodes to the sink node [15, 16, 43]. Event dependability ensures that the sensed information gathered from the sensor nodes will be conveyed to the sink node and it accumulates the adequate data around a particular event. In hop-by-hop methodology, the next hop ensures the reliable transmission whereas end points are responsible for the successful data transmission in end-to-end reliability.

Density and network size: The network size affects accuracy, reliability and data processing algorithms. The density of the network starts from less number of nodes to huge number of sensor nodes and it is calculated by considering the amount of scattered sensor nodes in the transmission range [44, 45].

Sensor network topology: The sensor network topology determines the capacity, robustness, and latency. The sensor hubs define the three phases related to topological changes and maintenance:

1. Pre-deployment
2. Post-deployment
3. Redeployment.

Energy consumption: The lifetime of a sensor node is completely dependent on battery life-time and it plays a vital role on the strength of sensor node and energy effectiveness; recharging power sources are difficult in some critical situations. The main objective of sensor hubs is sensing data, information handling and transmission (Sensing, computation, communication). The researcher's attention turns the investigation on power aware protocols with the objective of minimizing the energy utilization [46, 47].

Hardware Constraints: The sensor hub contains several parts such as radio transceiver, storage space, implanted processor, and sensors. The sensor nodes transmit the gathered data to a CPU for processing.

Data aggregation: This method assists in reducing the amount of message that is being transmitted and the distributed data in different messages will be aggregated together to form as a single message. In most of the sensor network applications, the constant rate of data supply is required. Hence, the quality of service is considerably affected by huge amount of data loss.

Transmission media: A wireless transmission medium is used in multi-hop sensor network for connecting nodes which enables communication among sensor nodes. The connections may be provided using Bluetooth, infrared and optical medium.

Quality of Service: The data should be delivered within a bounded latency otherwise it is of no use in many applications. The conservation of energy in sensor network is actually required when compared to the quality of delivered data. Hence, there is a trade-off between the energy conservation and quality of service according to the desired purposes.

Coverage: The capability of sensor nodes relies in the coverage area of the environment though it is limited in range and accuracy [45].

Connectivity: The connectivity is a significant factor since it has a huge impact on communication protocols and data dissemination techniques. The permanent link exists among two sensor nodes that define the actual network connectivity in the sensor network [16, 48].

5.5.3 Sensor Node Deployment Models

Sensor network is capable of monitoring the real-world phenomena at a large scale and embeds the sensor nodes of wireless network in the real world. Deployment is concerned about the set-up process of an operational sensor network in the real world [48, 49]. Deployment is cumbersome and labor-intensive as bugs may be triggered or the performance is degraded that was not observed at the time pre-deployment. The real world has an influence on the functionality of sensor network by influencing the quality of communication links, tracking the output of sensors, and by having physical strain on wireless sensor nodes. Deploying sensors by covering the complete area is considered as a design problem in various WSN applications. The three common deployment approaches are random deployment, deterministic deployment and grid (pattern) based deployment [50, 51]. Deterministic deployment is suitable for small-scale applications because of deliberate location of sensors. Non-deterministic deployment is commonly suitable for large-scale applications.

- Random deployment: It is quite challenging to locate the spot for each device since there is no prior configuration in randomized sensor deployment. In uniform random deployment, the ‘n’ number of sensors has an opportunity to place the sensor node at any point in a given field. WSN applications prefer uniform random method because of ease deployment and cost-effective.

Post self-deployment strategies obtain the desired connectivity and coverage [40, 52, 53, 54, 55]. The parameters that can be considered in uniform random deployment are the number of nodes and transmission range.

- Grid Deployment: The most popular grid layouts followed in grid deployment are a unit square, triangle, hexagon etc. Grid deployment [40, 52, 53, 54, 55] is suitable for several WSN applications due to its coverage performance. This kind of deployment is performed by placing sensors row-by-row based on moving carrier. The time interval is maintained between consecutive droppings to obtain the desired distance. However, this deployment model is not ideal because of placement errors. In unreliable grid model, if n nodes are spotted on a square grid with certain probability where the nodes are active in the defined transmission range. Scalability is a challenging issue if location constraints are rigid where nodes can or cannot be spotted for a given environment. If the number of nodes is less according to the operational coverage area size, then the number of routing and sensing nodes should be optimized.

On-site deployment optimization

The set-up mode of sensor nodes considers communication mechanisms and platform parameterization (hardware/software) by triggering a configuration procedure from the on-site deployment tool [56]. The target node performs two main actions by executing the frame dissemination task at the MAC layer,

(i) Network connectivity adaption with the surrounding environment (permits bidirectional routing).
(ii) Platform setup parameters (service provision, data transmission rate mask, power mode configuration, synchronization) and node properties (cluster based configuration entries, node weight) are distributed in the specified area.

5.6 Data Acquisition and Localization in Sensor Networks

Data acquisition with IoT gathers data from various kinds of devices/ objects and shared with multiple devices for processing in several IoT applications [57–59]. The reliable and efficient data aggregation techniques generally increase the network lifetime using appropriate sensors. The data acquisition process is facilitated in different technologies that consist of sensors, actuators, camera, RFID, GPS etc. The short-range communications enables information sharing among heterogeneous devices in IoT environment. IoT devices cover a wide range of applications across the globe, such as agriculture, transportation, healthcare, market, industry, smart school, smart home, smart city etc.

The information about the particular location is significant to know the current situation. Localization in WSN is the process of determining the location of unknown network sensor nodes. Localization plays role in many practical applications by determining the location of patients, equipments or personnel in a

hospital, swarm of robots work together toward a common goal. GPS is the straightforward solution for localization but it is not suitable for all applications. Router communicates the identity of its location and it can be realized using the two most significant bits of one byte data structure. The following possibilities are enabled: indoor and outdoor in a public area, personal indoor area, restricted area.

In indoor systems, there is no direct connection from GPS signal to satellites. However, there are obstacles in many situations where it blocks the direct communication with the GPS satellites in outdoor systems. Some other issues of GPS in WSN nodes are cost, size, and power consumption. Moreover, in various WSN applications, the localization problem is solved using network parameters, features of the received radio signal and location of fixed nodes (known as anchors or beacons). The localization problem is categorized into two levels:

i. Distance between two nodes are estimated
ii. Location of all unknown nodes is determined.

Distance estimation: There are several techniques available for distance estimation problem and the criteria for comparing the methods are: computational power, position accuracy and precision, robustness, hardware requirements.

Position accuracy: It shows that the estimated position is close to the real position using a particular technique. In fact, higher the accuracy leads to better quality of localization. Position precision determines that how the system works consistently and how frequently the accuracy is achieved.

Computational power: It refers the computational requirements of algorithms used for localization. It is considered as a significant metric, because it has an impact of the power consumption of the node. Clearly, lower the computational power, better the performance.

Hardware requirement: It indicates that the localization technique is in need of hardware features. For example, directional or multiple antennas are the requirements which have an impact of size and cost.

Robustness: It refers that how the system functions if input parameters do not exist or values are corrupted. The data gathered from the sensor node is processed to avoid data duplication and save limited resources. The steps involved in data processing are data aggregation and fusion. In data aggregation, network delay is minimized because of self-adaptive mechanism [60–62].

5.7 Open Research Issues and Challenges in IoT

IoT will face multiple challenges for adopting with several enterprises. According to Gartner report, due to the creation of enormous amount of data by IoT machines, data centers is the storage pool which would face challenges in consumer privacy, storage management, security, enterprise, server technologies and network communication [13].

Data vulnerability: The sensor devices connected with internet are highly vulnerable to various potential risks. Every sensor device should have the control in order to preserve confidentiality of gathered data and integrity of the data that is transmitted.

Data management: IoT sensors are generating huge amount of data that is to be processed and stored for further processing. The data center which is currently available is not efficient in handling heterogeneous data retrieved from different sources. Data centers would become more distributed in terms of improving response time and processing efficiency as IoT devices are widely used nowadays and consume lot of bandwidth. Massive amount of data is available for further processing and analysis, the preference of utilizing data mining tools becomes mandatory. The streamed data are about temperature, humidity, location, vibration, movement, and chemical changes in the air. The data mining tools invoke the correct action for the operational issues or the concerned authorities will be intimated in case of competitor's strategies steps and the preference of customer's will have an impact of both short and long term business activities.

Data privacy: The vision of IoT makes the people's everyday life easy and increases the efficiency of employees and productivity of businesses. The streamed data which is gathered assist in making smarter decisions and have a high impact on privacy expectation also. Suppose the data gathered from the connected devices is compromised, then the trust level of IoT will be decreased. In smart health equipment, IoT devices provide massive amount of data on IoT user's movement, location, purchasing preferences, health conditions, etc.—it is all about privacy concern. Preserving privacy is considered as counter-productive in the aspect of service providers, hence there is a trade-off between the quality of people's lives and service providers cost. According to TRUSTe IoT privacy index, 22% of internet users consented that the benefits outweighed the privacy concerns. With the wearable devices and smart home systems, IoT gains confidence whereas it highly depends on user's privacy protection.

Cloud attacks, security issues and botnet problems: The immense amount of IoT devices generated data is stored in the cloud and there is a growing awareness of cyber security is necessary to defend against the potential scale of threat. For ransomware attack, the magnitude of threat has grown 35 times larger since the last year and other types of attacks are also yet to arrive. As a growing number of heterogeneous connected devices in IoT networks, the potential threats escalate exponentially. IoT applications support strategic services and sensitive infra-structures such as smart grid, facility protection in terms of privacy concern. IoT botnet directs massive swarm of connected devices like sprinkler controllers or thermostats cause unexpected spikes and severe damage in infrastructure usage which leads to destructive water hammer attack, power surges, minimized the availability level of infrastructure on a city or state level. Solutions do exist for these types of attacks; the software can categorize the emergent and erroneous data and there is a boundary on which devices are allowed to transmit the data and how often they can transmit. Securing sensor devices is highly challenging especially when they are connected with the shared infrastructure.

In upcoming years, the real issue lies on making people to understand the updations and implications clearly and to proceed with corrective actions for the benefit of potential upside. IoT as connected devices become smarter day-by-day and expectations are increased to gain deep insight for financial value increase in IoT data. Algorithms and visualization techniques are also evolved so that the future use-cases can have the benefit of older ones. The exponential growth of IoT will bring down sensor device and acquisition costs that enable more viable business cases which were too expensive earlier.

References

1. Guinard, D., Trifa, V., Wilde, E.: A resource oriented architecture for the web of things. In: Proc. Internet Things (IOT), pp. 1–8 (2010)
2. Tan, L., Wang, N.: Future internet: the internet of things. In: Proceeding 3rd International Conference on Advanced Computer Theory and Engineering, vol. 5. pp. V5–376–V5-380 (2010)
3. Pang, Z.: Technologies and architectures of the Internet-of-Things (IoT) for health and well-being. M.S. thesis, Dept. Electron. Comput. Syst., KTH-Roy. Inst. Technol., Stockholm, Sweden (2013)
4. Höller, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S., Boyle, D.: From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Elsevier, Amsterdam, The Netherlands (2014)
5. Kortuem, G., Kawsar, F., Fitton, D., Sundramoorthy, V.: Smart objects as building blocks for the Internet of Things. IEEE Internet Comput. **14**(1), 44–51 (2010)
6. Romer, K., Ostermaier, B., Mattern, F., Fahrmair, M., Kellerer, W.: Real-time search for real-world entities: a survey. Proc. IEEE **98**(11), 1887–1902 (2010)
7. Zhao, F., Guibas, L.: Wireless Sensor Networks: An Information Processing Approach, pp. 240–245. Morgan Kaufmann, Los Altos, CA, USA (2004)
8. Jaradat, M., Jarrah, M., Bousselham, A., Jararweh, Y., Al-Ayyouba, M.: The internet of energy: smart sensor networks and big data management for smart grid. Procedia Comput. Sci. **56**:592–597
9. Jangili, S., Bikshalu, K.: Smart grid administration using big data and wireless sensor networks. Int. J. Adv. Res. Sci. Eng. **6**, 629–636 (2017)
10. Otto, C., Milenkovic, A., Sanders, C., Jovanov, E.: System architecture of a wireless body area sensor network for ubiquitous health monitoring. JMM **1**, 307–326 (2006)
11. Komalavalli, C.: Convergence of wireless sensor networks, internet of things, big data: challenges. Int. J. Sci. Res. Eng. & Technol. (IJSRET), **6**(6) (2017). ISSN 2278–0882
12. Sezer, O., Dogdu, E., Ozbayoglu, A.: Context-aware computing, learning, and big data in internet of things: a survey. IEEE Internet Things J. **5**:1–27 (2018)
13. Qian, L., Zhu, J., Zhang, S.: Survey of wireless big data. J. Commun. Inf. Netw. **2**(1), 1–18 (2017)
14. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Network J. Elsevier (2010)
15. Romer, K., Mattern, F.: The design space of wireless sensor networks. IEEE Wirel. Commun. **6**, 11–54 (2004)
16. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Networks **38**, 393–422 (2002)
17. Martelli, F., Verdone, R.: Coexistence issues for wireless body area networks at 2.45 ghz. In: 18th European Wireless Conference (EW) (2012)

18. Xiao, F., Zhang, C., Han, Z.: Editorial: big data in ubiquitous wireless sensor networks. Int. J. Distrib. Sens. Netw. (2014)
19. Rios, L., Diguez, J.: Big data infrastructure for analyzing data generated by wireless sensor networks. In: Proceedings of the IEEE International Congress on Big Data, Anchorage, AK, USA, 27 June to 2 July 2014, pp. 816–823 (2014)
20. Song, C.: A novel wireless sensor network architecture based on cloud computing and big data. Int. J. Online Eng. **13**, 18–25 (2017)
21. Gonzalez-Jaramillo, V.: Tutorial: internet of things and the upcoming wireless sensor networks related with the use of big data in mapping services; issues of smart cities. In: Proceedings of the International Conference on eDemocracy & eGovernment, Sangolqui, Ecuador, 30 March to 1 April 2016 (2016)
22. Poon, C., Lo, B., Yuce, M., Alomainy, A., Hao, Y.: Body sensor networks: in the era of big data and beyond. IEEE Reviews in Biomed. Eng. **8**, 4–16 (2015)
23. Du, Y., Hu, F., Wang, L., Wang, F. (2015). Framework and challenges for wireless body area networks based on big data. In: Proceedings of the IEEE International Conference on Digital Signal Processing, Singapore, 21–24 July 2015
24. Jovanov, E., Milenkovic, A., Otto, C., de Groen, P.: A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. J. Neuroeng. Rehabil **1**, 2–6 (2005)
25. Watteyne, T., Augé-Blum, I., Dohler, M., Barthel, D.: AnyBody: a self-organization protocol for body area networks. In: ICST 2nd International Conference on Body Area Networks BodyNet (2007)
26. Cunningham, D.D.: In Vivo Glucose Sensing, pp. 191–215. Wiley, Hoboken, NJ, USA (2010)
27. Webb, R.C., Bonifas, A.P., Behnaz, A., Zhang, Y., Yu, K.J., Cheng, H., Shi, M., Bian, Z., Liu, Z., Kim, Y.-S., Yeo, W.-H., Park, J. S., Song, J., Li, Y., Huang, Y., Gorbach, A.M., Rogers, J.A.: Nat. Mater. **12**, 938–944 (2013)
28. Hammock, M.L., Chortos, A., Tee, B.C.K., Tok, J.B.H., Bao, Z.A.: Adv. Mater. **25**, 5997–6037 (2013)
29. Nguyen Thanh, T., Jeon, S., Kim, D.-I., Tran Quang, T., Jang, M., Hwang, B.-U., Byun, K.-E., Bae, J., Lee, E., Tok, J.B.H., Bao, Z., Lee, N.-E., Park, J.-J.: Adv. Mater. **26**, 796–804 (2014)
30. Someya, T., Kato, Y., Sekitani, T., Iba, S., Noguchi, Y., Murase, Y., Kawaguchi, H., Sakurai, T.: Proc. Natl. Acad. Sci. U. S. A. **102**, 12321–12325 (2005)
31. Moser, Y., Gijs, M.A.: J. Microelectromechanical Syst. **16**, 1349–1354 (2007)
32. Kim, T. H., Kim, S. J.: J. Micromechanics Microengineering **16**, 2502–2508 (2006)
33. Ren, X. C., Chan, P.K.L., Lu, J.B., Huang, B.L., Leung, D.C.W.: Adv. Mater. **25**, 1291–1295 (2013)
34. Gong, S., Schwalb, W., Wang, Y., Chen, Y., Tang Y., Si, J., Shirinzadeh, B., Cheng, W.: A wearable and highly sensitive pressure sensor with ultrathin gold nanowires. Nat. Commun. (2014)
35. Schwartz, G., Tee, B.C.K., Mei, J., Appleton, A.L., Kim, D.H., Wang, H., Bao, Z.: Flexible polymer transistors with high pressure sensitivity for application in electronic skin and health monitoring. Nat. Commun. (2013)
36. Dagdeviren, C., Su, Y., Joe, P., Yona, R., Liu, Y., Kim, Y.S., Huang, Y., Damadoran, A.R., Xia, J., Martin, L.W., Huang, Y., Rogers, J.A.: Conformable amplified lead zirconate titanate sensors with enhanced piezoelectric response for cutaneous pressure monitoring. Nat. Commun. (2014)
37. Zang, Y., Zhang, F., Di, C.A., Zhu, D.: Advances of flexible pressure sensors toward artificial intelligence and health care applications. Mater. Horiz. **2**, 140–156 (2015)
38. http://www.wearable-technologies.com/, [Online]. Available: http://www.wearabletechnologies.com/2015/01/meet-the-wt-wearable-technologies-heroes-of-the-year/

39. Pham, H.N., Pediaditakis, D., Boulis, A.: From simulation to real deployments inWSN and back. In: IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'07), 18–21 June 2007, pp. 1–6
40. Li, J., Bai, Y., Ji, H., Ma, J., Tian, Y., Qian, D.: POWER: planning and deployment platform for wireless sensor networks. In: Proceedings of the Fifth International Conference on Grid and Cooperative Computing Workshops (GCCW 06), IEEE (2006)
41. Halde, S., Khot, S.: Big data in wireless sensor network: issues and challenges. Int. J. Adv. Eng., Manag. Sci. (IJAEMS) **2**(9):1618–1621 (2016)
42. Harb, H., Idrees, A., Jaber, A., Makhoul, A., Zahwe, O., Taam, M.: Wireless sensor networks: a big data source in internet of things. Int. J. Sens. Wirel. Commun. Control. **7**, 141–149 (2017)
43. Stankovic, J.A.; Abdelzaher, T.E., Lu, C., Sha, L., Hou, J.C.: Real-time communication and coordination in embedded sensor networks. Proc. IEEE 2003, **91**, 1002–1022 (2003)
44. Sheldon, M., Chen, D., Nixon, M., Mok, A.K.: A practical approach to deploy large scale wireless sensor networks. Proc. IEEE MASS, Washington, DC (November 2005)
45. Cardone, G., Bellavista, P., Corradi, A., Foschini, L.: Effective collaborative monitoring in smart cities: convergingMANET and WSN for fast data collection. In: Kaleidoscope 2011: The Fully Networked Human? Innovations for Future Networks and Services, pp. 1–8 (2011)
46. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocols for wireless microsensor networks. In: Proceedings of the 37th Annual Hawaii International Conference, pp. 1–10 (2000)
47. Kalantari, M., Shayman, M.: Design optimization of multi-sink sensor networks by analogy to electrostatic theory. In: Proc. IEEE Wireless Comm. and Networking Conf. (WCNC), pp. 431–438 (2006)
48. Wang, Y., Kelly, B.M., Li. X.: On the network connectivity of wireless sensor networks following a random and non-uniform distribution. In: IEEE 9th Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'13), 7–9 Oct 2013, pp. 69–74 (2013)
49. Chatterjee, P., Das, N.: Coverage constrained non-uniform node deployment in wireless sensor networks for load balancing. Appl. Innov. Mob. Comput. (AIMoC'14), pp. 126–132 (2014)
50. Xu, K., Hassanein, H., Takahara, G., Wang, Q.: Relay node deployment strategies in heterogeneous wireless sensor networks. IEEE Trans. Mob. Comput. **9**(2), 145–159 (2010)
51. Misra, S., Hong, S.D., Xue, G., Tang, J.: Constrained relay node placement in wireless sensor networks: formulation and approximations. IEEE/ACM Trans. Networking **18**(2), 434–447 (2010)
52. Marsh, D., Tynan, R., Hare, G.M.P.O., Ruzzelli, A.: The effects of deployment irregularity on coverage in wireless sensor networks. IEEE (2005)
53. Chang, C.-Y., Shih, K.-P., Chang, H.-R., Liu, H.-J.: Energy-balanced deployment and topology control for wireless sensor networks. In: IEEE GLOBECOM proceedings (2006)
54. Ringwald, M., Romer, K.: Deployment of sensor networks: problems and passive inspection. IEEE (2007)
55. Gajbhiye, P., Mahajan A.: A survey of architecture and node deployment in wireless sensor network. First International Conference on the Applications of Digital Information and Web Technologies (ICADIWT). IEEE (2008)
56. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): a vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. **29**, 1645–1660 (2013)
57. Olariu, S., Stojmenovic, I.: Design guidelines for maximizing lifetime and avoiding energy holes in sensor networks with uniform distribution and uniform reporting. Proc. IEEE INFOCOM06, pp. 1–12, April 2006 (2006)
58. Chamam, A.: On the planning of wireless sensor networks: energy- efficient clustering under the joint routing and coverage constraint. IEEE Tran. on Mobile Computing **8**(8), 1077–1086 (2009)

59. Chatterjee, P., Das, N.: A distributed algorithm for load-balanced routing in multihop wireless sensor networks. Proc. ICDCN08, LNCS4904, pp. 332–338
60. Fouad, M., Oweis, N., Gaber, T., Ahmed, M., Snasel, V.: Data mining and fusion techniques for WSNs as a source of the big data. Procedia Comput. Sci. **65**, 778–786 (2015)
61. Boubiche, S., Boubiche, D., Bilami, A., Toral-Cruz, H.: Big data challenges and data aggregation strategies in wireless sensor networks. IEEE Access 2018, **6**, 20558–20571 (2018)
62. Djedouboum, A., Ari, A., Gueroui, A., Mohamadou, A., Aliouat, Z.: Big data collection in large-scale wireless sensor networks. sensors **18**, 4474 (2018)

Chapter 6
Role of Smart Sensors in Minimizing Food Deficit by Prediction of Shelf-Life in Agricultural Supply Chain

Ganesan Sangeetha and Muthuswamy Vijayalakshmi

Abstract Food shortage is a major problem across the world caused due to larger food wastages. Food wastage includes the lifespan from fruit or vegetable produce till its edible nature on consumer side. Sensors play an important factor in sensing the quality of food produce and reaching customer end without any degradation. There is a high demand to use wireless sensors to reduce food spoilage by inspecting agricultural produce to reach consumers in an efficient way. Existing works include wireless shelf period, improving resource knowledge of produce among stakeholders to achieve timely decisions in supply chain and real-time prediction of perishable agricultural produce. However, there is lacking requirement on efficient usage of IoT sensors to induce no food dumping in agricultural logistics during pre-harvest and post-harvest phases. This Chapter gives a review on the prevailing techniques that use IoT sensors to monitor and prevent perishable food spoilage. An outline of suggestions to increase functioning of sensors using new methods has also been listed.

Keywords Food shortage · Degradation · Agricultural produce · Shelf period · Stakeholders · IoT sensors

6.1 Introduction

Food loss [1] is a major issue that affects the economical, social and human welfare aspects in a nation. In the recent years, these food waste dumping has gradually increased due to improper planning on the yield producer, market supplier and customers. On the producer part, perishable wastage occurs as a result of less

G. Sangeetha (✉) · M. Vijayalakshmi
Department of Information Science and Technology, Anna University, Chennai, India
e-mail: sangeetha.g@auist.net

M. Vijayalakshmi
e-mail: vijim@auist.net

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_6

periodic monitoring of cultivated plants and lack of organized supplying of excess produce to market suppliers. The duty of market sellers involves porting perishable food produce from growers or farmers to customers. End users have the responsibility to preserve fresh fruits or vegetables until their maximum durability and consume them without any wastage. The food yield is brought all the way from plantation area to dining that needs to be effectively utilized. This food cycle has to be carried on carefully in order to fulfil a nation's hunger and achieve independent sustainability.

"Food for all" is the general principle that all the users in food supply chain have to remember. Earlier, there was lack of advanced technologies used in favour of monitoring plant growth, predicting yield, harvesting, storing produce and supplying products to customers. In recent years, Internet of Things (IoT) [2, 3] technology has gained a fast increase in the field of agricultural automation. Different wireless sensors [4] and tag indicators [5] are embedded in crop soil, plantation area, intelligent containers [6] and stuck around plastic covers or containers. The advantages of applying IoT to horticulture include live tracking of plantation environment, plant's growth condition, pre-estimating yield harvest time span, predicting shelf-life for storage commodity in reaching stakeholders and consumers [7]. Various special sensors such as Electronic Nose, RFID tags [8], Ultrasonic and gas sensors are used to ripeness [9] and shelf-life of fresh fruits or vegetables [10, 11].

There are certain integrated functions performed when horticulture is operated via IoT communication. The environmental factors such as temperature, plant moisture content, relative humidity are collected using sensors and given as input to remote computer acting as a gateway. Many sensors track the crop and yield images, ripeness and decaying of produce. The gateway keeps the grower informed about crop's growth periodically and triggers grower on unpleasant and urgent situations such as plant infections, low water levels or fire spreading. An intelligent crop decider can be employed on the grower side to take corrective remedial measures from updated online resources and automatically indicate them to producers.

Recently, predictions on yield maturity and harvest period, amount of sufficient produce or deficit conditions and shelf-life duration of fruits or vegetables thereby informing growers are made with ease. Even after harvest period, sensors and tags are used to give updated information about changes in packed yield. Hence, IoT sensors play a critical role in crop growing and after harvest cycles [12]. Recent research includes IoT techniques to estimate varied lifetime of each produce and connects grower to safely dispose them without any decaying. The retailers or consumers can also set up automated shops or kitchens to use the stored fruits and vegetables on time without degrading their freshness [13]. A connected environment enabled using IoT helps all the users involved in food cycle starting from production till consumption [14].

Pre-estimation of shelf-life span is an essential criteria to predict lifetime of a fruit or vegetable to prevent yield spoilage [15, 16]. Shelf period of yield refers to the duration of plant produce from its fully developed state till the time it reaches

consumer's usage. This paper considers a brief review about the shelf-life prediction of perishable agricultural produce using IoT sensors. One of the main activity in food cycle is to perform minimal storage period for horticultural yield and to enable accelerated pick up by market sellers to suppress food wastage. Market holders play an important intermediate role to import yield from grower and plan for efficient transit to people. On the consumer side, shelf-life can be monitored regularly on daily basis by looking at attached tags and indicators [17] to holder bags. Shelf period for stored food produce is calculated every day and the degradation is informed to consumer thereby stopping perishable food spoilage [18].

Food wastage is an important concern to be considered to avoid lack of food situation among people. Food crisis may occur in a nation not only based on drought conditions, but also due to devastation of yield resources. This paper sketches a survey of IoT sensors that can support plantation monitoring and can predict lifespan of produce to give deadlines to each of users in food chain to utilize yield without quality ruination. The rest of the paper is mapped in following manner. Existing techniques in relation to reduce food spoilage by early prediction of shelf-life in agricultural produce are enumerated in Sect. 6.2. Sections 6.3 and 6.4 highlight the different types of IoT sensors used in agriculture and major divisions in food chain. The basics of shelf-life of a perishable commodity and its prediction in agriculture are listed in Sects. 6.5 and 6.6 illustrates the other technologies used in IoT horticulture to pre-examine various plant conditions. Sections 6.7 and 6.8 outline the efficiency on working of agricultural sensors and recommendations to overcome food drought occurrences. Section 6.9 flashes the future directions of pre-finding shelf-life to stop food degradation in IoT agriculture.

6.2 Related Work

In the previous works, many researchers have furnished both reviews and techniques related to prediction of yield shelf-life duration using IoT sensors used in eliminating food decay. This is an essential feature in the perishable commodity food process. Venuto et al. [19] designed a low cost programmable WSN for warehouse maintenance is devised. There are continuous observations of environmental factors namely temperature, relative humidity and light illumination performed to compute a spatial prediction of commodity shelf-life. The product is checked for quality deterioration using 1st order kinetic Arrhenius model across whole storage area. The proposed system serves as an effective tool for waste control in supply chain by framing a Quality Controlled Logistic algorithm to increase product shelf-life. The recorded readings of agricultural yield shows an increment of nearly 1.2 days of normal expiration date. Jedermann et al. summarizes the findings of study results in promoting intelligent food logistics [4]. Case studies on cold chain cycle of berries, bananas and meat have been discussed along with post-harvest measures. A wireless communication system is set up to perform

quality inspection, gas sensors to trace ethylene indicating ripening and other volatile substances to mark mould infections.

Melis et al. presented combined results on RFID and sensor network devices [5] utilizing three commercial 1848 m^3 chambers using various positions and commodities. Many 3D temperature mapped charts and psychometric data model was obtained based on enthalpy calculation and water content in air. The energy usage in cold room, stored product condensation and water loss from commodities is detected using integrated operation of RFID and WSNs. Annese et al. [20] proposed an effective solution towards reduction of food losses and increasing the monitoring procedure with certification. A shelf-life span of a product and its accuracy is calculated from an algorithm based on Arrhenius law 1. A case study on analyzing three storage factors such as temperature, light intensity and humidity that influence the organoleptic nature of perishable goods is reviewed. This technique is cost-effective with minimal waste release by correct prediction on product life. Kuswandi et al. described a review on smart packaging method [17] that uses chemical or biosensors to monitor from producers to consumers. A variety of sensors monitor food safety preserving freshness, microbes, toxins and pathogens. Smartness in food packing includes yield tracking and authentication of food products.

Buisman et al. [21] studied about the reduction of food waste by retailers using a dynamic shelf life (DSL) or expiration date for perishable agricultural produce. DSL exhibits better performance compared to fixed shelf life (FSL). A Gompertz model is a continuous time growth model is the simulation to update the biological count of products at discrete time points. The perishable product considered here is meat for which a system is developed for profit, waste and safety. The combines application of both DSL and discounting emerges to be a fruitful strategy to manage food quality. Jagtap et al. [22] explored the ease of applying IoT to develop resource in food supply chains. This paper brings out a survey of IoT in maintaining inventory and tracing food supply with labour handling. Fuertes et al. [6] outlines the functions of intelligent packing technology. Various commercial indicators are listed along with their detailed working with their merits and demerits. Bhushan et al. described about Least Shelf Life First Out (LSFO). A Petri Net approach [23] is used for simulation involving Time-Temperature Indicator (TTI) labels and wireless solution. The Generalized Stochastic Petri Net (GSPN) in this system model consists of five collector phases namely Requested, CategoryASold, CategoryBSold, CategoryCSold and Total Perished. Results prove that perishable goods can decrease spoilage by selling more than 90% thereby shooting up profit rate by 10%.

Biccario et al. [24] framed a feasible control operation in perishable food supply-chain by combining WSN in real time for environmental perceiving and carry out data processing to state the product shelf-life. Temperature, humidity and light sensors are used for live sensing with a Zigbee communication between each sensor and gateway. A linear model for prediction of quality perishing is given accompanied by finding accuracy of shelf span evaluated using Arrhenius law. Broekmeulen et al. listed concepts to improve working of fresh produce departments in supermarkets by lowering food rottening, growth of freshness and expanding sales. Two methods that are applied to improve food potential are called

fresh case cover and efficient frontiers [1]. These concepts show an increased shelf life with 43.1% less spoilage, 17% higher freshness with one day parameters and unpacking results with 2.0% On-Shelf Availability (OSA) executed for medium and large stores. Hertog et al. [25] focussed on various model techniques to inspect quality variations and shelf span can be merged in lifting first-expired first-out cold food chain. An exhaustive search algorithm is used for feasibility for shelf spanning optimization. An integrated strategy is formed where front end sensors enable post harvest to alter cold chain dynamics.

Jha et al. [26] illustrated recent works towards measuring quality parameters, before and after harvest treatments with respect to the condition of mango fruits and lists non-destructive methods for spotting quality. This paper shows physiological and physical disorganization in mango fruit such as sap burn, spongy tissue, black-tip, soft-nose and chilling injury. Hong et al. used eight data sets retrieved from e-nose, e-tongue and a combination of both sensors to trace 100% juice from cherry tomatoes used with various storage times [27]. Tracing and predicting physiochemical behaviour of fruit is performed using principle component regression. Sensor fusion gives better performance when appropriate feature selection and data integration techniques are used. Wang et al. [28] devised an experimental system for dynamically obtaining resonance based on frequency response of excited pear with variations in excited points. Other measures include excitation medium and material, detection points, stike intensity under different pear firmness and weight conditions. A firmness index was regressed based on Magness-Taylor firmness exhibited a better relationship when pears were knocked with 0.392, 0.84 and 1.26 velocities. Li et al. investigated a sensing approach to inspect sour skin of onion using gas sensor and support vector machine (SVM) [29]. Sour infected onions were dropped in a concentration container for headspace gathering and was present three to six days after inoculation. Different analytical methods namely Principal component analysis (PCA) sum plots Multivariate analysis of variance (MANOVA) were used to find healthy onion bulbs (not $P < 0.0001$). The six-sensor usage scheme performed well in validation phase with 85 and 67% classification rate.

Ketelaere et al. [30] demonstrated the firm nature of 13 unsteady tomato cultivars during a 2-week container experiment using acoustic firmness sensor. Linear model variables are used to cluster tomato cultivars according to firmness variations, shelf-life and variance. Pasquariello et al. [31] investigated physical-chemical and sensory assessment after 4, 8, 12 and 16 weeks with 2 °C and with five-day period of 20 °C after 5-day period. A multivariate statistical approach was reduce datasets that showed 78.83% variability and also provided an entire view of early ripening pear cultivars with respect to cold storage. Ignat et al. [32] presented a combined approach of non-disasterous outputs and a set of damaging reference factors associated to bell pepper. Spectrophotometer sensors are utilized here and bell pepper maturity is found by applying both linear and non-linear regression techniques.

Ostojic et al. [33] presented a dynamic shelf span prediction framework based on kinetic Arrhenius model to reduce food wastage in supply chains. Watteyne et al.

developed a methodology to foresee frosting activity by considering sensor measurements from orchard. This article provides an in-depth discussion of how IoT technology impacts precision agriculture by selecting rightly capable sensors for performance. Heising et al. [34] described about intelligent packaging in food supply chain using quality-controlled logistics (QCL). QCL is combined with dynamic pricing to predict expiration dates leading to minimization of yield waste. Venuto et al. [35] aimed to increase shelf life using a low cost and reconstructable Wireless Sensor Network (WSN). A spatio-temporal prediction of commodity by employing 1st order kinetic model.

Witjaksono et al. [36] explored application of IoT to spot food quality and trace safety. This quality information can be shared across all food growers and consumers via IoT network and application layers. Reid et al. [37] proposed a new procedure involving the detection of shelf spans of produce at more frozen temperatures. Information on mobile temperature is established with a less temperature storage is collected. On an average if shelf duration is 60 days, using this method of working freezing storage can provide a life of 1 or 2 years or much longer spans. Dermesonluoglu et al. put forth a kinetic study [38] depending on quality degradation of frozen spinach to calculate remaining storage duration. Variuos parameters such as chlorophyll, surface texture, colour, Vitamin C and receptive parameters were measured in frozen spinach. Both isothermal tests at −5 to −18 °C and non-isothermal conditions with −6.9 °C efficiency were conducted for model validation. Arrhenius equation was used for modelling energy values and quality depletion. The shelf period of yield stored at −18 °C ranged from 400–500 days depending on distinct quality indices.

Popovic et al. [39] discussed a summarized study on designing IoT for findings in precision farming and ecological supervising domains. A list of end user demands are found considering logistical high-level instances. Further expansion of IoT protocols, analytical tools and data types are solutions that contribute to upcoming researches. Bing et al. [40] investigated sensors used in perception layer with Bluetooth and 4G applied in transport layer. A small scale farm experiment was done to monitor plant cultivations, posing alerts about pests and diseases and their diagnosis. Nobrega et al. focussed on intelligent farming based on IoT and M2M intercommunication [41] with gateway deployment. SheepIT is an automated system using IoT to manage/sheep grazing in vineyards. An evaluation on the gateway analysis is done to illustrate ease and scalability using real cases.

Luthra et al. [42] introduced the employment of IoT in Agriculture supply chain management (ASCM) to lower food decay by fulfilling user needs efficiently. The scope of IoT in industrial ASCM functions in India is concentrated. Karkkainen et al. [43] illustrated the potential of deploying RFID in supply chain of lower shelf life commodities to retailers and other participants. Numerous operational benefits on using RFID in farm supply chains are discussed. Duan et al. analyzed attributes used in process of agricultural supply chains [44] and management. Connecting farms can also solve emergency dispatch of crops in critical situations apart from improving quality.

6.3 IoT Sensors in Agricultural Food Production

Wireless Sensor Networks [19] form the basic working structure of IoT to observe and collect information and readings from environment. Sensors used in agricultural food chain predict crop growth, essential utilities such as water, temperature, humidity, O_2 and CO_2 levels, harvest time, and shelf-life determination using respiration rate. Now-a-days moving one step ahead, sensor observations also predict the existing market indexes (QIM, QSM) for perishable produce. Smart sensors integrate hardware measurement readings and mathematical prototypes to relate sensed readings, quality effectiveness and varying time limits.

6.3.1 Basic Wireless Sensor Design

The fundamental level formation of a smart wireless surround for monitoring plant produce [45, 46] include a temperature sensor with an AC input voltage of 3 AA battery of 1.5 V. The range covers 18 to +55 °C and an accuracy level of ±2 reading value. Temperature sensors are fixed on grounds, plant pots or indoor walls to find weather differences. A Relative humidity sensor is used with range 0–95% RH. Replaceable humidity value ranges with ±5% for 0–59% humidity and ±8% for 60–95% humidity. The RH accuracy level covers ±3.5%RH. Humidity levels are equally important indicating the amount of water content present in atmosphere as it influences plant growth. Soil sensors read moisture. FC-28 sensor has a range from 0 to 1023, giving moisture percentage between 0 and 100. Input voltage is from 3.3 to 5 V, with outputted voltage of 0–4.2 V. A soil hygrometer detection sensor can be used with Arduino to initiate a self-watering cycle in plants. Other accurate soil sensors include SEN-13322 ROHS by SparkFun and VH400 low-cost soil moisture sensors by Vegetronix. These are the basic sensors that are used in IoT agriculture for setting up a start-up maintenance with minimum cost.

An Arduino Uno R3 ATmega328P microcontroller is used to store and execute programs to sense the environmental parameters. A ESP8266 WiFi module is connected to Arduino board for exchange of data packets between the surrounding environment and food produce maintainer. The collected data values from plant production is fed into an intermediate gateway machine that acts as a coordinator. The gateway feeds these readings into the data cloud applications that are available namely Microsoft Azure IoT Suite, Thingspeak from MATLAB, Google Cloud IoT, IBM Bluemix. A web service is required to handle the data values in data cloud and to enable the client and server interactions using REST APIs. End user or food producer devices may use a personal computer, tablet or smart phones that need to be compatible with sensor devices. Both hardware devices and end user device must provide user API where the food producer can initiate commands for which wireless sensors need to respond and take corrective measures. Certain mobile application platforms like EvoThings, Blynk and ThingStudi enable creating

IoT live running iterations using simple scripting languages such as HTML, Javascript and CSS. This is the general outline of how IoT communication takes place between the sensor nodes and producer agent.

Currently IEEE 802.11 WiFi technology is widely used for device interaction using RF (Radio Frequency) waves. WiFi utilizes either universal 2.4 GHz UHF or 5 GHz SHF ISM bands. Network band versions IEEE 802.11b, 802.11 g and 802.11n operate within 2.4 GHz band. Other communication technologies that can be used include IEEE 802.15.4 (Zigbee), IEEE 802.15.1 (Bluetooth and Bluetooth Low Energy) and IEEE 802.16 (WiMax).

6.3.2 Incorporation of Other Wireless Sensors Depending on Utilization

In addition to above mentioned sensors, other sensors can be joined to provide more functionality. Foot-candle meters were used earlier to measure light intensity but faces drawback of erroneous reading in electric lights. Lux meters were similar to foot-candle with 10.8 lx for all illuminant sources. Quantum sensors used recently sense light and display output values directly. LI-COR, Kipp & Zonen and Apogee Instruments manufacture these output sensors. Another type of light sensor reading is based on its power called radiant flux. The input energy from a source namely sunlight or bulb can be measured at a particular distance. A radiometer measures the light power whereas a pyranometer traces short radiation including photosynthetic light, energy from UV light and IR light. However, light sensor has a standardised bandwidth range from 360 to 970 nm, peak wavelength of 570 nm and luminance range of 10–1000 lx with ±20% difference range. An electrochemical pH sensor is used to find the concentration of hydrogen-ions in water marking acidity or alkalinity. Zerone pH tester and pH1000 from Sensorex are better solutions to determine water quality. Figure 6.1 depicts the basic framework of IoT in smart agriculture.

Table 6.1 shows the connection between Arduino microcontroller and WiFi chip. According to our application requirement, sensors are connected to data input/output ports (14 pins available) and analog ports in Arduino (6 pins).

Table 6.2 depicts a collection of different sensors used in agriculture starting from the growth of a plant, monitoring produce, pre-harvest and post-harvest conditions. Different sensors are used for each level to perform its own task.

6.4 Major Phases in Food Supply Chain

There are two main branches in IoT agriculture in producing food crops namely fruits, vegetables, cereals and other essential crops. They include stages of pre-harvest and post-harvest.

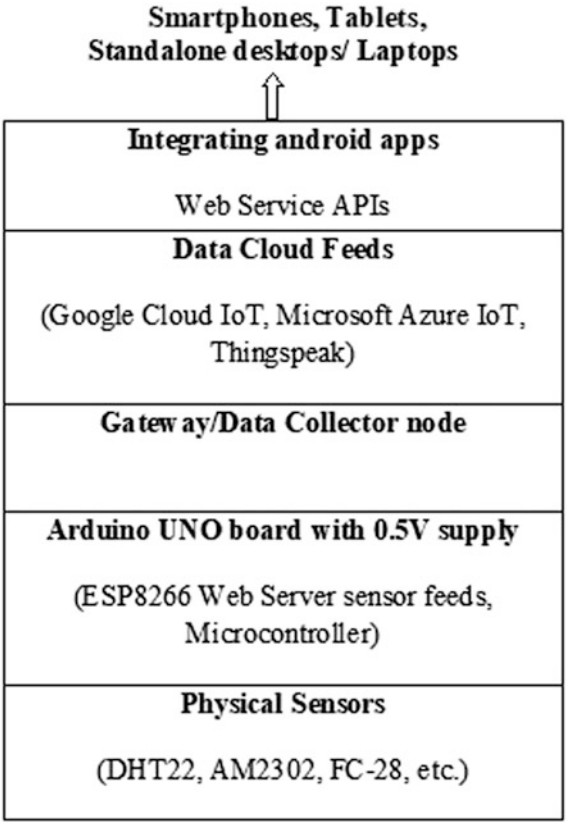


Fig. 6.1 Sensing architecture in IoT applications

Table 6.1 Connecting pins on Arduino and WiFi module

Arduino	ESP8266	Resistor (K)
GND	GND	–
VCC/3.3 V/power	3.3 V	10
CH_EN/enable	3.3 V	10
TX	PIN3	–
RX	PIN2	1
RX	GND	1

6.4.1 Pre-harvest Environment

The functions of the first harvesting phase includes frequent examination of plant growth stages, supplying needful fertilizers to boost plant development with yielding produce, pre-analyzing the time period for harvest and informing market vendors about the period of collecting produced yield crops. The main sensors used in this phase include temperature, relative humidity and soil moisture monitoring

Table 6.2 Classification of various sensors used in IoT agriculture supply chain

Sensor	Operating voltage	Range	Utilization
Temperature—LM35	+10-mV/°C	−55 to 150 °C	Reads centigrade scaling
Relative humidity—DHT22	3–5 V	0–100% humidity and 40–80 °C temperature	Senses digital-output for relative humidity, and temperature
Soil Moisture FC-28	Input voltage: 3.3–5 V, Output voltage: 0–4.2 V	0–100 (0–1023 mapped in percentage); operates in analog and digital modes	Measures dampness value.
pH—PH meter SKU SEN0161	5 V	0–14 PH	Used in water quality testing and aquaculture
Rain—chip-based LM393	0–5 V, Buzzer driver circuit—5–12 V	Rain threshold—300, time delay—30 s	Tracing rain occurrence
Light—LM 393	3.3–5 V	15 mA Driving ability	Detects light brightness in the environment and decides to switch OFF or ON light.
Radiation—Geiger Sensor board SEN-14209	3–9 V	Reliability up to 1 mSv/h (1000 uSv/h—Sievert is derived unit of ionizing radiation)	Detects Alpha, Beta and Gamma radiation on integration of Geiger Tube
Wind—Adafruit anemometer	7–24 V	Up to 70 m/s or 156 mph	Measures wind speeds

sensors. Certain protective sensors namely MQ2 Flammable Gas and Smoke Sensor with 5 V power supply can be used to detect fire incidents in plantation area. Smart motion sensors can be installed in wide plantations to provide a good coverage about field activity. As our paper is targeted on short area plantations such as terrace cultivation and greenhouses, it is sufficient to use reasonable coverage sensors. HomeMate is a WiFi smart motion sensor that can be used to monitor plants before plantation harvest with a wireless coverage of 45 m and sensitive angle of 110° that is compatible with Alexa and Google home. D-Link WiFi Motion sensors are also available to send alerts to user phones. These sensors add more capability to safeguard plant yields, moreover optional requiring high maintenance.

These sensors send their perceived growth progress information to producer or farmer. Apart from above mentioned sensors, there are other sensors that track data on O_2 and CO_2 levels, ripe nature of fruits or vegetables and freshness indicator that can measure chlorophyll in plants and presence of chemical levels such as ethylene compounds. A crop yield tester framework analyzes and detects any fungal or bacterial infection and ripeness of produce. This tester also provides the approximate shelf-life and harvest period sign to end producer or farmer. These are the functionalities of predicting shelf period in pre-harvest stage.

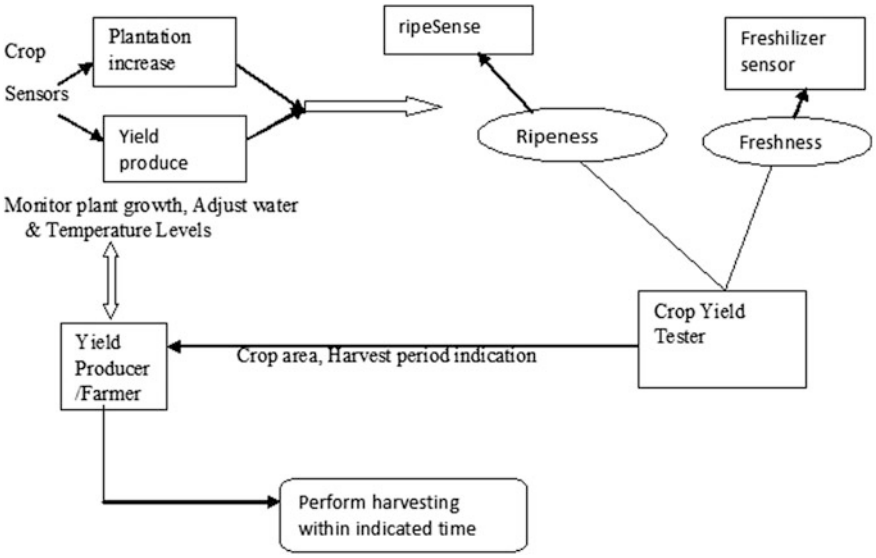


Fig. 6.2 Steps involved in pre-harvest cycle

The above sketched diagram in Fig. 6.2 illustrates the major steps taking place during prior period before harvesting.

6.4.2 Post-harvest Phase

There are three major steps in this phase for enabling producer to reach customers with the yield [47]. After the cultivated produce has been harvested, it is temporarily stored in an intelligent refrigeration container [34] with smart tags and sensors. Firstly, the respiration levels of fruits or vegetables are supervised using certain special functionality indicators as discussed in Sect. 6.5. Depending on these parameters, a time indication is sent to stakeholders. Both the producer and stakeholders are informed about the remaining shelf-life of produce as sensors indicate freshness time to time. This is the second major step to disperse fruits and vegetable commodity to market owners. Thirdly, if produced stock is not collected by stakeholders within time limits an indication is sent to producer to take immediate action to avoid food spoilage. A threshold range is set for each parameter such as freshness and ripeness. On exceeding these values, the sensors send emergency alarm notifications to producer.

Figure 6.3 describes the basic steps involved after harvesting crops in agricultural logistic chain.

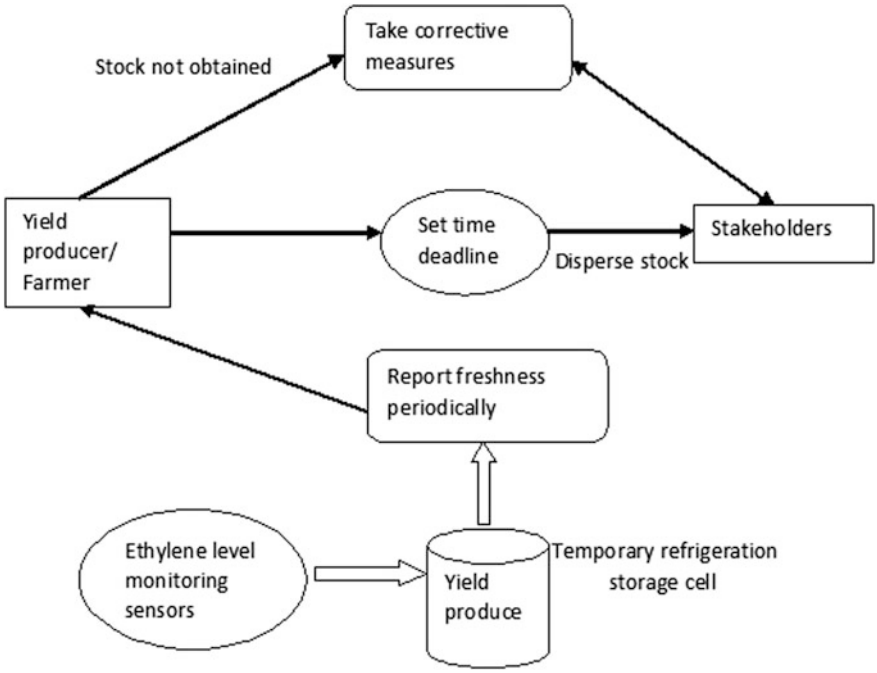


Fig. 6.3 Stages in post-harvest system in smart agriculture

6.5 Smart Shelf-Life Predictions

Shelf-life is the time length that a produce or commodity is stored till it remains fresh, consumable and fit for usage. In agriculture, shelf-life of a fruit or vegetable is the duration from the time when yield is matured till it reaches consumer's plate for utilization. All the agricultural yield products are perishable having their own shelf duration. Agricultural yield products are subjected to several factors such as heat, gas releases, moisture, light, soil permeability and infections caused by insects and microorganisms. Shelf life of agricultural commodity depends on three main factors namely nature of product, packaging and distribution frequency. Temperature is a critical element that is to be kept under control by means of shipping containers, automated cold chain and refrigeration. Chemical reactions consisting of catalytic enzymes speed up when temperature increases causing bacterial and fungal infections. Minimal yield storage has to be done with accelerated delivery to consumers to avoid food loss.

Smart farming is the integration of communicating technologies to collect and coordinate data from fields and alert the farmer about emergency situations that need to be treated without any delay. Lower moisture content in soil, improper nutrition, fire accidents, drying of leaves or produce due to excess heat comprise of emergency cases in agriculture. Instead of manual operation by growers, an

automated solution can be initiated by machines operated with wireless sensors form an intelligent IoT farming potency. A farmer can perform remedial actions with plantations by easily accepting or rejecting the indications and measures flashed by IoT connected widgets. So there is a one touch action dispatched by farmer from anywhere, at any time.

6.5.1 Network Communication in Smart Agriculture

There are different communication means used for varying distances. In case of shorter distances, Radio Frequency Identification (RFID) or near field communication (NFC) can be utilized. These technologies can be also used to keep track of net weightage of a feedbag for example, a soya or an apple bag. RFID tags reads encoded digital data via radio waves. RFID system is composed of smart labels, RFID reader and an antenna. NFC is an upgradation to RFID that joins smart card interface and reader into a single component. NFC enables two-way communication between visible devices within closer proximity. Advantages of NFC are quicker connection establishment (within 0.1 s) and greater degree of accuracy. When distance increases up to 10 m or closer, Bluetooth Low Energy (BLE), Bluetooth or Zigbee can be used. BLE is used for short-range communication when battery power is opted over higher data transfer speeds.

BLE data exchange consists of 40 frequency channels with 2 MHz divisions. There are three primary channels for advertisement and 37 secondary or data channels. Both the traditional Bluetooth and BLE are same except for power consumption. BLE requires less power having devices operating for several years. BLE is well-suited for temporal data transfer as in IoT applications whereas Bluetooth is used for continuous streaming of data such as headphone usage or exchange within closer proximity. BLE can handle up to 20 connections simultaneously for example, its usage in smart proximity marketing with 200 Kbps. Classic Bluetooth can initiate only 7 connections at the same time with 2–3 Mbps.

Zigbee is a wireless technology for IoT and Machine-to-Machine (M2M) devices with low cost and power. This is based on IEEE 802.15 standard operating with 2.4 GHz, 900 MHz and 868 MHz frequencies. Zigbee PRO specification provides IoT features such as low cost, high reliability and energy harvesting feature named green power that boosts devices to operate without batteries or power supply for prolonged deployment. If working of IoT application transmitting data around hundreds or thousands of meters, then Low Power Wide Area Network (LPWAN) can be used for high-end interaction. Symphony Link builds greater reliability and scalability to set up a smart farming application. There are two main considerations to keep in mind while configuring an IoT application in agriculture namely establishing sensor connection for measuring data values, choosing sensor position and proper mounting for optimal path traversing for transmission. The communication technology utilized in application should not be a barrier for end

grower measurements. These are the intercommunication technologies from which best fit that can be selected according to our agricultural application.

Figure 6.4 shows a collection of activities inspected by IoT in agriculture. Different wireless sensors are used to carry out IoT interaction between the harvested yield of matured fruits or vegetables, farmer or grower and stakeholders. Sensors serve as an interface to build a triangular communication between the users. Various tags, indicators and sensors are operated to maintain automated environmental and yield updates to crop grower and market sellers. RFID tags play a main role in IoT agriculture for enabling ease operations. TempTRIP uses RFID smart antenna reader that operates with class 1 ultra high frequency that can wirelessly send temperature configurations in stored produce. The reporting intervals can be adjusted from 1/min to 1/day with a battery power of up to 5 years. This low cost smart reader sustains a range of −30 and +50 °C with an accuracy time interval less than 0.5% error rate. Intelligent box from Mondi Plc consists of a RFID tag enables to identify, live track and spot crop produce inside the store container. Another RFID tag named CS8304 from Convergence Systems Ltd is a sensitive cold chain temperature logging tag. This Battery Assisted Passive (BAP) tag has 10 K memory to save temperature samples. These tags can be read using any EPC class 1 gen 2 reader with a reading coverage of 2 m thereby offering a good performance in produce with higher water content. Another easy2log tag from CAEN RFID uses RAIN RFID, a passive UHF belonging to class1 gen 2 standard. This temperature logger can store up to 8000 samples at 0–5 °C accuracy. This has features such as fast data download with automatic inspection on quality.

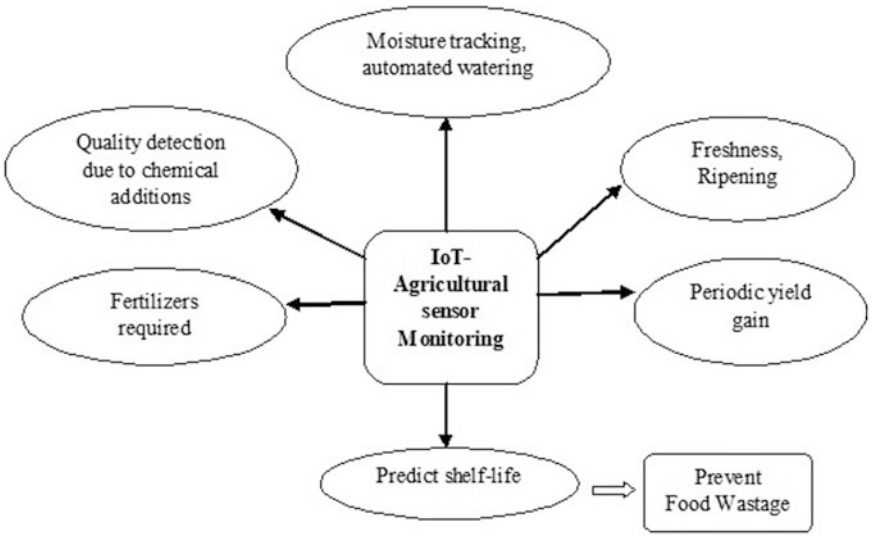


Fig. 6.4 Functionalities of IoT sensors in agricultural sector

Freshness indicator is the next important criteria needed by yield to indicate its edible nature to consume with proper nutrients. Freshtag is an ultra low-cost tags that can sense parameters like temperature, O_2, CO_2, pH or ascorbic acid and hydrogen peroxide. The search of fresh parameter defines the disposable chip technique to Internet of Everything (IoE). A near-field communication (NFC) tag enabled device is used to read fresh property from package in real time. This also determines a dynamic expiration date for a product based on acquired data parameters. SensorQ from DSM NV and Food Quality Sensor International to detect bacterial spoilage in packed food produces. This biosensor label responds to bacterial infection changing its colour from orange to tan as microbes increase. The level of ripeness is indicated using ripeSense manufactured by RipeSense and Hort Research. This sensor reduces chances of damage and shrinking, managing a good shelf-life of each stock production item. The sensor changes colour reacting to fruit aroma during ripening, initially red, progresses to orange reaching yellow at last. The customers can opt for the ripened fruit level they need matching with sensor colour. Integrity indicators are also equally important to trace produce quality for increased shelf-life.

Timestrip from Timestrip Ltd flashes the occurrence of a temperature breach and its duration. Novas label manufactured by Insignia Technologies Ltd marks food freshness from pack opening by detecting changes in CO_2 levels. Centre dot changes colour when temperature increases over product shelf-life resulting in reduction of food wastage. Ageless Eye from Mitsubishi Gas Chemical Inc. is a gas indicator that turns colour when oxygen in a package is depleted. The in-package monitor changes blue or purple colour when oxygen exposed, then jumps back to original pink colour as oxygen in container is reduced. Best-by time indicator label from FreshPoint Lab is another sensor used to detect shelf-life of yield produce. This label is of tablet form and needs to be stored below 15 C with no oxygen until use. Vitalon from Toagosei Chemical Inc. and Freshilizer from Toppan Printing CO are CO_2 gas indicators to detect and avoid food wastages. Certain time-temperature indicators (TTIs) are available to monitor safety of food produced. Fresh-Check from Temptime Corp. is based on Polymerization reaction TTI, OnVu from Freshpoint and Ciba based on Photochemical reaction TTI, FreshCode from Varcode Ltd. and Tempix manufactured by Tempix AB relying on Barcode based label TTI and 3 M Monitor Mark from 3 M Company based on Fatty acid ester TTI, TopCryo from TRACEO based on Microbiological TTI are the various types of TTIs across wide usability to maintain shelf-life period.

6.6 Other Technologies for Predicting Shelf-Life of Crop Production

There are several technologies that can be operated with a sensor to predict the life of a yield produced. Apart from the common sensors and tag indicators there are chemical and gas means used to determine the yield quality. This quality of

Table 6.3 Various other sensors used in horticulture logistics

Sensor type	Comprising material	Determination
Electronic nose	Ethylene VOCs, uses tin/metal oxide	Yield ripeness, decaying
RGB camera TCS230	Array of photodiodes	Recording yield images
Near infrared (NIR) spectrometry AS7263	Detects 610, 680, 730, 760, 810, and 860 nm of light with 20 nm of full-width half-max detection	Produce freshness by measuring chlorophyll fluorescence
Electrochemical—Ion-sensitive field-effect transistor	Surface hydrolysis of Si–OH groups of the gate materials varies in aqueous solutions due to pH value. Gate materials are SiO_2, Si_3N_4, Al_2O_3 and Ta_2O_5	Portable for ethylene detection
Microwave imaging RCWL-0516	Doppler radar effect	Measures entire component of produce
Ultrasonic, cavity ring-down spectroscopy (CRDS)	Tunable diode laser beam sent into a high-fine cavity	Freshness spotting
Laser biospeckle	Optical phenomenon occurring during illumination form random, granular patterns consisting of dark and bright spots	Freshness detection
Photoacoustic spectroscopy	intense lasers, sensitive microphones, lock-in amplifiers	Freshness
Ultrasonic sensing	piezoelectric transducers or capacitive transducers	Freshness
Micro gas chromatography	Source of carrier gas, preconcentrator-injector, separation column, detector, pump, valves, and software for instrument control	Crop health and diseases

shelf-life is pre-determined to avoid excess wastage of unconsumed food produce. Table 6.3 summarizes a collection of other sensing technologies used in agriculture.

Certain sensor technology can be utilized during both the pre-harvest and post-harvest phases to prevent food spoilage and dumping. Sensors used based on electrochemical and gas chromatography are accurately suitable for finding ripeness in fruits and vegetables. Cost cautious E-Nose takes the top place in determining freshness in agricultural produce. Another cost-efficient and provable remedy for analyzing fruit ripeness is using NIR spectroscopy. There is next level of technologies that form a better identification of plant produce conditions. Hyperspectral imaging has capability to acquire more information about freshness and demands higher storage requirements to frequently monitor yield. Terahertz Imaging and X-Ray form different case technologies for detecting edible nature of fruits and vegetables for providing a better shelf-life. Photoacoustic spectroscopy technology is used for inspecting the quality in fruits and vegetables before and after harvest. CRDS infrared laser enables satisfactory quality detection but it is cost-sensitive.

There are certain basic recommendations to be followed for selecting the sensors based on more suitable technologies. The first constraint is to select a cost-efficient and accurate sensing technology for freshness identification. Second consideration is the use of ethylene aids to trace ripeness of fruits and vegetables so that it is more appropriately edible thereby providing food safety to customers. Existing ethylene examining techniques are very expensive involving many process steps. A very good option to find fruit ripeness is to use E-Noses to detect volatile organic compounds. Ethylene is a main chemical compound responsible for the decay or ripening of fruits and vegetables. Thus ethylene is a major sensing parameter to mark if a food product is reaching its boundary of shelf-life.

6.7 Performance of IoT Agricultural Sensors in Preventing Food Wastage

IoT technology is entirely about data perception from surroundings and accurate data processing with predictions. The power of IoT lies in trustworthy data provided by many low cost sensors. Selection of best suited sensor with acceptable accuracy limits and low cost are the important constraints to keep in mind while designing an active application. For example, consider two temperature sensor cases where first sensor has a higher cost of accuracy ±0.001 °C and second case has an accuracy of ±1 °C. Between these ranges there might be other sensors with accuracy levels of ±0.07 °C, ±0.5 °C or ±0.3 °C. From these use cases, as a common rule the lowest price sensor providing better accuracy is chosen. This usage is still limited to fact that the above rule can be applied to basic non-critical application such as tracking terrace weather but cannot be used to analyze climate changes.

Table 6.4 shows the major sensors in relation with IoT agriculture which has considerably better accuracy measurements. However, there are practically many sensors available for commercial use, only a few with acceptable accuracy and cost are listed in context.

6.8 Suggestions to Meet Future Demands in Agri-Conservation

A set of pre-measures can be taken prior to conserve food degradation in agricultural logistics. The producers or growers need to introduce new prediction models for extending shelf duration to improvise their market supply without wastage. Applying e-nose for detecting pesticide traces on fruit exteriors after harvest, detecting fruit disease and taking remedial measures and inspecting fruit quality by observing gases in fruits to reduce ripening. Wireless Nano Sensor Nodes

Table 6.4 Performance limits of different sensors utilized in IoT agriculture

Sensor model	Accuracy level	Measurement range
Temperature-Texas Instruments' LMT84LP, SparkFun DS18B20	±0.4 °C, ±0.5 °C	−50–150 °C, −55–125 °C
Relative Humidity-HMP110	± 1.5% RH	0–100%
(i) Sonkir Soil pH Meter, MS02 3-in-1 Soil Moisture/Light/pH Tester (ii) Soil Moisture-XLUX T10	–	3.5–8 pH (3.5–6.5 Acid, 7–8 Alkaline); 1–10 scale Levels 1–3: dry, 4–7: moist, 8–10: wet. Lengths varying from 15″–48″
Grove-Gas Sensor (MQ5)	–	Detects LPG, natural gas, town gas
pH meter-DFROBOT SEN0161	±0.1pH (25 °C)	014pH (0–60 °C)
Optical-LIDAR-lite V3	±2.5 cm at >2 m	up to 40 m
Electrochemical- (i) Texas instruments LMP91002 Sensor AFE (ii) Winsen Ethylene Oxide ME4-ETO	0.1% active energy (1.8 ±0.3) μA/ppm	Up to 900-pA at 85 °C 0 ∼ 20 ppm
Ultrasonic-HC-SR04	3 mm	2–80 cm, <15°
Mechanical-Honeywell FSG15N1A	0.5%	Up to 1.5 kgf

(WNSNs) can increase cooperation and sharing produce information among users. The development of WNSNs in future will definitely bring greater impact in IoT integrated agricultural industry. Smart labelling and wrapping are the areas that need good attention for controlling food loss even after harvest. On the consumer side, assume restaurants, can prefer counter timers as of how many times certain meal is cooked, which recipe is opted more by clients and quantity of ingredients required for each meal to make dishes for consumption. Smart sensors in this operation need to perform data analysis to track purchasing of fruits or vegetables, remaining stock available and their shelf span enabling to construct new analytics for foreseeing good yield management.

Incorporation of IoT for increasing resource efficiency in food chains and enhancing decision-making techniques has given rise to framing of decision-making processes. Various non-destructive methods for quality inspection in case of major tropical fruits is a critical requirement in precision agriculture. Freshness sensors had to be embedded in packaging and required to be compatible with printing technology to create a safe environment and customer friendly experience. Freshness sensors can communicate with customers directly using their smart-phones and gadgets, so compatibility is a major concern that is to be supported for interfacing. Integration of details about pathogen databases can improve the detection conditions and data processing. A dynamic sensor portfolio is required to

turn off unused sensors and thereby deactivating devices in field with backend network. This cuts down hardware and maintenance cost of sensors. There are several technical limitations in designing IoT solutions such as low power consumption design, energy saving, system compatibility, reliable and data roaming communication and signal coverage.

Consumer studies to analyze whether dynamic expiration date with intelligent packaging can help customers to plan their purchases at retailer and consumption at home. This is an important area of research that is to be extended to reduce food ruin. Priority levels can be adjusted such as the high-quality perishables can be sold to customers at a premium cost when compared to longer shelf duration commodity. Thus priority shifting is an essential move in reaching zero food wastage. Customer withdrawal of yield products, weekly purchase patterns and ordering behaviour depending on consumer actions are various fields requiring more examination. Regression analysis can be employed on empirical data to scan degradation percentage depending on store and product divisions. Implementation of dedicated applications and appropriate sensor deployment at points for improving remote monitoring require development. This saves the overall cost, energy and maintenance of produced food.

Several analytics can be foreseen before their occurrences in farmland or terrace plantations. IoT allows farmers to plan which crop to plant and harvesting times to produce highest yield accounting nutrition and surrounding factors. Thus aiming for maximum and fertile cultivation within farm area to yield good profit is an essential criteria in smart horticulture. Green house farming is another technique that is getting more smarter with IoT integrated systems thereby intelligently controlling climate using monitors. A cloud server enables data processing and takes remedial action. A Illuminium greenhouse has gained popularity by the usage of solar powered IoT sensors. Information on temperature, pressure, humidity and light limits are examined in this Agri-Tech greenhouse. Exploration of other factors to stimulate plant and yield growth can be initiated. Development of ground and aerial based drones to assess crop health and field analysis have increased in recent years collecting data and images. Integrated GIS mapping using drones have ability to increase yields that need more constructive techniques for efficient utility. However, the discussion on drones is of less concern in our summary. More Variable Rate Irrigation (VRI) optimization methods for improving profitability and water use effectiveness need to be formulated. Another research area that is gaining importance is farm vehicle tracking and smart tractor operations. New innovative initiatives are to be taken to implement intelligent farm vehicles. Fertigation using drip system is a developing zone that requires further advancement to yield fertile produce for consumption.

Monitoring crop growth activity and anomalies prevent harm nature in crop yield. New methodologies to efficiently analyze infections from sample images should be devised though there are many other solutions given by researchers by combining IoT with intense image processing. In the cold storage mechanism to freeze yield, there are several tags and indicators embedded with sensing technology using intelligent packaging are currently employed. Safe embedding of such

reactive sensing tags, accurate indications on food degradation, alerting users towards stages of decaying are important challenges to develop in food chain logistics. Internet of Tractors is another new area of research emerging to perform smart agriculture by interconnecting several agricultural vehicles. Smart wireless warehousing, logistics and distribution is another sector that requires research in future across agricultural logistics. The above mentioned scope areas are booming development belts in IoT agriculture.

6.9 Conclusions

Food degradation and dumping in agricultural supply chain is a major problem to be resolved in the coming years to achieve goal of providing daily bread to every individual in a nation. Application of IoT to control food wastage has enabled the users in food chain to operate with ease communication by pre-estimating shelf-life duration. This paper emphasized a brief exploration on different types of IoT sensors and their capabilities to handle food decay by passing alert information to growers or producers, vendors and buyers. The performance evaluation of vital IoT wireless sensors and suggestions to overcome food spoilage were discussed. Deployment of sensors varies upon each practical implementation of the proposed application due to changing factors. Therefore, choosing wireless network design for IoT communication and employing suitable sensors in pre-harvest and post-harvest stages is a challenging area that needs to be traversed in the coming years.

References

1. Broekmeulen, R.A.C.M., Donselaar, K.H.: Quantifying the potential to improve on food waste, freshness and sales for perishables in supermarkets. Int. J. Prod. Economics **209**, 265–273 (2019)
2. Pang, Z., Chen, Q., Han, W., Zheng, L.: Value-centric design of the internet-of-things solution for food supply chain Value creation, sensor portfolio and information fusion. Inf. Syst. Frontiers **7**(2), 289–319 (2015)
3. Nukala, R., Panduru, K., Shields, A., Riordan, D., Doody, P., Walsh J.: Internet of things: a review from 'Farm to Fork'. In: 27th Irish Signals and Systems Conference (ISSC), IEEE, Londonderry, UK, June 21–22
4. Jedermann, R., Nicometo, M., Uysal, I., Lang, W.: Reducing food losses by intelligent food logistics. Philos. Trans. R. Soc. A. **372**, 1–20 (2013)
5. Badia-Melis, R., Ruiz-Garcia, L., Garcia-Hierro, J., Villalba, J.I.R.: Refrigerated fruit storage monitoring combining two different wireless sensing technologies: RFID and WSN. Sensors **15**, 4781–4795 (2015)
6. Fuertes, G., Soto, I., Carrasco, R., Vargas, M., Sabattin, J., Lagos, C.: Intelligent packaging systems: sensors and nanosensors to monitor food quality and safety. J. Sens. 1–8 (2016)
7. Gong, W., Li, D., Liu, X., Yue, J., Fu, Z.: A model to predict shelf-life loss of horticultural produce during distribution with fluctuated temperature and vehicle vibration. In: Zhao, C.,

Li, D. (eds.) Computer and computing technologies in agriculture II, Volume 3. CCTA 2008. IFIP Advances in Information and Communication Technology, Springer, Boston, MA **3** (295), 2197–2206 (2009)
8. Ruiz-Garcia, L., Lunadei, L.: The role of RFID in agriculture: applications, limitations and challenges. Comput. Electron. Agric. **79**(1), 42–50 (2011)
9. Oms-Oliu G, Soliva-Fortuny R, Martín-Belloso O (2007). Effect of ripeness on the shelf-life of fresh-cut melon preserved by modified atmosphere packaging. Eur. Food Res. Technol. **225** (3–4), pp. 301–311
10. Guohua, H., Yuling, W., Dandan, Y., Wenwen, D., Linshan, Z., Lvye, W.: Study of peach freshness predictive method based on electronic nose. Food Control. **28**(1), 25–32 (2012)
11. Ruiz-Altisent, M., Ruiz-Garcia, L., Moreda, G.P., Lu, R., Hernandez-Sanchez, N., Correa, E. C., Diezma, B., Nicolai, B., García-Ramos, J.: Sensors for product characterization and quality of specialty crops—A review. Comput. Electron. Agric. **74**(2), 176–194 (2010)
12. Raid, M., Elgammal, A., Elzanfaly, D.: Efficient management of perishable inventory by utilizing IoT. In: International Conference on Engineering, Technology and Innovation (ICE/ITMC), IEEE, Stuttgart, Germany, June 17–20 (2018)
13. Baietto, M., Wilson, A.D.: Electronic-nose applications for fruit identification, ripeness and quality grading. Sensors **15**, 899–931 (2015)
14. Salinas-Hernández, R.M., González-Aguilar, G.A., Tiznado-Hernández, M.E.: Utilization of physicochemical variables developed from changes in sensory attributes and consumer acceptability to predict the shelf life of fresh-cut mango fruit. J. Food Sci. Technology. **52**(1), 63–77 (2015)
15. Buisman, M.E., Haijema, R., Bloemhof-Ruwaard, J.M.: Discounting and dynamic shelf life to reduce fresh food waste at retailers. Int. J. Prod. Economics. **209**, 274–284 (2019)
16. Watteyne, T., Diedrichs, A., Brun-Laguna, K., Chaar, J.E., Dujovne, D.: PEACH: predicting frost events in peach orchards using IoT technology. EAI Endorsed Trans. Internet Things **16** (5), 1–12 (2016)
17. Kuswandi, B., Wicaksono, Y., Jayus, A., Abdullah, Y.H., Lee, M., Ahmad, M.: Smart packaging: sensors for monitoring of food quality and safety. Sens. Instrum. Food Qual. Saf. **5** (3–4), 137–146 (2011)
18. Sousa-Gallagher, M.J., Tank, A., Sousa, R.: Emerging technologies to extend the shelf life and stability of fruits and vegetables. In: Woodhead Publishing Series in Food Science, Technology and Nutrition. Elsevier, pp. 399–430 (2016)
19. Venuto, D., Mezzina, G.: Spatio-temporal optimization of perishable goods' shelf life by a pro-active WSN-based architecture. Sensors **18**, 1–19. (2018)
20. Annese, V.F., Biccario, G.E., Cipriani, S., Venuto, D.: Organoleptic properties remote sensing and lifetime prediction along the perishables goods supply-chain. Int. J. Smart Sens. Intell. Syst. **S21S**, 130–135 (2014)
21. Kuswandi, B., Nurfawaidi, A.: On-package dual sensors label based on pH indicators for real-time monitoring of beef freshness. Food Control **82**, 91–100 (2017)
22. Jagtap, S., Rahimfard, S.: Utilisation of internet of things to improve resource efficiency of food supply chains. In: Proceedings of the 8th International Conference on Information and Communication Technologies in Agriculture, Food and Environment (HAICTA). CEUR Workshop Proceedings, Chania, Greece, September 21–24, 2030, pp 8–19 (2017)
23. Bhushan, N., Gummaraju, K.: A Petri Net based simulation approach for evaluating benefits of time temperature indicator and wireless technologies in perishable goods retail management. In: Conference on FoodSim. IEEE, Ireland (2002)
24. Biccario, G.E., Annese, V.F., Cipriani, S., De Venuto, D.: WSN-based near real-time environmental monitoring for shelf life prediction through data processing to improve food safety and certification. In: 11th International Conference on Informatics in Control, Automation and Robotics (ICINCO). IEEE, vol. 1, Vienna, Austria, September 1–3, pp. 777–782 (2014)

25. Hertog, M.L.A.T.M., Uysal, I., McCarthy, U., Verlinden, B.M., Nicolai, B.M.: Shelf life modelling for first-expired-first-out warehouse management. Philos. Trans. R. Soc. A, **372**, 1–15 (2014)
26. Jha, S.N., Narsaiah, K., Sharma, A.D., Singh, M., Bansal, S., Kumar, R.: Quality parameters of mango and potential of non-destructive techniques for their measurement—a review. J. Food Sci. Technol. **47**(1), 1–14 (2010)
27. Hong, X., Wang, J.: Use of electronic nose and tongue to track freshness of cherry tomatoes squeezed for juice consumption: comparison of different sensor fusion approaches. Food Bioprocess Technol. **8**(1), 158–170 (2015)
28. Wang, J., Teng, B., Yu, Y.: Pear dynamic characteristics and firmness detection. Eur. Food Res. Technol. **218**(3), 289–294 (2004)
29. Li, C., Gitaitis, R., Tollner, B., Sumner, P., MacLean, D.: Onion sour skin detection using a gas sensor array and support vector machine. Sens. Instrum. Food Qual. Saf. **3**, 193–202 (2009)
30. Ketelaere, B.D., Lammertyn, J., Molenberghs, G., Desmet, M., Nicolai, B., Baerdemaekera, J. D.: Tomato cultivar grouping based on firmness change, shelf life and variance during postharvest storage. Postharvest Biol. Technology. **34**(2), 187–201 (2004)
31. Pasquariello, M.S., Rega, P., Migliozzi, T., Capuano, L.R., Scortichini, M., Petriccione, M.: Effect of cold storage and shelf life on physiological and quality traits of early ripening pear cultivars. Sci. Hortic. **162**, 341–350 (2013)
32. Ignat, T., Alchanatis, V., Schmilovitch, Z.: Maturity prediction of intact bell peppers by sensor fusion. Comput. Electron. Agric. **104**, 9–17 (2014)
33. Ostojic, G., Stankovski, S., Tegeltijia, S., Dukic, N., Tejic, B.: Implementation of IoT for food wastage minimisation. In: XVII International Scientific Conference on Industrial Systems (IS'17), Novi Sad, Serbia, October 4–6, pp. 116–121 (2017)
34. Heising, J.K., Claassen, G.D.H., Dekker, M.: Options for reducing food waste by quality-controlled logistics using intelligent packaging along the supply chain. Food Addit. & Contam.: Part A **34**(10), 1672–1680 (2017)
35. Venuto, D., Mezzina, G.: Automatic perishable goods shelf life optimization in no-refrigerated warehouses by using a WSN-based architecture. In: Applications in Electronics Pervading Industry, Environment and Society, Lecture Notes in Electrical Engineering. Springer Nature Switzerland AG, vol. 550, pp. 287–294 (2018)
36. Witjaksono, G., Rabih, A.A.S., Yahya, N., Alva, S.: IOT for agriculture: food quality and safety. In: IOP Conference Series: Materials Science and Engineering (ICEAMM 2017). IOP Publishing, vol. 343, pp. 1–7 (2018)
37. Reid, D.S., Kotte, K., Kilmartin, P., Young, M.: A new method for accelerated shelf-life prediction for frozen foods. J. Sci. Food Agric. **83**(10), 1018–1021 (2003)
38. Dermesonluoglu, E., Katsaros, G., Tsevdou, M., Giannakourou, M., Taoukis, P.: Kinetic study of quality indices and shelf life modelling of frozen spinach under dynamic conditions of the cold chain. J. Food Eng. **148**(13), 13–23 (2015)
39. Popovic, T., Latinovic, N., Pesic, A., Zecevic, Z., Krstajic, B., Djukanovi, S.: Architecting an IoT-enabled platform for precision agriculture and ecological monitoring: a case study. Comput. Electron. Agriculture **140**, 255–265 (2017)
40. Bing, F.: The research of IOT of agriculture based on three layers architecture. In: 2nd International Conference on Cloud Computing and Internet of Things (CCIOT). IEEE, Dalian, China, October 22–23 (2016)
41. Nobrega, L., Goncalves, P., Pedreiras, P., Pereira, J.: An IoT-based solution for intelligent farming. In: Sensors. MDPI, 19(603), Number 3, pp/ 1–24
42. Luthra, S., Dixit, S.K.M., Kumar, G.A.: Internet of things (IoT) in agriculture supply chain management: a developing country perspective. In: Dwivedi, Y., et al. (eds.) Emerging Markets from a Multidisciplinary Perspective. Advances in Theory and Practice of Emerging Markets, pp. 209–220. Springer Nature, Switzerland AG (2018)
43. Karkkainen, M.: Increasing efficiency in the supply chain for short shelf life goods using RFID tagging. Int. J. Retail. & Distrib. Manag. **31**(10), 529–536 (2003)

44. Duan, Y.E.: Research on integrated information platform of agricultural supply chain management based on internet of things. J. Softw. **6**(5), 944–950 (2011)
45. Jaiganesh, S., Gunaseelan, K., Ellappan, V.: IOT agriculture to improve food and farming technology. In: Conference on Emerging Devices and Smart Systems (ICEDSS). IEEE, Tiruchengode, India, March 3–4 (2017)
46. Mohanraj, I., Ashokumar, K., Naren, J.: Field monitoring and automation using IOT in agriculture domain. Procedia Comput. Sci. **93**, 931–939 (2016)
47. LeBlanc, D., Vigneault, C.: Predicting quality changes of fresh fruits and vegetables during postharvest handling and distribution. Stewart Postharvest Review **4**(1), 1–3 (2008)

Chapter 7
Sensor Information Processing for Wearable IoT Devices

Meetha. V. Shenoy

Abstract Sensing technology is one of the core enablers of IoT and the improvement in sensing technology has lead to the proliferation of small form-factor, cost-effective and accurate sensors for wide variety of wearable applications. With wearable devices receiving widespread acceptance, their requirements are becoming more demanding, with the focus shifting from simple monitoring to context aware intelligent devices. This chapter presents a comprehensive description of the technical opportunities and challenges in the design of sensor information processing systems for wearables. A systematic survey of the state of the art architectures for sensor fusion for different application classes of wearable's is presented. A discussion on design considerations for architecting sensor processing systems, including hardware, networking protocols, and algorithms at the edge, cloud level is provided. The chapter is concluded with a discussion on innovation directions in smart sensing and information processing in wearable devices.

Keywords Sensor fusion · Context-aware · Cloud computing · Neural networks · Fog computing

7.1 Introduction

Making "Sense" of the real world is critical for any IoT application. Sensing technology is one of the core enablers of IoT and the improvement in sensing technology has lead to the proliferation of low form-factor, cost-effective and accurate sensors. Growth in the area of Artificial intelligence and embedded technology has accelerated the deployment of wearable devices. Last decade has witnessed considerable developments in wearable devices for applications such as health monitors, smart clothing, fitness trackers, smart watches, etc. However, despite its growing maturity, there remain numerous challenges in the realm of

Meetha.V. Shenoy (✉)
Birla Institute of Technology and Science, Pilani, Pilani Campus, Jhunjhunu, Rajasthan, India
e-mail: meetha.shenoy@pilani.bits-pilani.ac.in

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_7

sensor information processing that require research effort in order to further the technology. With these devices receiving widespread acceptance in the consumer market, the requirements are becoming more and more demanding, shifting the focus from simple monitoring devices to devices which performs full interpretation of the context and provides intelligent response. This makes it imperative to develop smarter ways to manage the sensed information to actionable information.

A wearable IoT system can be considered to be a 3 tier structure as shown in Fig. 7.1. First tier performs most of the sensing and basic processing of sensed data. The data obtained from the sensors will be transmitted to the second tier which mainly includes the gateways and/or routers which often provides connectivity to an infrastructured network or internet. An example of such a tiered architecture can be explained with an example of Sensoria Smart socks [1]. Sensoria smart socks help the runners and sports enthusiasts to improve their running pattern by identifying and assessing incorrect running styles. The socks which house the sensors and pre-processing unit amounts for the first tier of the architecture. The socks will also have sensors to measure certain environmental parameters along with the physiological parameters of the user, thus providing the context related information. The Sensoria Fitness socks can be paired with a gateway device such as a smartphone which hosts the Sensoria Fitness mobile app. The preprocessed data corresponding to the user movement and the context information will be transmitted to the smartphone which accounts for the second tier of the architecture. The mobile-app implements the required algorithms for interpretation of the data, analysis and visualization. The Sensoria Virtual Coach module within the app continuously checks the running form and provides real-time feedback to the user through video and audio cues. The app pushes the data to cloud services which will also provide predictive analysis of the running pattern based on the context.

An exception to the three tiered architecture mentioned is a wireless sensor system, in which the wearable devices can be the nodes in the network. For example, in an IoT system which tracks the movement of animals in the forest, the end-devices which are mounted on the animals as well as at marked locations in the forest may communicate with the other end-devices in a multi-hop manner before they communicate with a gateway device. The third layer is the cloud level where

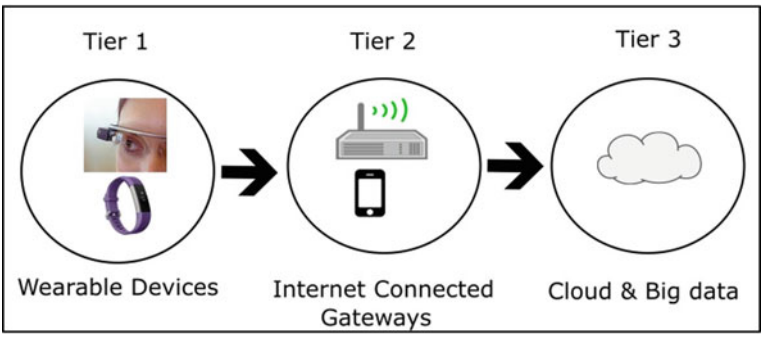


Fig. 7.1 Wearable IoT Device Life Cycle

the large amounts of data are processed, analyzed, stored and the knowledge extraction is performed.

The wearable devices might require fusion of data from multiple sensors to compensate for the individual sensor deficiencies to provide a more accurate assessment of the sensed parameter. Smart sensor fusion will help to develop proactive systems, augmenting the reactive behaviors of wearable devices via predictive maintenance and analytics. Sensor fusion at the first tier will allow high response rate without consuming the communication bandwidth required for transferring the data to the gateway or cloud. The fusion at the end device or the edge level also helps to minimize the security and privacy vulnerabilities. However, current functional limitations of the edge devices in terms of processing power, available memory and power capacity often necessitates the fusion of data to be performed at a gateway or at the cloud. According to a study conducted by ABI research in 2018, the wearable device market can be segmented into seven major groups, i.e. smart phone-compatible watches, smart glasses, sports and activity tracker, cameras, healthcare, smart clothing, and 3D motion trackers [2]. Another study conducted by CCS insight reveals that while the smart watches & wrist bands may continue to find the best market, smart hearable (VI & AI augmented head-sets), wearable cameras, smart eyewear's etc. will also find considerable market share, which implies that wearable devices may have to perform increased level of real-time multi-media processing while the processing power, available energy and memory capabilities still may continue to be limited at the edge device level [3].

Sensor signal processing & sensor fusion require hardware, networking and software elements that intelligently combine data from several sensors to improve overall performance. This book-chapter presents a comprehensive description of the technical opportunities and challenges in designing sensor information processing systems for wearable devices. A brief review of the commercially available non-invasive wearable IoT systems is explained in Sect. 7.2. A systematic survey of the state of the art architectures for sensor fusion for different application classes of wearable devices is presented in Sect. 7.3. A detailed discussion on design considerations for architecting energy and memory efficient sensor information processing systems, including hardware, networking protocols, and algorithms at the edge and fog level is presented in Sect. 7.3. The chapter concludes with an analysis of the innovation directions in smart sensing and information processing in wearable devices.

7.2 Spectrum of Wearable IoT Applications- Challenges and Opportunities

Wearable's are now integral components in larger ecosystem of the Internet of Things (IoT), in which the computing power of all the interconnected elements can be harnessed for collective data acquisition and decision-making. Wearable devices

are expected to acquire and provide information to users in real-time. Wearable smart bands such as Microsoft Band, Fitbit Surge and Jawbone UP Move are devices which measure physical activity, physiological parameters such as sleep, etc. while there are more advanced smart watches which include an embedded OS which provides functionalities and allows installation of third-party applications similar to the ones that are available in smart phones. Current generation of wearable's support handsfree operation and the wearable's deliver actionable information by computation at the device itself or at the gateway level or hosted in an enterprise or public cloud. As such, wearables provide users access to massive computing power while maintaining mobility. The wearable devices are now available which can be work on wrist, arm, ear, head, torso, feet, thigh and so on. A brief overview of the commercially available wearable IoT devices is provided in Table 7.1 which include the broad application classes of non-invasive wearable devices, i.e. smart phone-compatible watches, Wearable Health Devices (WHDs) including devices for healthcare, smart glasses, sports and activity trackers, cameras, smart clothing and 3D motion trackers.

Wearable Health Devices (WHDs) enables continuous ambulatory monitoring of vital parameters of user during activities of daily life, while minimizing interference with activities of daily living, medical diagnosis or even at times facilitating faster recovery from a body injury or a medical intervention. WHDs improve the patient-physician interaction beyond the boundaries of the hospital or clinic. Proactive medical support can be provided to the user based on their health conditions. Most of the currently available devices are not Food and Drug Administration (FDA) compliant; still they do provide reasonable accuracy. The wearable sensors can be classified as non-contact sensors or peripheral sensors and contact sensors. The contact sensors include the ones for monitoring physiological data (ECG, EMG, EEG), chemical (sweat, glucose, saliva) or optical (tissue properties). The contact sensors are also used for emergency relief stimulation during chronic pain or for medication in the form of drug delivery patches. The peripheral and non-contact sensors are mostly deployed in devices for fitness & wellness such as motion assessment (physical activity measurement, calorie count), localization (tracking in Ambient Assisted Living Systems), behavioral analysis (emotional analysis, anxiety, stress measurement), aids for rehabilitation from impairments affecting speech, vision, etc. WHDs are also very useful in monitoring of sport activities, fitness of athlete, military personnel, etc. and as they can provide information to users to better manage their effort and occupational health. Inter-network of wearable sensors, mobile phones and medical infrastructure enable efficient communication between physicians and patients, allowing them to micro-manage interventions, provide feedback on symptoms, and adapt to new treatments.

The vital signs which are generally measured are Heart Rate (HR), Blood Pressure (BP), blood oxygen saturation, respiratory rate, and body temperature. Determining the most suitable sensing technology and the location of mounting of the sensor on human body is critical while designing a wearable module for health monitoring and is still an open area of research. Pulse record can provide insights to

Table 7.1 Brief review of some of the wearable IoT devices and their applications

Worn on	Product	Application
Eye	Glass [4]	Lightweight wearable computer with a transparent display for hands-free operation
Eye	SMI Eye [5]	Captures eye gaze of consumers, athletes, patients and other users allowing them to naturally perform their tasks at hand
Eye	Smart Contact Lens [6]	Assist diabetic people by constantly measuring the glucose levels in their tears
Eye	Atheer dev kit [7]	Augmented Reality supported wearable enabling professionals, such as doctors, technicians, and engineers, to enhance their productivity with distraction free communication and rich information
Ear	Aquapulse [8]	Count calories which are consumed and burned, and monitor the heart rate.
Ear	Dash [9]	Smart earphone which also serves as activity tracker, communicating information such as your heart rate, oxygen levels, and energy levels
Ear	FreeWavz [10]	Smart earphone which records heart rate, oxygen saturation, measure steps, calories burned, report distance, duration and speed
Finger	Nod [11]	Gesture control for TVs, phones, tablets, smart thermostats, smart lighting systems and smart watches
Finger	Xenxo S-Ring [12]	Supports health parameter recording, Google Assistant, Access card, Gesture control, Silent Alarm, NFC payment
Neck	Whistle [13]	Activity monitoring of pets
Neck	Amulyte [14]	Voice Enabled Emergency response system for seniors
Chest	HXM [15]	Capture physiological and biomechanical performance data
Chest	Smart Monbaby [16]	Monitoring of child's breathing movements, body position (on the back or on the stomach), fall detection
Chest	OmSignal [17]	Smart shirt which can track daily steps, calories burned, heart rate, breathing pattern and emotional well-being
Thigh	Leo [18]	Bio-signal monitoring technology which optimizes workouts and reduces the chances of injuries and any other health obstructions
Thigh	Dorsavi [19]	Track the effectiveness of interventions and motion monitoring to reduce the risk of lower limb injury
Torso	Bioharness 3 [20]	Monitor individual's health status (including ECG) so that work levels can be modified to reduce the risk of threats such as heat stress
Head	Fitguard [21]	Head Injury Monitor
Head	IMEC EEG [22]	Measure emotions and cognitive processes in the brain, emotion measurement for therapeutic, learning and gaming applications.
Head	Melon Band [23]	Monitor brain activity and provide feedback to improve brains focus

(continued)

Table 7.1 (continued)

Worn on	Product	Application
Wrist	Kapture [24]	Record 60 sec of audio and transmit to phone
Wrist	Amulet [25]	Detect food allergy
ARM	Shot Tracker [26]	Provide players with in-depth statistical and performance data about the basketball game
ARM	SkinPut [27]	Skinput technology allows the human skin for acoustic transmission so that we can give inputs and information through our skin
Waist	Game Golf [28]	Helps golfers make data-driven decisions during the game considering course and weather conditions
Waist	Lumo Back [29]	Provide posture correction warnings using vibration
Shoulder	Lumo Lift [30]	Provide posture correction warnings
Leg	LegSys [31]	Gait monitoring and fall risk assessment
Feet	Lechal Shoe [32]	Provides haptic feedback, via simple vibrations, providing detailed route guidance at every turn
Feet	Smart SoX [33]	Continuously track foot temperature, sending information to your doctor to help them track issues related to foot inflammation

detecting different critical health conditions such as such as heart ailments, conditions such as clotting of blood in arteries, etc. Pulse sensors can provide useful information for medical purposes as well as for applications such as fitness tracking. Pulse can be recorded from the earlobe, chest, finger tip or wrist. Sensors placed on earlobe and fingertips provide high accuracy, but are not highly wearable when compared to a chest worn system. Wrist mounted sensors are comfortable and preferred for a long term wearable system. Various sensor types such as pressure, ultrasonic, photoplethysmographic (PPG) and radio frequency (RF) are currently available.

PPG sensors include a light source and a photo detector, with red, infrared, or green LEDs [34]. PPG sensors transmit LED light into the artery, and consist of a photodiode mounted suitably to detect the light not absorbed by the blood. Most of the off-the- shelf wearable activity trackers for PPG based HR monitoring use two green light sources because of its robustness against signal noises [34]. Accuracy of pulse readings from PPG sensors, are significantly affected by movements and hence an accelerometer may be used to identify movements. Thus, during the times of high mobility, the device can be switched to a low power mode and recording of the pulse can be stopped. However, there are applications in which pulse statistics may be relevant even when motion is high, such as during exercise or activities of daily living. Studies have demonstrated that the effects of motion on PPG sensors can be reduced by using two LEDs of different light intensities and comparing the amount of light not absorbed by the blood [34].

Pressure based sensors for pulse measurement aim to mimic the role of a healthcare professional who manually reads the pulse by pressing down against the wrist with their fingers. Researchers have developed a highly sensitive pressure

sensor for pulse detection and demonstrated promising results [35]. However, it has to be noted that with increasing sensitivity, sensitivity to noise also increases. The pressure sensor has to be placed firmly against the wrist, and continuous measurement of the pulse can be recorded. This sensor was tested for accurate results under rest conditions, is still requires improvement to provide reasonable results during motion. Pressure sensors and PPG sensors can also be combined such that pulse sensor modules are developed with arrays of PPG sensors and pressure sensor. Diagnostics through pulse sensing is also investigated in some researches where pressure, PPG, and ultrasonic sensors are compared [36]. For respiratory sensors nasal sensors [37] and pressure sensors [38] are common. Pressure sensors are susceptible to noise due to walking, wind, external pressure, etc.

Stretch sensors can also be used for respiration measurement. The properties of stretch sensors change in response to the application of tensile force. The sensors will be stretched during inhalation and exhalation and can be used for respiration measurement [39, 40]. Stretch sensors are highly recommended in future systems for respiration measurement. However, it can be noted that the activities of daily living can cause stretching of the sensor, similar to movement caused due to breathing. Hence, it is imperative that future works should focus on developing techniques and algorithms to improve robustness of stretch sensor based respiration measurement against motion. Estimate of blood pressure (BP) can be obtained through the calculation of Pulse Transit Time (PTT). PTT is the time difference between time at which the pulse recorded at the heart and pulse recorded at another location, such as the earlobe or radial artery [40]. The outcomes of some of the research works indicate that the use of PTT to calculate BP is not yet an accurate solution. Moreover, PPT sensors are obtrusive. PTT is dependent on various physiological factors, such as arterial stiffness. Wearable PPG sensors measure signals from earlobe and wrist to estimate pulse arrival time (or time taken to travel) between these locations and thus estimate blood pressure. The results showed reasonable measurements for healthy subjects, even while measured during the times when the subject is mobile. Most of the pulse oximeters use PPG signals for measurement of blood oxygen. Usually, two types LEDs, red and infrared are directed through the skin. The amount of light not absorbed is measured by receiving photodiodes, and the difference between the received lights is used to calculate blood oxygen. Investigations on implementing power efficient techniques to enable switching of LEDs at appropriate times are being carried out by the researchers. An in-ear reflective pulse oximeter was proposed for situations in which the patient is suffering from conditions such as shock, hypothermia in which the pulse may not be detectable at the fingertips. The sensor (oximeter) can be placed inside the ear canal, ensuring no disruption to hearing.

Electrocardiograms (ECGs) are one of the most crucial biosignals which is used as diagnostic tool for deriving valuable information regarding the cardiac electrical cycle. The ECG waveform (P, Q, R, S, T, U features) is used to analyze the ischemic changes, cardiac cycle, and to treat and predict coronary events including myocardial infractions. ECG records are obtained by sampling the bioelectric currents sensed by several electrodes, known as leads. Generally twelve electrodes

affixed to the skin on the chest, arms, and legs sense the impulses. The P wave, QRS complex, and T wave occur in sequence in a regular pattern with R-R interval in the range 600 ms- 1200 ms for normal heart. Researchers have successfully demonstrated Holter ECG systems with single lead devices, where leads can be placed Lower limb, along the chest area (Right Auricle & Left Auricle). The signals captured by these sensors should be processed via a front end device which performs filtering of power supply noise, DC offset compensation, low pass filter, amplification and analog to digital conversion before the data can be processed in digital domain. Accelerometer or motion detector modules are also utilized to filter out the ECG signal from the noise due to movements. Signal processing techniques such as discrete wavelet transform (DWT), recursive principal component analysis (RPCA), empirical mode decomposition (EMD) based adaptive filter, independent component analysis (ICA), have been applied on the ECG waveform for removing the artifacts due to motion. Nowadays sensors are embedded in fabric as dry electrodes can be used instead of wet electrodes for monitoring (ECG) signals, thus avoiding the need for skin preparation as is required in the use of wet electrode [39]. Even with the proliferation of large number of fitness trackers or health monitoring IoT devices, design of non-obtrusive systems which are robust and reliable is still an open area of research.

While the monitoring of health and fitness parameters is now feasible with the various sensing techniques, the data collected from these devices is not usable until it is associated with a time stamp and location stamp to provide the required context to the data collected. For e.g.: fall detection among elderly is a research area which has got leverage in the IoT community. While time stamping is easier, still accurate tracking of a person or object inside indoor environment is a challenge. Dead reckoning based localization is prone to accumulative errors and beacons (Ultra Wide band, ultrasonic or RF) are utilized to calculate the relative position of the object. This necessitates the use of additional hardware in-addition to Global Positioning System (GPS) receivers in wearable's meant for user tracking in indoor environments. The beacon signals are susceptible to Non-Line-of-Sight (NLOS) conditions due to the presence of obstacles and other moving objects in indoor environments. Hence, localization in indoor environments is challenging when compared to localization in outdoor environments. Range-based beacon based indoor localization is generally implemented in two steps, i.e. (1) estimation of distance between the object to be localized (target node) and beacon nodes and (2) estimation of location of the target. By multiplying the time of travel measurement of the transmitted signal between the beacon node and the target node and the velocity of signal, the distance between the target and beacon nodes can be calculated. NLOS is generally described as the "large and always a positive error that arises when the distance between the transmitter and receiver is estimated from the measurement of signal transmitted between the transmitter and the receiver". In indoor environments, the beacon signals may also get severely reflected and scattered leading to multipath effects. At least three timestamps from different beacon nodes are generally required to calculate the position of an object. The presence of NLOS in even one of the timestamp will provide a completely wrong assessment of

the position of the object. Hence, it is crucial to identify the presence of NLOS in the time stamp measurements. Most of the work available as literature on indoor localization under NLOS conditions is based on the off-line profiling of the indoor deployment area under various NLOS conditions and then using this information for removing NLOS affected timestamps from the measurements. However, it is not feasible to obtain a comprehensive data set containing all possible conditions of NLOS in indoor environments. Also, the requirement of offline training makes the deployment or use of these devices in newer environments challenging as the system can be used only after elaborate training of the device. [41] proposes a localization technique which utilizes artificial neural networks for localization. The system requires training only under LOS conditions, thus enabling faster deployment in new environments. Localization in indoor environments under NLOS conditions still remain an open area of research.

Natural User Interface (NUI) lets users quickly attain mastery in control of appliances/devices with minimum learning. Human computer interfaces (HCI) in near future will be mostly implemented using Gesture based control, especially the Gesture in the air inference is becoming more important in ambient intelligence systems, for Augmented reality (AR) and Virtual Reality (VR) applications [42]. Gesture recognition can be implemented by using wearable electromagnetic devices mounted on special gloves. Another technique is using the principles of computer vision. In this technique, the performance of gesture recognition is highly dependent on the features extracted. Although sensors, such as Microsoft Kinect provide moderately good accuracy, their cost is still prohibitive for use in commercial wearable systems. The accuracy of the optical sensors is dependent on environmental and ambient lighting conditions. For e.g., the attenuation of infrared ray in water could largely limit the use of Microsoft Kinect sensors in water under good light conditions [43].

Devices such Amazon's Alexa or Google assistant are now becoming popular in home automation applications. Soon voice controlled wearable devices will be in demand and performing real time speech recognition on end devices is a challenging task. Sensory Inc announced TrulyNatural—a deep neural net speech recognition technology that combines neural networks with deep learning for acoustic modeling. The network is small enough to fit into an embedded system without compromise to the accuracy. TrulyNatural allows users to speak to devices naturally, and the speech recognition works even when the system is not connected to the Internet, and also ensures that there's no risk of conversations being recorded in a distant cloud unlike what was observed as a privacy breach in case of Amazons Alexa.

Consumer trends indicate that there will be increased demand of wearable's in the next decade and the IoT system architecture including the hardware, software and networking should be designed in a holistic manner to meet the requirements of future systems.

7.3 Architecturing Wearable IoT Devices

Design of an IoT system is typically performed via a top down design methodology. Embedded Systems, Communication & Networking, Sensors and Actuators, Software and Data Analytics are key enablers of IoT systems. Most of the design choices are based on the type of sensing or actuation expected from the IoT system. Sensing and actuation requirements typically end up being the driving factors which decide the kind of computation hardware, algorithm, software components, networking components, analytics, storage and other requirements of the IoT System.

A physical sensor measurement generally suffers from the following problems

- **Sensor Deprivation**: The breakdown of a sensor element causes a loss of perception of the measurand.
- **Limited spatial coverage**: Usually an individual sensor only covers a restricted region.
- **Limited temporal coverage**: Some sensors incurs considerable update rate, thus limiting the maximum frequency of measurements.
- **Imprecision**: Measurements from individual sensors are limited to the precision of the employed sensing element.
- **Uncertainty**: Uncertainty arises due to ambiguous information or missing features in the observation. Uncertainty arises due to the characteristics of the measurand.

Sensor fusion can be defined as combining sensory data or data derived from sensory data such that the resulting information is in some sense better than would be possible when these sources were used individually. The sensor fusion above does not necessarily require that inputs from multiple sensors. The term sensor fusion only says that sensor data or derived from sensor have to be combined. For example, the definition also encompasses sensor fusion systems that takes multiple measurements from a single sensor at different instants of time which are then combined. Sensor fusion can also be classified into (1) Direct fusion, i.e. fusion of sensor data from a set of heterogeneous or homogeneous sensors, soft sensors, and historical values of sensor data. (2) Indirect fusion uses information sources like a priori knowledge about the environment and human input.

Sensor fusion process can also be categorized into three broad classes- complementary, competitive and cooperative [44]. In complementary sensor fusion, independent sensor outputs are combined in order to give a more complete perspective of the measurand or phenomenon being observed. E.g: Camera outputs from different cameras, each observing different parts of a room can be combined to obtain a more holistic observation of the activities in the room. In competitive configuration output of each sensor delivering independent measurements of the same property are combined together. Competitive configurations are used for fault-tolerant and robust systems. E.g. Noise in the image output can be reduced by combining two overlaying camera images. Cooperative sensor fusion uses the information provided by two independent sensors to derive information that would

not be available from a single sensor. E.g. In stereoscopic vision technique, two-dimensional images from two cameras at slightly different viewpoints are combined to derive a three-dimensional image of the observed scene.

Fusion processes are often categorized as low (Raw data or Level 1), intermediate (Feature level or Level 2), or high (Decision level or Level 3), depending on the processing stage at which fusion takes place as shown in Fig. 7.2 [45]. At the Level 1, the data directly obtained from the sensors are fused. For e.g.: an accelerometer providing raw acceleration along the three axes can be used to measure tilt, yaw or pitch of an object. Accelerometer and gyroscope values can be fused together to improve accuracy of tilt, pitch or yaw. The raw data input can at-times be used to extract features. For e.g.: data from an image sensor can be utilized to extract out edges of interest in the image. At the secondary level we can utilize Feature in-Feature out or Feature in-Decision out fusion techniques. E.g. from accelerometer data, movement of object can be observed-say object is static or moving. Higher details such as, whether the object is accelerating or decelerating can be observed through a Feature in-Decision out fusion process. Decisions made at the second level of fusion can be combined together to make higher level of decision as a part of high level fusion. Although all three levels of fusion can be performed at edge, gateway, fog or cloud level- level 1 fusion is predominantly done at edge level, level 2 at fog or gateway level and level 3 fusion is performed mostly at the cloud level.

The Sensor fusion algorithm/methods can be broadly classified into four categories [46]

- Estimation
- Classification
- Inference
- Artificial Intelligence.

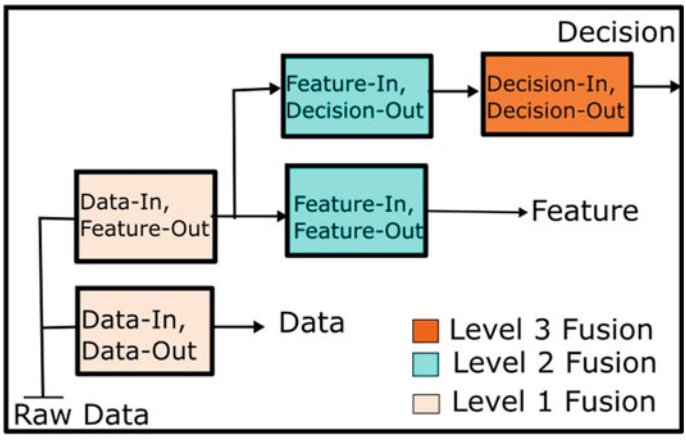


Fig. 7.2 Sensor fusion classification based on sensor configuration

In Estimation methods, if we have a set of redundant observations, the goal is to find the set of parameters that provides the best fit to the observed data. The estimation problem will include finding the values of the vector state such as position, velocity, or size that best fits the observed data. State estimation techniques are also referred in literature as tracking techniques. The estimation techniques are broadly classified into Non-Recursive techniques and Recursive Techniques. Examples of Non-Recursive Techniques include techniques such as—Weighted Average, maximum likelihood, Least squares, and Recursive techniques include– Kalman Filtering, Particle Filter, Extended Kalman Filtering, etc.

In classification techniques, the multidimensional feature space is partitioned into regions each representing a distinct identity class. The partitioning of the feature space can be done based on statistical or geometric parameters, a similarity measure for each observation belonging to the class is calculated in an iterative manner so as to optimize the similarity index. Examples of such techniques include K-means Clustering, Learning Vector Quantization (LVQ), etc. [47, 48].

In Inference techniques, based on the knowledge of the perceived situation provided by the various sources in the data fusion domain, a decision is typically taken. These techniques aim to make a high -level inference about the events and activities that are produced from the measurements. Examples include Bayesian Methods, and Dempster-Shafer Inference [49].

Artificial Intelligence methods have been found to be useful in for solving complex engineering problems that are extremely difficult to be modeled using simple equations. Examples of artificial intelligence techniques are- Support Vector Machines (SVMs), Fuzzy Logic, Artificial Neural Networks, Deep Neural Networks etc.

The sensor fusion techniques are implemented either at the edge level/gateway level or cloud level depending upon the resources available with the nodes and the response characteristics (speed, security) etc. as demanded by the application. Practically all wearable devices must meet design criteria of miniature size, operation at ultra-low power, sensing of physiological or local environmental parameters, and capable of communicating with the network. At the edge level, microcontroller or microprocessor based systems with Embedded OS or custom OS is utilized because of its limited memory availability. Most of these systems may not have a Memory Management Unit (MMU) and as a result a Full OS cannot be utilized in these systems. However, the microcontrollers at the edge level can be embedded microcontrollers which provide less jitter in their interrupt response. The type of computational units deployed inside wearable connected devices is largely influenced by the type of sensing/actuation needed for the application. IoT end devices require some form of wireless/wired connectivity as a mandatory feature and hence integrating the radio baseband on chip is becoming a standard practice. At the edge level instead of using a microcontroller or microprocessor, a System on Chip (SoC) can also be utilized. An SoC will at least have more than one processor (CPU) inside the SoC chip which can be additional CPU core(s), a Digital Signal Processor (DSP) or other General Purpose Processor (GPU). Currently, a number of wearable's make use of digital signal processing (DSP) techniques to extract raw

data from sensors. Especially in the healthcare and personal sensing contexts, such techniques are employed to post-process (removing noise, treating artifacts, applying different filters and extracting features) the information acquired by sensors such as ECG, EEG, EMG, PPG, IMUs and so on. In addition to this, depending upon the target application, SoCs may support dedicated hardware accelerators for supporting specific functionalities. E.g: Artik Series 0 SoCs support General Purpose CRC, Hardware Cryptographic Acceleration for Advanced Encryption Standard (AES) 128/256, Secure Hash Algorithm (SHA)-1, SHA-2, SHA-224, SHA-256, and Elliptic Curve Cryptography (ECC).

While the selection of the computational elements for edge/gateway level is an important design choice to be made in an IoT system, this is not included within the scope of the chapter. However, it is important to know that much of the systems response and behavior will be determined by the edge device nodes which interface with the external world. Dedicated peripheral modules are included in some of the microcontrollers/SoC for specialized functionalities and selection of such SoCs can offload much of the processing burden from the processors. For example, most of the modern wearable systems require data collection from large number of sensors which sense various health parameters. ARTIK 030 SoC support the Peripheral Reflex System (PRS) system, which is a network which lets the different peripheral modules producing the reflex signals (also called as producers) to communicate directly with each other without involving the CPU. The PRS routes the reflex signals to the intended consumer peripherals which can then apply actions depending on the Reflex signals received. These architectural features in computational modules or SoCs will be immensely useful for performance and power optimization in health monitoring applications. Other specialized components may include Power Management Integrated Circuits (PMIC) or dedicated Analog Front End (AFE) circuits. The edge devices may also be required to perform the raw data acquisition and processing, depending upon whether the input signal is an analog, digital or quasi digital signal. For an analog signal the typical processing include buffering, isolation, amplification/attenuation, filtering (anti-aliasing, low pass, high pass, band pass, band stop), level shifting, linearization, etc.

Gateway nodes generally support high levels of data processing, including machine learning. The gateway level SoC nodes mostly support application class CPUs with wired/wireless connectivity, high speed interfaces (such as PCIe, SATA, USB, etc.), DSPs, hardware accelerators and also have sufficient mechanisms to securely connect local devices to the cloud. The major components of edge or gateway level SoCs are shown in Fig. 7.3. Owing to high computing efficiency, Reduced instruction Set Computing (RISC) architecture and high power efficiency, ARM based processors are included in majority of the commercially available computational units used in Internet of Things Domain.

Today, CPUs are utilized for optimized ML and ML-related tasks such as natural language processing. In the current scenario, the trained networks are implemented on edge CPUs and training of the network is performed offline. Studies have shown that despite memory and compute constraints, many complex neural networks have been deployed on MCUs. Techniques such as pruning and

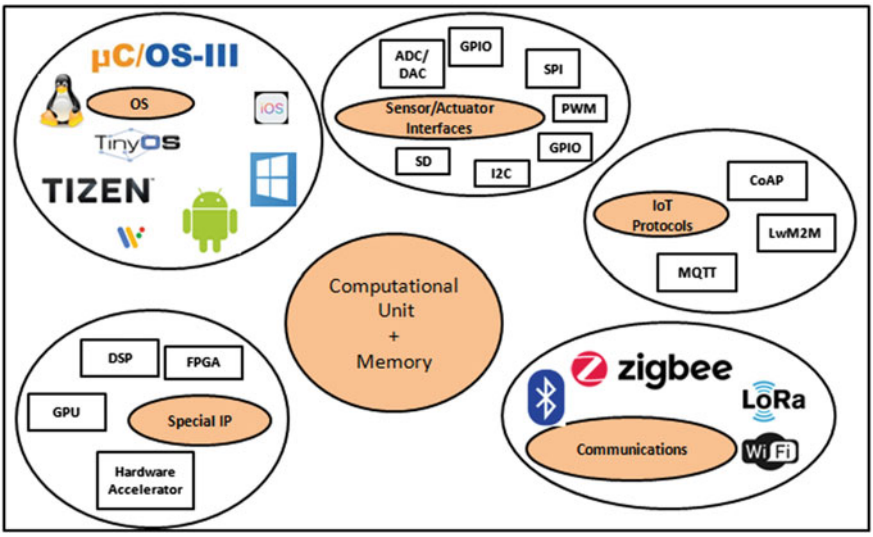


Fig. 7.3 Components of edge or gateway level SoCs

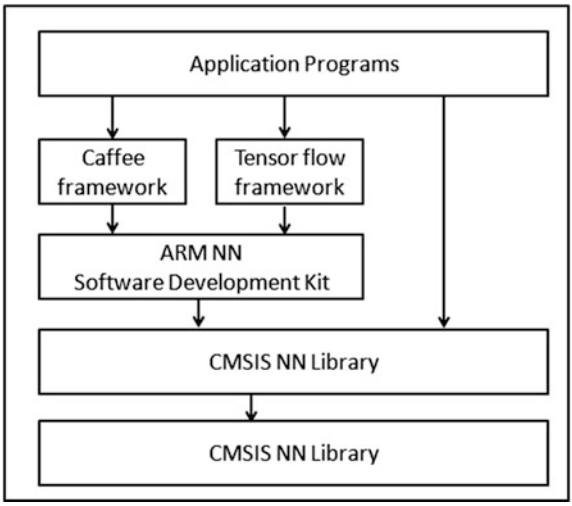


Fig. 7.4 CMSIS-NN and ARM—ANN architectures for neural network implementation

quantization help to compress the neural networks to make them suitable for deployment on CPUs, Neural Processing Units (NPUs) and GPUs. The neural network must also be updated securely over time via over the air programming. ARM designs are being designed to incorporate the need for enabling neural network deployment on edge devices. A team of ARM engineers have demonstrated scalable and secure remote updates from the cloud to neutral nets deployed on MCUs. They used an Mbed OS-enabled Arm Cortex-M4 running at 100 MHz,

Google TensorFlow and the ARM Pelion Device management platform for updating the neural network. Helium feature, introduced with the ARMv8.1-M architecture, is a new optmized vector architecture for the Cortex-M architecture that delivers up to 15× performance improvement for AI applications.

Running standard ML frameworks such as Keras or Tensorflow on Cortex-M systems is impractical. CMSIS-NN, is a collection of efficient neural network kernels which are provided by ARM for Cortex-M series of processor cores. The kernels are designed to maximize the performance and minimize the memory utilization of neural networks. Arm NN translates trained model to the code that runs on Cortex-M cores using CMSIS-NN functions Fig. 7.4. CMSIS-NN APIs may also be directly used in the application code.

The mid-level CPU architectures support embedded OS on which third-party applications can be installed similar to the ones available in smart phones which utilize full application class OS. While the versions of traditional OS such as iOS, windows, Linux are widely in use, dedicated OS are being developed for wearable application. Examples include Android Wear, Wear OS by Google, MediaTek LinkIt, Tizen, etc. Smart devices need an OS to run applications and services to support Internet of Things protocols. Several Software Development Kits (SDKs) and REpresentational State Transfer (REST) Application Programming Interfaces are available now to support users as well as third- party developers. Users can gain access to the data collected by the wearable's, using services available on these platforms and third-party developers can build new applications and services.

Generally the smart device architectures can be divided into three categories [50]

- Method 1: Edge devices with or without SDK, collect data directly from the sensors in the wearable. The architecture is shown in Fig. 7.5. In such systems, an application installed on a smart phone collects data from the wearable. For this, the native app running in the smart phone subscribes to the events recorded using wearable. The wearable sends out periodic notification of the new data and the smart phone collects it. Transfer is commonly done using Wi-Fi or Bluetooth Low Energy protocols.

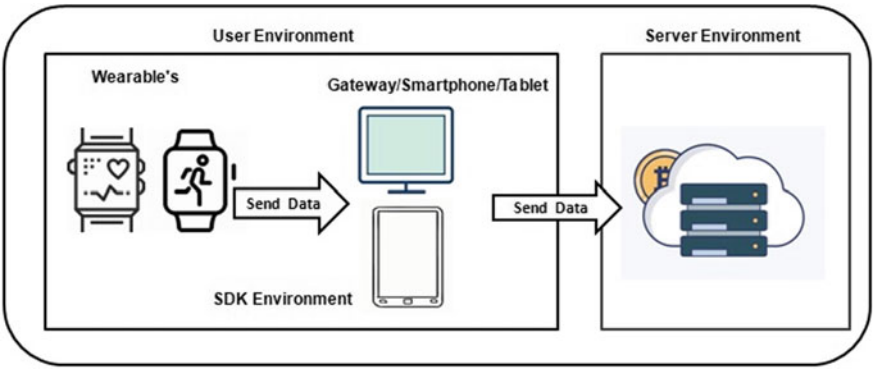


Fig. 7.5 Data transfer architecture—method 1 [50]

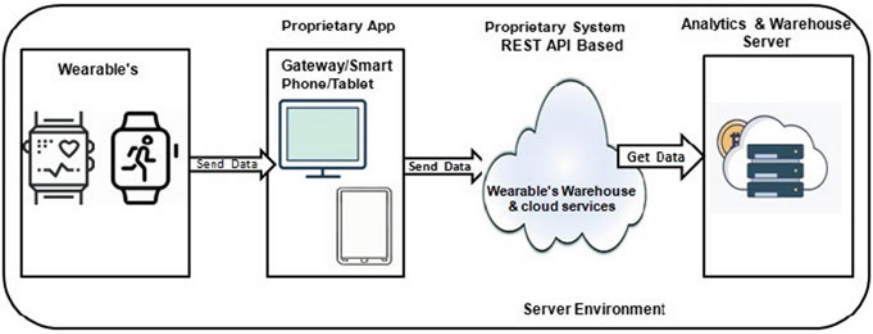


Fig. 7.6 Data transfer architecture—method 2 [50]

- Method 2: The wearable sends data to its proprietary app which resides on a PC or smart phone, which serves as a gateway transmitting the data towards the server. Wearable devices send the data to the intermediate application residing on PC or smart phone wirelessly. This data is stored locally and then transmitted only at periodical intervals to the application to minimize the energy consumption. The interval has to be decided based on the memory capacity of the wearable so as to ensure no data loss. The REST APIs are utilized by third-party systems/analytic servers to request data from wearable warehouse. This architecture is depicted in Fig. 7.6.
- Method 3: In this architecture indirect access is granted to the proprietary warehouse using an intermediate smart phone. The Smartphone or tablet will support SDK environment. An application running on the smart phone/tablet receive the data from the proprietary warehouse and cloud service. The app sends the data to the third-party server. This architecture is depicted in Fig. 7.7. This architecture may be utilized in the cases in which the warehouse allows operation from the SDK but does not provide a REST API.

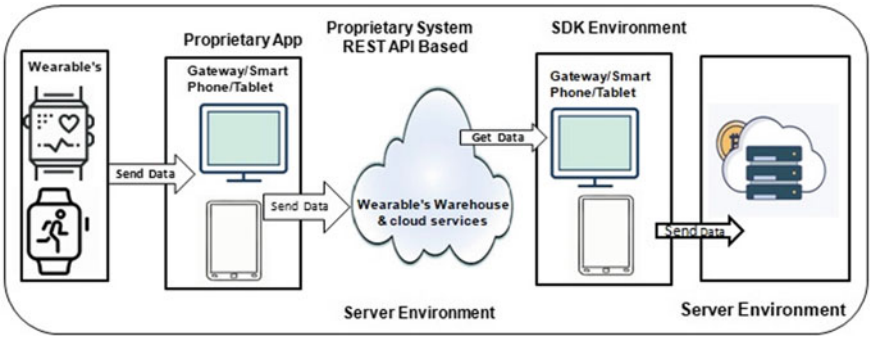


Fig. 7.7 Data transfer architecture—method 3 [50]

In RESTful implementation, a server owns the state of the resource but the state is not transferred in a message from client to server. RESTful implementations utilize HTTP methods such as PUT, POST, GET and DELETE to place requests. No broker or middle agent is required in this implementation. As they are based on HTTP, they support majority of HTTPS security services. RESTful implementations are typically client-server architectures and initiate access to the resources through request-response patterns. Another example of RESTful service is the Constrained Application Protocol (CoAP). CoAP is based on the concept of mimicking and replacing HTTP abilities and usage with a light weight equivalent for IoT. CoAP is build upon UDP unlike TCP/UDP for a normal HTTP session.

An alternative to the RESTful implementation is the use of Message oriented Middleware (MOM) implementation. In MOM the communication between devices takes place through message queues which are distributed. The device which produces data places in the queue and the consumer obtains the data from the queue. Some implementations of MOM such as Message Queuing Telemetry Transport (MQTT) requires a broker or middleman to provide the central service. In such situations the producers and consumers must establish a publisher-subscriber relationship with the broker. Advanced Message Queuing Protocol (AMQP), Streaming Text Oriented Messaging Protocol (STOMP) are popular MOM implementations other than MQTT. A variant of MQTT called as MQTT-SN (sometimes referred to as MQTT-S) for constrained devices is available. While being lightweight as similar to MQTT, the MQTT-S is designed specifically for low-bandwidth links in wireless personal area network. MQTT-S supports link failure, short message length and resource constrained hardware.

'Cloud' typically refers to an infrastructure of computing services that are generally on-demand. The resources such as computing, networking, storage and associated software services can be dynamically scaled up or down based in the load conditions or required quality of service constraints. Clouds are typically data centers that provide services to customers on a pay-for-use model. The clouds typically use geographically dispersed resources providing scalability and fault tolerance. Cloud service providers generally provide services which include Networking as Service (NaaS), Software as Service (SaaS), Platform as Service (PaaS) and Infrastructure as Service (SaaS).

Shown below is a typical flow of data in an end-to end wearable IoT system. Figure 7.8 provides a typical flow of data of an IoT system. The analytics portion of cloud which performs the prediction and response can be different entities such as Complex Event Processing (CEP), Rule Engines, Stream Processor, Lambda Architecture, etc. CEP is commonly used for pattern detection and it uses SQL-like queries, but rather than using a database backend, it searches an incoming stream for the pattern or rule suggested. Since, it uses SQL-like semantics, it is designed to be appreciably faster than a regular database query. Lambda Architecture analytics engine helps to perform batch processing on massive datasets.

The major issue with relying on the cloud services is the latency associated with the transfer of information to the cloud and the processing latency as represented in Fig. 7.9. Also, with the widespread proliferation of IoT devices, available

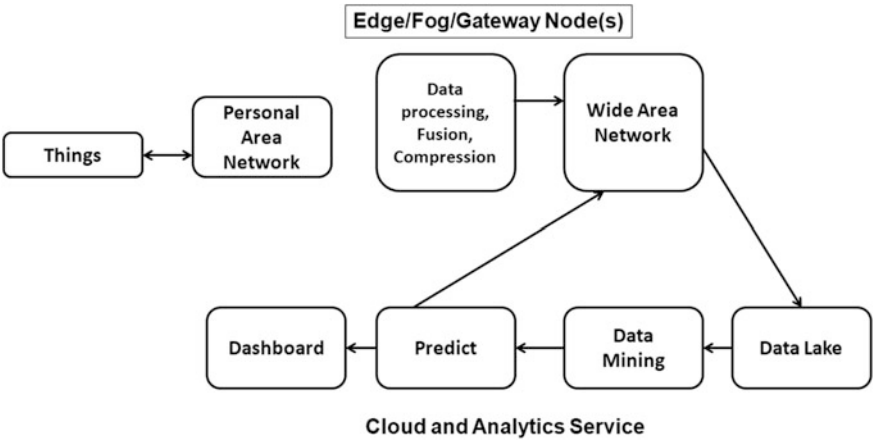


Fig. 7.8 Typical IoT data flow representation

bandwidth limitations will also pose serious limitations on cloud based analytics and force the computing to be performed as close to the source of data generation. Recently, the concept of fog computing is getting prominence. Fog is a decentralized computing paradigm which proposes to extend the cloud services closer to IoT edge devices by acting as an intermediate layer between the traditional cloud and the edge devices. In primary concept behind 'Fog computing' is to migrate at least some of the tasks of data centers or clouds to fog nodes situated at the edge of the network.

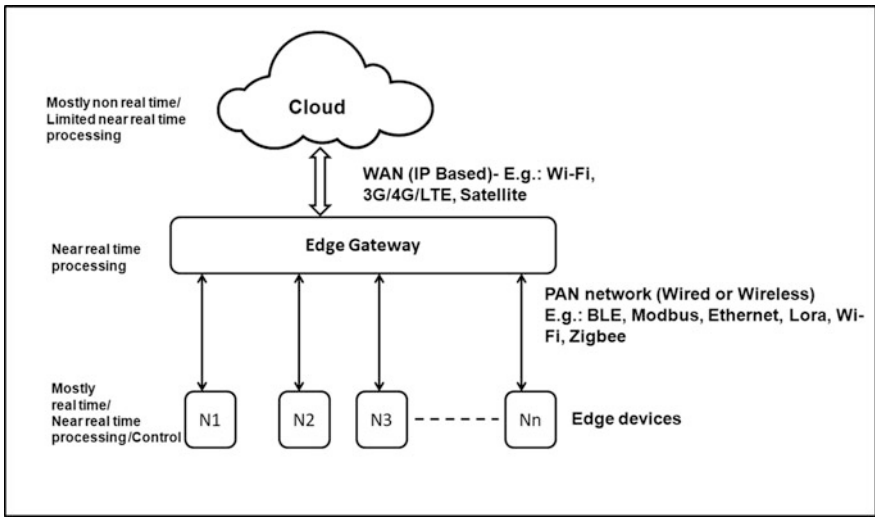


Fig. 7.9 IoT multi-level data processing and latency issues

7.4 Conclusions and Future Directions

The concept of the Internet of Things (IoT) emerged in the 1980s and became popular in late 1990s. Currently, IoT applications exist in nearly every field (e.g., healthcare systems, energy management and transportation systems, building and home automation, environmental monitoring, infrastructure management), and are playing an increasingly important role in our daily life. According to the Federal Trade Commission (FTC), "the number of IoT devices has already outnumbered the number of people in the workplace [51], and the number of wireless devices connected to the Internet of Things will be about 26 billion by 2020 and will greatly out number hub devices (smartphones, tablets and PCs)". IoT will assist in the optimization of processes through advanced data analytics, and will be the catalyst for new market segments, giving rise to cross-cutting applications and services.

Developments are expected to happen in every technology, enabling Internet of Things and the scope of emerging products will be limited by only ones imagination. For example, while we do have flexible displays already in market, future beholds rollable displays which can be rolled or unrolled to increase or decrease the screen size. The newer applications may include systems which can automatically detect human emotions, read the mind and receive commands using miniature versions of brain computer interfaces. The wearable's can revolutionize the field of geriatric care by providing services such as automatic medication reminders, support telemedicine facilities, prevent falls, etc. This will allow the elderly to feel secure and safe at home while also being independent to a great extent. Using the wearables, it will be possible to track the elderly in indoor environments and the caregivers can remotely monitor the elderly. Similarly, with the implementation of smart cities and buildings, it should be possible to track any user wearing the smart device in indoors or outdoors.

As the scope of IoT expands and becomes more ubiquitous in our daily lives, it is vital that we secure the systems and ensure the privacy of users. Security implies that the data is protected from unauthorized users while being transferred, collected, processed and remains safely stored. On the other hand, privacy suggests the authority to control the gathering and usage of one's personal information. Listed below are some examples of the security and privacy breaches reported in IoT systems which are introduced through the network in the last few years.

- Hacking of automobile using a smartphone: Researchers at the University of Washington were able to demonstrate attack on a car's Bluetooth system; the system which enables drivers to make hands-free cell phone calls [52]. The attackers could send commands and override several of the vehicles controls.
- At the Midwestern medical facility chain, attackers were able to attack the IoT-enabled defibrillators and manipulate the control system to deliver shocks to a patient's heart. The study also demonstrated that the attacker could also have prevented a medically needed shock from being administered [53].

- Experts at Bit defender demonstrated a security attack targeted at a Samsung Gear Live smart watch that was paired with a Google Nexus 4 smartphone [54]. The attacker was able to decode a user's data, including Google Hangout messages and Facebook conversations.
- According to Wessex Institute of Technology Press, "A researcher at Tech Leader, AppSec Labs executed a Man-in-the-Middle attack on a Bluetooth smart mobile app [55]. The smart bracelet selected for the attack was a Dax-Hub SW-28 smart bracelet, which is a bracelet that captures information on an individual's sports activities, as well as other health related data".
- Several studies reveal that the digital information and/or RF trace obtained from a smart home can be used by adversaries to determine if the house is occupied or to track users movements [53, 54]. This information can be used by adversaries to even rob a house or apartment.
- In 2018, a woman in Portland, Oregon found out that her family's home digital assistant, Amazon's Alexa, recorded a private conversation inside the house and without her permission or awareness, transmitted the audio recording to a random person on their contacts list [56].

Even though IoT offers immense potential to make human lives easier, the wide spread deployment is not viable unless these systems are secured from vulnerabilities.

- According to a study conducted by IDC Worldwide Security Predictions in 2016, "two-thirds of enterprises are expected to experience IoT security breaches by 2018. By 2020, more than 25% of identified enterprise attacks could be IoT-related—but IoT security accounts for only 10 percent of IT security budgets."
- According to the study conducted by Aruba Networks in 2017, "Among 3100 companies which they surveyed globally, just over half have implemented IoT —and 84% have already experienced a security breach as a result."
- According to AT&T's Cyber security Insights Report published in 2016, "among more than 5000 enterprises surveyed around the world, 85% are, or will be, deploying IoT devices—yet just 10% feel confident about securing those devices against hackers".

IoT security breach statistics is a cause for major concern for even the IoT system developers today. Having said that, we cannot play 'defense' and avoid the benefits of IoT. Due to the intrinsic capability limits of edge devices, it is challenging to implement traditional methods to secure IoT systems, which opens up door for further exploits and attacks. Although several independent studies have exposed several security and privacy vulnerabilities and suggested/implemented the methods to make the systems robust, there is a need to formalize the methods of evaluating ethical standards, security and privacy risks of IoT systems.

The fog computing paradigm will gain significant boost in the upcoming years. Currently most of the edge devices execute the trained neural networks. It is expected that reconfigurable architectures including FPGAs will find significant

importance and the neural networks can be dynamically trained in the edge devices itself. This will further open up several application areas. Another frontier in the wearables is the concept of distributed computing. The wearable devices can cooperate with each other and then perform the complex signal processing functionalities by sharing the resources of multiple wearables in a secured manner. As the computation and storage of data collected from the wearable devices is performed in a distributed manner, Blockchain technology will find a critical role in securing these systems.

A large number of wireless and wired networking technologies are utilized in the field of IoT. The key is to identify the major security and privacy vulnerabilities in the wireless/wired networks and formalize their security & privacy risk assessment methodologies. Development of a field portable system which will evaluate the security and privacy of the system during development as well as offer continued risk assessment post the deployment might be a need of the hour. Continued support post deployment is of significance as the IoT systems co-exist with other networks and some of the IoT systems are incrementally developed over a period of time.

Development of low power, multi-modal biopotential analog front end (AFE) with support of energy harvesting would continue to be a critical factor which will assist the development of future wearables. Also, to enable complex signal processing which offers high performance/watt, the development of hardware accelerators for identification or removal of signal artifacts may become inevitable. Energy harvesting and storage from human motion, ambient radio frequency, body heat, etc. is another promising area of research.

Having discussed the possibilities offered by wearable devices, the wide-spread use of wearable technology will only be possible with a paradigm shift in the user-perception towards accepting the invasion of these devices to our daily lives.

References

1. Sensoriafitness.com: Sensoria Fitness. [online] Available at: http://www.sensoriafitness.com/smartsocks/ (2019). Accessed 25 Jul 2019
2. Abiresearch.com: Wearable Device Market Share and Forecasts. [online] Available at: https://www.abiresearch.com/market-research/product/1019580-wearable-device-market-share-and-forecasts/ (2019). Accessed 25 Jul 2019
3. Insight, C., Portela, R., Wood, B.; Optimistic Outlook for Wearables—CCS Insight. [online] CCS Insight. Available at: https://www.ccsinsight.com/press/company-news/optimistic-outlook-for-wearables/ (2019). Accessed 25 Jul 2019
4. Cognolato, M., Atzori, M., Müller, H.: Head-mounted eye gaze tracking devices: an overview of modern devices and recent advances. J. Rehabil. Assist. Technol. Eng., **5** (2018)
5. Park, J., Kim, J., Kim, S., Cheong, W.H., Jang, J., Park, Y.G., Ung, Jang: Soft, smart contact lenses with integrations of wireless circuits, glucose sensors, and displays. Appl. Sci. Eng. **4**(1), 1–12 (2018)
6. Atheer: The Standard for Enterprise Augmented Reality (AR)|Atheer. [online] Available at: https://atheerair.com/ (2019). Accessed 25 Jul 2019

7. Hänsel, K., Katevas K., Orgs, G., Richardson, D.C., Alomainy, A., Haddadi, H.: The potential of wearable technology for monitoring social interactions based on interpersonal synchrony. In: Proceedings of the ACM Conference on Wearable Systems and Applications (WearSys) (2018)
8. Bonato, P.: Advances in wearable technology and applications in physical medicine and rehabilitation. J. Neuroeng. Rehabil. **2**(1) (2005)
9. Aliverti, A.: Wearable technology: role in respiratory health and disease. Breathe **13**(2), 27–36 (2017)
10. Shilkrot, R., Huber, J., Urgen, J., Nanayakkara, S., Maes, P.: Digital digits : a comprehensive survey of finger. ACM Comput. Surv. **48**(2) (2015)
11. Xenxo: Xenxo—The World's Smartest Ring that you have been Waiting for. [online] Available at: https://www.xenxo.pro/ (2019). Accessed 25 Jul 2019
12. Yatani, K., Truong, K.N.: BodyScope: a wearable acoustic sensor for activity recognition. In: The Proceedings of ACM Conference on Ubiquitous Computing, pp. 341–350 (2012)
13. Tedesco, S., Barton, J., O'Flynn, B.: A review of activity trackers for senior citizens: research perspectives, commercial landscape and the role of the insurance industry. Sensors, **17**(6) (2017)
14. Dias, D., Cunha, J.S.: Wearable health devices—vital sign monitoring, systems and technologies, Sensors, **18**(8) (2018). https://doi.org/10.3390/s18082414
15. Venkataramani, D., Jadhav, A., Wadzirkar, S., Ambekar, J., Dive, K., Sharma, S., Khadse, G.: Infant monitoring using wearable computing. Int. J. Eng. Tech. Res. **11**(3), 95–98 (2015)
16. Bennett, J., Rokas, Chen L.: Healthcare in the smart home: a study of past. Present. Futur., Sustain. **9**(5), 1–23 (2017). https://doi.org/10.3390/su9050840
17. Wearabletechdigest.com: Leo Fitness Intelligence- A Wearable Tracking Your Body's Biosignal. [online] Available at: https://www.wearabletechdigest.com/leo-fitness-intelligence.html (2019). Accessed 25 Jul 2019
18. dorsaVi EU: ViMove2: Analyse Patient Movement & Muscle Activity—dorsaVi EU. [online] Available at: https://www.dorsavi.com/uk/en/vimove/ (2019). Accessed 25 Jul 2019
19. Dubosson, F., Ranvier, J., Bromuri, S., Calbimonte, J., Ruiz, J., Schumacher, M.: The open D1NAMO dataset: a multi-modal dataset for research on non- invasive type 1 diabetes management. Inform. Med. Unlocked **13**, 92–100 (2018)
20. Chalif, B.: Dartmouth Computer Science Technical Report TR2016-805. Security and Privacy Analysis of Medical Wearables (2016)
21. Miao, F., Cheng, Y., He, Y., He, Q., Li, Y.: A wearable context-aware ECG monitoring system integrated with built-in kinematic sensors of the smartphone. Sensors **15**(5), 11465–11484 (2015). https://doi.org/10.3390/s150511465
22. Marin, J.: Octopus: a design methodology for motion capture wearables. Sensors **17**(8), 1–24 (2017). https://doi.org/10.3390/s17081875
23. Wearable Tech|CrunchWear: Kapture—Wearable Tech|CrunchWear. [online] Available at: https://crunchwear.com/category/companies/kapture/ (2019). Accessed 25 Jul 2019
24. Hester, J., Peters, T., Yun, T., Peterson, R., Skinner, J., Golla B., Sorber, J.: Demo abstract: the amulet wearable platform. In: Proceedings of the ACM Conference on Embedded Network Sensor Systems (SenSys), pp. 290–291 (2016)
25. Shottracker.com: ShotTracker| Automatically captures statistics for your entire team—Klaycamp Site. [online] Available at: https://shottracker.com/klaycamp (2019). Accessed 25 Jul 2019
26. Skinput: Appropriating the Body as anInput Surface. Available at: http://www.chrisharrison.net/index.php/Research/Skinput (2019). Accessed 25 Jul 2019
27. Game Golf Pro: Available at: https://www.gamegolf.com/home/?v=27f1fb0 (2019). Accessed 25 Jul 2019
28. LumoBack: Available at: https://www.mobihealthnews.com/tag/lumoback (2019). Accessed 25 Jul 2019
29. Anon: [online] Available at: https://vandrico.com/wearables/device/lumo-lift (2019) Accessed 25 Jul 2019

30. Wang, W., Adamczyk, P.G.: Analyzing gait in the real world using wearable movement sensors and frequently repeated movement paths. Sensors **19**(8) (2019)
31. Hegde, N., Bries, M., Sazonov, E.: A comparative review of footwear-based wearable systems. Electronics **5**(4) (2016)
32. Sensoriafitness.com: Sensoria Home Page. [online] Available at: https://www.sensoriafitness.com/ (2019). Accessed 25 Jul 2019
33. Lee, H., Ko, H., Jeong, C., Lee, J.: Wearable photoplethysmographic sensor based on different LED light intensities. IEEE Sens. J. **17**(3), 587–588 (2017)
34. Shu, Y. Li, C., Wang, Z., Mi, W., Li, Y., Ren, T.L.: A pressure sensing system for heart rate monitoring with polymer -based pressure sensors and an anti-interference post processing circuit, Sensors **15**(2), 3224–3235 (2015)
35. Zuo, P., Wang, D.Zhang: Comparison of three different types of wrist pulse signals by their physical meanings and diagnosis performance. IEEE J. Biomed. Health Inform. **20**(1), 119–127 (2016)
36. Milici, J., Lorenzo, A., Lázaro, R., Villarino, D.Girbau: Wireless breathing sensor based on wearable modulated frequency selective surface. IEEE Sens. J. **17**(5), 1285–1292 (2017)
37. Mahbubet, et al.: A low-power wireless piezoelectric sensor-based respiration monitoring system realized in CMOS process. IEEE Sens. J. **17**(6), 1858–1864 (2017)
38. Atalay, O., Kennon, W.R., Demirok, E.: Weft-knitted strain sensor for monitoring respiratory rate and its electro-mechanical modeling. J. IEEE Sens. **15**(1), 110–122 (2015)
39. Aqueveque, C., Gutiérrez, F., Rodríguez, S., Pino, E.J., Morales, A., Wiechmann, E.P.: Monitoring physiological variables of mining workers at high altitude. IEEE Trans. Ind. Appl. **53**(3), 2628–2634 (2017)
40. Griggs, D., et al.: Design and development of continuous cuff-less bloodpressure monitoring devices. In: The Proceedings of IEEE SENSORS, pp. 1–3 (2016)
41. Shenoy, M.V., Karuppiah, A., Manjarekar, N.: A lightweight ANN based robust localization technique for rapid deployment of autonomous systems. J. Ambient Intell. Humaniz. Comput. (2019). https://doi.org/10.1007/s12652-019-01331-0
42. Escalera, S., Athitsos, Vassilis, Guyon, I.: Challenges in multimodal gesture recognition. J. Mach. Learn. Res. **17**, 1–54 (2016)
43. Xu, P.: A Real-time hand gesture recognition and human-computer interaction system. CoRR, Vol. abs/1704.07296, pp. 1–8 (2017)
44. Dasarathy, B.V.: Sensor fusion potential exploitation innovative architectures and illustrative applications. Proc. IEEE, 24–38 (1997)
45. Durrant Whyte, H.F.: Sensor models and multisensory integration. Int. J. Robot. Res. **7**(6), 97–113 (1988)
46. Elmenreich, W., Pitzek, S.: Using sensor fusion in a time-triggered network. In: Proceedings of the 27th Annual Conference of the IEEE Industrial Electronics Society, Denver, USA, vol. 1, pp. 369–374 (2001)
47. Luo, R.C., Chou, Y.C., Chen, O.: Multisensor fusion and integration: Algorithms, applications, and future research directions. In: Proceedings of the 2007 IEEE International Conference on Mechatronics and Automation, ICMA 2007, vol. 2(2), pp. 1986–1991. https://doi.org/10.1109/ICMA.2007.4303855 (2007)
48. Ribas, A.D., Colonna, J.G., Figueiredo, C.M.S., Nakamura, E.F.: Similarity clustering for data fusion in Wireless Sensor Networks using k-means. In: Proceedings of the International Joint Conference on Neural Networks, pp. 1–7, (2012)
49. Smaili, C., El Najjar, F.: Multi-sensor fusion method using Bayesian network for precise multi-vehicle localization. In: Proceedings of the IEEE Conference on Intelligent Transportation Systems, ITSC, pp. 906–911 (2008). https://doi.org/10.1109/ITSC.2008.4732643
50. Federal Trade Commission Staff Report: Internet of Things—Privacy and Security in a Connected World; FTC: Seattle. WA, USA (2013)

51. Naone, E.: Taking Control of Cars from afar. 14 March 2011. Available online: https://www.technologyreview.com/s/423292/taking-control-of-cars-from-afar/ (2011). Accessed on 11 April 2016
52. Kijewski, M.: The Medical Devices Most Vulnerable to Hackers. Available online:https://www.medtechintelligence.com/feature_article/medical-devices-vulnerable-hackers/ (2018). Accessed on 10 April 2018
53. Paganini, P.: Smartwatch Hacked, How to Access Data Exchanged with Smartphone, 11 December 2014. Available online: http://securityaffairs.co/wordpress/31007/intelligence/smartwatch-hacked.html (2014). Accessed on 5 April 2018
54. Fitbit.com: Fitbit Versa|Smartwatch Family. [online] Available at: https://www.fitbit.com/in/versa (2019). Accessed 25 Jul 2019
55. Melamed, T.: An active man-in-the-middle attack on bluetooth smart devices. Int. J. Saf. Secur. **8**, 200–211 (2018)
56. Arriba-Pérez, F., Caeiro-Rodríguez, M., Santos-Gago, J.M.: Collection and processing of data from wrist wearable devices in heterogeneous and multiple-user scenarios. Sensors (Switzerland), **16**(9) (2019). https://doi.org/10.3390/s16091538

Chapter 8
Cyber-Physical Cloud Computing Systems and Internet of Everything

Maninder Jeet Kaur, Sadia Riaz and Arif Mushtaq

Abstract The Industry 4.0 is experiencing massive transition in terms of performance and cost efficiency due to the emergence of Disruptive technologies. This applies in particular to smart computing on a big scale such as Cyber Physical Systems (CPS), Cloud Computing, the Internet of Things (IoTs), the Internet of Everything (IoE), Robotics (Mechatronics), Renewable Energy Systems, Autonomous vehicles and Intelligent Cities/Devices. CPS integrates networks, computations and physical processes to control process, respond, give feedback and adapt to changing conditions in the real time. Success of Industry 4.0 is confronted by disruptive CPS difficulties regulated by IoTs and IoE; integration with machine learning functionalities, cloud computing and growing but challenging concentration on the main fields of Big Data Analytics, Virtualization, and Automation. The chapter synthesizes existing literature to highlight drastic alterations that Industry 4.0 will apply on manufacturing systems and processes and explores the various domains revolving around CPS, challenges, applications and the ecosystem. It discusses studies and ways of implementing solutions that have been simplified using standards and systematic methods of investigation.

Keywords Internet-of-Things (IoTs) · Industry 4.0 · Cyber Physical Systems (CPS)

8.1 Introduction

In some certifiable frameworks, computational and physical assets are carefully interconnected: installed PCs and correspondence systems oversee physical actuators that work in the outside world and get contributions from sensors, making a

M. J. Kaur (✉)
Amity University Dubai International Academic City, Dubai, UAE
e-mail: mani356@gmail.com

S. Riaz
SP Jain School of Global Management, Dubai International Academic City, Dubai, UAE

A. Mushtaq
City University College of Ajman, Dubai, UAE

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_8

shrewd control circle equipped for adjustment, self-sufficiency and improved proficiency. These are known as Cyber-Physical Systems (CPS). The prefix "cyber" is an extended derivation of the Greek adjective "kyberneticos" ("cybernetic") that implies being talented in guiding or overseeing. Likewise, Aristotle used the word "cybernetic" to denote "technology of governance". Thus, the term was used by Ancient Greeks to support different contextual implications [1].

Sztipanovits characterizes Cyber-Physical Systems as "a new discipline of research that is at the intersection of the sciences of physics, biology, engineering and information" [2]. Konrad Zuse was a pioneer in digital physical frameworks as he built an extraordinary gadget for the examination of airship wings not long after the innovation of the Z3 in 1941; the main fully practical program that could control computational machine. Zuse later considered this assembly the main continuous PC. This programmed PC could read from around forty sensors filling in as simple to-advanced converters, and prepared these qualities as input factors inside a program. The substantial output of Zuse's finding was that constant capacities, reactivity, control building, programming and physical assets are inborn part of digital physical frameworks [3].

CPS combines the ability to calculate and correspond with the physical environment. CPS was recognized by the US National Science Foundation (NSF) as a crucial study area in 2008 and was acknowledged by the US President's Council of Advisors on Science and Technology as the main research need of the recent times [4]. CPS relies on sensors, retrieval and virtualization. Continuing developments in remote sensor systems, Internet of Things, and cloud computing make CPS an amazing candidate for some apps that will be considered later in this chapter. Whatever it may be, remote sensor systems collect the information and are seriously prepared to limit vitality, preparation and capacity, hence are relatively weak systems. It is primarily due to their inability to store large amounts of information and lack of required assets to process information. To resolve these issues, distributed computing can possibly provide answers or solutions. The continuous contemporary research is attempting to utilize and establish Cloud Computing advancements as the computational spine of CPS to improve the adaptability of the framework and to empower investigation of the constant information. Distributed computing interestingly deploys computing infrastructure that can be approached by anyone or individual whenever from anyplace on the planet. This platform is like an active administration that offers figuring, stockpiling, systems management, and programming as an administration. Authors in [5] have characterized Cloud Computing as: "cloud is a parallel and appropriated processing framework comprising of a gathering of interconnected and virtualized PCs that are powerfully provisioned and exhibited as at least one brought together registering assets dependent on the administration level understandings (SLA) set up through exchange between the specialist co-op and purchasers".

Along these lines, from the definitions, it tends to be accepted that the cloud ought to have following attributes: (1) self-administration, (2) per-utilization metering and charging, (3) versatility and (4) customization. Two parts of Cloud Computing are communicating to the end clients; first, clients can get to individual

information and applications utilizing any PC associated with the Internet, and second, programming applications are not required to be introduced in the client's PC and as they are accessible on the cloud. Besides, Cloud Computing suppliers offer different programming administrations, APIs and improvement instruments for designers. These empower the clients to move their processing framework to the cloud. The Cloud Computing is the consequence of headway of couple of innovations, for example, disseminated registering, Internet advances (administration arranged design, web administrations), framework the executives (autonomic processing), and equipment (virtualization, multicore chips) [6].

8.1.1 Principle of Embedded Computing

Embedded framework, structures the premise of all gadgets that are right now developing and being investigated. With progressively refined innovation headways, the components of the gadgets are getting littler, and the registering capacities are presently nearly keeping pace with the PC. In light of those capacities, we now see latest gadgets that can be matched with different segments; for example, remote correspondence innovation, sensors and other supportive parts to determine earth's condition, or actuators to register sensory reactions. For our specific situation, this implies we talk about frameworks in which physical articles and computational assets are firmly incorporated and show a level of persistent coordination between one another.

Installed frameworks have dependably been held to a higher unwavering quality and consistency standard than universally useful figuring. An implanted framework (not at all like an independent PC) is a digital framework which is an indistinguishable component of a specific bigger framework (item or foundation). It serves a particular point (for example observing, control and so on.) in this bigger framework through (over and over) executing explicit calculation and correspondence procedures required by its application. It is application explicit. It must be particularly planned or embraced to enough serve the execution of these particular calculation forms, and fulfill the application's prerequisites identified with so much qualities as utilitarian conduct, response speed or throughput, vitality utilization, geometrical measurements, value, unwavering quality, wellbeing, security and so on. Regularly, implanted frameworks are (receptive) continuous frameworks, incorporate detecting, interfacing, handling and additionally impelling sub-frameworks, and include in their execution different blends of advanced and simple equipment, and inserted programming. In short, implanted frameworks are digital frameworks that are firmly combined with (installed in) the frameworks that they control, manage, screen or analyze. Unavoidable (Ubiquitous) Computing is a worldview of a consistent incorporation of data preparing and correspondence into items and conditions. An unavoidable framework is in truth an "in a perfect world" coordinated installed framework [7].

This section focuses on embedded computing technology desirable for the complicated and highly challenging CPS. From the perspective of embedded

computing requirements, it will consider various CPS classes. It will also discuss the heterogeneous MPSoC and layout techniques required to implement the Cyber-Physical Systems, which are deeply in demand as well. The discussed MPSoC technology exploits heterogeneous computation and communication resources involving general purpose processors as well as application-specific instruction-set processors (GPPs), as well as, application-specific instruction-set processors (ASIPs), distributed parallel memories, HW accelerators and hierarchical communication structures.

8.1.2 Concept of Cyber-Physical Systems

At present, numerous specialists from different fields are giving close consideration to the rise of new paradigm—Cyber Physical Systems (CPS). CPS are multidisciplinary frameworks that lead feedback control on widely dispersed embedded computing frameworks by the mix of communication, computation and control technologies. They are the result of integration and transformation of the current system frameworks and embedded systems. Through joining, CPS can understand the ongoing, protected, dependable and dynamic integration of physical frameworks with software, providing design and analysis along with abstraction and modelling for the framework [8]. The relationships among computers, networking and physical frameworks connect in manners that require essentially new structure advances. The innovation relies upon various areas like computers, embedded systems and software. CPS has a wide scope of uses, for example, digital medical instruments and systems adopting automatic acquisition and control technology, aerospace and aircraft control, distributed energy systems, industrial control etc. [9–11]. CPS can likewise bring gigantic financial advantages and will in the end carry basic change to the capacity of existing engineering physical systems.

U.S. Defense Advanced Research Projects Agency (DARPA) is of the view that physical network system are basically frameworks using capabilities of software and electromechanical systems. CPS are deployed and collaborated within all defense systems (such as aircraft, spacecraft, naval vessels, ground vehicles etc.). Additionally, micro-electro-mechanical system (MEMS), integrated circuits, and nano-electro mechanical systems (NEMS) are also collaborated into CPS [12].

Tremendous research opportunities are available within CPS field as it is relatively a new dimension and offers multidimensional research on application as well as creation of CPS. These dimensions signify, where exactly frameworks can be manufactured as current research demonstrates the basic technical problems but lacks a well-founded conceptualization for CPS; adequately reflecting its nature as a software-enabled hybrid option consisting of computer, service and meaningful product components. However, these challenges should be addressed at the time of device creation. Thus, it is important to have a design-based CPS framework, as an advance reference point. Furthermore, difficulties arising due to execution of mathematical equation methods, are also faced. Such complicated conditions must

be dealt, without compromising on the CPS framework. Research in the CPS field is as yet developing, while some broad prerequisites of this framework are unsurprising. The vision of the CPS framework can be interconnected with huge scale extended framework eventually. CPS research in the future is going to be based on sectors including: energy, transportation and mechanical autonomy fields. Not to close the potential outcomes, the wellbeing or health care field will be a trend again. This will be because of an ever-increasing number of individuals exploring this field, for instance wearable electronic gadgets or sensors [13].

8.1.3 Cyber-Physical Systems Applications

Applications of CPS include in healthcare industry, traffic control, environmental control, communications systems and more. Immense energy efficiency and considerable enhancement in demand variation will be experienced due to networking of building control systems under CPS. Networked autonomous vehicles could improve the disaster recovery techniques. Applications of CPS are huge which will be discussed in this section [14, 15].

1. Healthcare—CPS plays a major role in the healthcare services sector. Ongoing research focuses on smart sensor frameworks for continuous observation and cautionary patient well-being conditions, telemedicine frameworks that enable distant healthcare administration arrangements, semi-autonomous tele-operated home service robots that can help with patient physical tasks. In medical facilities, Cyber Physical Systems (MCPS) are progressively being used to provide patients with quality nonstop care. One of the most researched topics in the field of MCPS is 'Telemonitoring'. It would help attending patients at the right time in most critical situations. Patients, by the virtue of MCPS will not be required to visit hospitals as frequently with these monitors installed in their homes. It will be extremely beneficial for expecting women, elderly people, patients with critical diseases and those who require monitoring at all the times. The patients feel at ease and are safer with medical Cyber Physical Systems. However, there is still a long way to go for these machines to equal human care and treatment. It still faces some challenges like context aware intelligence, security, autonomy and privacy and device verifiability. If there is a fault in the system at any point, it may lead to more damage than accounted for.
2. Transportation—The ongoing development of science and technology enhances the relation between computational and physical systems. The Cartel Project is a great example where the artificial and the real-world crossover, at MIT, where a fleet of taxis run by gathering real time traffic information and put this data together to use it for calculating the fastest routes to the required destination. Increasing urbanization is a challenge faced by many governments and technological industries; with the steady advance in population rate and global warming, there is a dire need for sustainable methods of living and increased

efficiency of the energy and resources available. AUTOSAR is yet another development of cleaner and intelligent means of transportation. Here, human factors are fused with vehicular Cyber Physical Systems along with safety applications to assist human drivers. The psychological human traits can be incorporated to increase the accuracy of the automobile models. Implementation of the data fusion algorithm here allows optimal utilization of these messages. This method avoids the most common negative aspects of CPS which includes distraction, confusion and overloading of information.

3. Infrastructure—Sustainable use of resources available has become a vital challenge in the modern world. Designing buildings in a way the net energy consumption is zero is a challenge taken up by many architects. Different infrastructures are studied and their alternatives explored to minimize the use of electrical energy by using renewable energy resources and computing. Protecting all within and around the structure is necessary too. In 2014, the Department of Homeland Security (DHS) awarded Northrop Grumman a five-year contract to support the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). As part of that work, Northrop Grumman's government contractors handle incidents by notifying victims of Cyber Physical Systems and Critical Infrastructure: Highlighting Northrop Grumman Corporation's Work cyber threats, providing mitigation measures, and working with asset owners/operators to improve awareness. The ICS-CERT provides critical infrastructure entities in the private and public sectors with mitigation strategies and incident response services that are tailored to the sector and the entity's needs.
4. Manufacturing—The use of Cyber Physical Systems in the manufacturing industry can predict potential faults or wear in equipments with ease. It has cut down costs from the traditional methods by more than 30%. According to [16], there is a five-tier pyramid that uses machine history data and processes it to understand the system better.

   – Component Level: This level virtually duplicates all the critical components of a machine. They work parallel with the physical machines and are not bound by time or location. These virtual twins are stored in the cloud and are able to detect the lifespan of each component of the machine. They are also able to remotely interact with the machines when geographically far away from it.
   – Machine Level: Virtual twins of machines are created by recording the operation history, system settings as well as core components. The twins are able to compare one machine/component with another and identify the better performing, efficient ones.
   – Cyber Level: The data extracted from the monitored system may speak to system conditions at that time point on the off chance that it tends to be contrasted to other comparable machines or with machines with a different history, clients can acquire knowledge on the framework variation and life

forecast. It is called cyber level because the data is used in creating cyber avatars for physical machines and building an incredible learning base for each machine framework.
- Fleet Level: The virtual twins of machines are not bounded by time or location, this can be used to our advantage to optimize production, life span and quality of the components. Using previous performance data and status of the machine parts, the machine can be set to perform accordingly in order to create a self-maintaining and self-configuring system.
- Enterprise Level: This level uses the previous data to produce performance reports and improve fleet level performance. The Cyber Physical System is able to store data as well as maintain it in the cloud. Developers are able to create mobile applications to present information to all users in and around the company.

5. Communication—It is possible to model a data center as a Cyber Physical System . Online apps and facilities that ensure communication and computation are the cyber component. The physical components ensure proper operation and non-stop procedure. Cyber and physical component cooperation is difficult in power management. Expenses can be reduced if CPS can replace cables and network topologies and they are easy to manage. These include, however, some important downtimes, wireless communication depicting a broad range of problems and challenges that developers and analysts need to tackle. In most cases, wireless sensors and actuators in such applications are systems that are restricted in terms of power utilization, communication and energy resources and issues such as reliability of data transmission, energy efficiency and real-time data delivery need to be addressed. It includes ongoing evaluation, starting with the layout stage, continuing with developments and finishing with the execution stage.

8.2 Internet of Things and Ubiquitous Computing

8.2.1 Smart Devices/Smart Cities

A Smart City's developing model is based on an urban environment. It has new age of advanced housing systems, production processes, health care support facilities, efficient energy, environmental monitoring, business innovation, trade, and social activities. To empower the technology for such a setting requires an outlook on smart cities incorporating within Cyber Physical Systems (CPSs) and providing innovative software platforms equipped with state-of-the-art data security, privacy management features, mobility and swift handling of huge measures of raw data.

The application of Cyber Physical Systems in the present world is plenty and very common since most of the major cities in the world are transitioning to smart cities concept and are completely depending upon advancements in technology. Especially factors like innovative modes of transport, security, healthcare services, energy distribution management and environmental monitoring require use of eco-friendly and automated machines. Tokyo, for example is considered to be one of the leading smart cities in the whole world. They have used technology to improve their quality of living in a very interesting and inspiring way. For instance, "The Meguro Sky Garden, where noise minimization technology is being used to preserve the serenity of the garden and Henna Cafe, where you'll find yourself in a traditional coffee shop with a robot barista serving customers". They have deployed excellent sewerage and educational systems that also add up to the exceptional use of technology in daily life. The use of smart cars that are eco-friendly is yet another application of Cyber Physical Systems. Smart Grids are further advanced application of Cyber Physical Systems, which are digitalized electric grids that allow communication between customers and producers. Smart Grids are vital as they support energy conservation, and increase the efficiency and transparency of the transaction. The use of more smart electrical systems however also pose a greater risk to the security of CPS due to the need for cyber security.

Smart devices are currently implemented in various sectors including, but not limited to: smart and uninterrupted glucose monitoring insulin pens in the medical field, real time smart sensors in industries, smart weather stations and sensors used for agriculture. They are even used in our homes in the form of smart speakers, smart thermostats and cameras that can be connected to our personal devices. Smart devices are taking over majority of the components in our lives and makes everything much easier. Yet another efficient application of smart devices are in prisons. China already has a fully functional smart prison where smart sensors are used to track each prisoner and their activities to detect any unseemly activities and notify the guards. This is connected to an artificially intelligent computer where all the data is recorded with the help of facial recognition while analyzing movements. Smart towns are becoming more crucial with the advent of CPS. Smart cities can be seen as CPS implementations on a big scale [17]. In smart cities, however, there are different challenges to adopt CPS, listed as under [18, 19].

(1) CPS Heterogeneity concerns
(2) Large and complicated networks
(3) Limited resources and limitations on budget
(4) CPS attacks and safety problems
(5) Reliability
(6) Data management
(7) Real time

Table 8.1 Smart city parameters, CPS applications and effects

Smart city parameters	CPS applications	Effects
Smart governance	E-governance and E-democracy	Quality and effective services to citizens
Smart security	Coordination of advanced surveillance	Improves the quality and standard of living through crime mitigation
Smart energy	Smart grid technologies	Less fuel consumption
Smart transportation	E-mobility using GPS	Reduces emissions of gases, Reduces traffic congestion, Controls noise pollution

ICT infrastructure is intelligent city's cornerstone. CPS supports openness and requires coordination of ICT [20] In Table 8.1 [21], smart city parameters, CPS applications and CPS usage effects are shown.

With the improvements in ICT technology, individuals migrate to metropolitan regions. Urbanization is turning into a worldwide phenomenon. By 2030, 60% of the population will be living in urban areas. Smart cities development is therefore inevitable. Our daily activities are supported by Cyber Physical Systems (CPS) and smart cities are becoming more important with the emergence of CPS. The next section sheds light on the ideas of CPS and different difficulties posed when implemented in smart cities.

8.2.2 Big Data and Cyber Physical Systems

Big data is a term used for datasets whose size or type exceeds the traditional relational database's ability to capture, manage and process low latency data. Big data can be produced from devices such as video and audio, log files and the worldwide web. Cyber Physical Systems are commonly used for crucial functions like maintenance of security, power, automations, machines and many other applications. This is modernizing the world and gives more responsibility to technology and machines in almost all fields. Cyber Physical Systems optimise decision making and eliminate inefficiencies by translating enormous amounts of data in information in an orderly manner. For example, intelligent systems can be used to predict customer patterns in big businesses and planning out their inventory as well as managing costs. Social media is one of the best-known examples of big data. Enormous amounts of data in various forms can be processed and dealt with using Cyber Physical Systems. Smart home assistants are fairly common in houses today. Using Natural Language Processing and voice recognition algorithms these assistants are able to provide assistance to the queries requested. The size of data is increasing with time. There are many struggles associated with big data such as storage, sharing, security, visualizing and storage. The larger the data gets, it is

harder to manage and store it securely. It is predicted that with the growth of data at its current pace, by 2020, an average man will be generating more than 1.5 MB of data every second in a day. Companies harness their information and use it to find new opportunities with the help of Big Data Analytics. There are 3 benefits for a company to use big data analytics namely:

- Reduced costs.
- Smarter and quicker decision making.
- Satisfying customers with new products with the help of technologies such as Hadoop and MongoDB.

The processing demands that need to be renovated by big data sets may not be handled by traditional data warehouses efficiently in real time which is required in case of stock trades and online activities of users. Especially, unstructured and semi structured data are not handled well by relational databases.

We know that latest smart embedded systems and devices are produced for connecting to the Internet. These systems and devices haven given rise to the term Internet of Things (IoT), because it is believed that these instruments, too, can independently behave, store and intelligently operate in the real world. Their artificial intelligence clubbed with sensing and actuating capabilities provide unprecedented interaction opportunities in different situations and environments between real and virtual world. These exceptional devices will push the scalability demands of Big Data architectures to highest boundaries. Additionally, it will generate an overwhelming flow of real-world data, enriching apps significantly, making them more conscious of what is happening in the true world, everywhere, in real time. The new circumstances required advanced data mining and machine learning techniques to be able to extract insights from such large streaming data. A major goal for CPS Big Data is to evaluate very big, rapid and heterogeneous information streams from industrial settings which uses machine learning to extract information from the data. In order to learn from big data machines, at present, there are two main strategies. One of the strategy is based using distributed systems (Hadoop and MapReduce outlined). Mahout [22] is a software project, popularly deployed for open-source system for batch-setting machine learning. While, in a cluster setting, many algorithms are ported to operate in parallel [23]. Online learning [24] uses one instance at a time to update models in real time. Likewise, MOA [25] is an online machine learning software framework that runs on standalone machines. It includes classification, clustering and frequent mining of graphs. Online algorithms use approximation and statistical data structures extensively [26]. These data structures use statistical data characteristics to decrease computational and memory costs by forfeiting accurate responses and trading off accuracy [27]. Some of these data structures were either transferred to the distributed setting [28] or applied to stream mining [29, 30]. To date, however, their primary use has been peer-to-peer systems and distributed retrieval of information, and their application to data mining and machine learning has not been fully investigated. Researchers have recently started investigating practical problems

encountered when these algorithms are applied in specific [31]. Therefore, correct assessment of mining algorithms has become even more crucial, when dealing with big flows of data. The main issues include, data skewness, class imbalances and scarcity [32]. Some of these issues have recently been studied [33, 34], but their impact on the overall assessment has yet to be completely evaluated.

8.2.3 Cloud Computing and CPS

A customer requires the capacity to create its own apps running on cloud information to allow overall utilities in the cloud. Although, Google has originally developed Hadoop Map/Reduce, it is now available as open source through Apache Hadoop Project [35]. It has gained massive success by providing popular framework that enabled clients to run and deploy distributed analytics in the cloud server. Likewise, another framework by Apache Spark [36] is knows as Map/Reduce. Under this model, data is disseminated on a large 378 numbers of storage servers. Each storage server unit has "Map" operation running in parallel to appropriate information products stored on each storage server. The results of the map operation are collated from these storage servers and subjected to reduction "Reduce" process that essentially accumulates data results distributed across all storage servers. Hadoop implements HDFS (Hadoop File System) which is a special purpose file system that promotes the Map/Reduce Programming Model. The operation of the map runs and stores data results in HDFS. In the beginning, significant overheads are required to be setup to implement a Hadoop Map/Reduce program. However, once setup, it is pertinent to mention that data mapping and items calculations take place in parallel. There is an ongoing research and debate to comprehend program's ability to perform analytics in a storage cloud as well as how it can be expanded, while analytics performed on an embedded system to be synthesized with analytics performed in the storage cloud. Hadoop applications now involve information to be stored in HDFS (Hadoop File System), whereas not all clouds are constructed on a file system like this. For instance, Openstack is built on Swift (not on HDFS). It requires extensions through Openstack Swift to be able to perform procedures like Hadoop. In order to make this workable, extensions are also needed to allow analytics operations to flow, with one operation feeding the other [37].

8.2.4 Artificial Intelligence and Smart Cities

A Cyber Physical System is controlled and maintained by computer algorithms that are integrated with internet and its users. It is enables artifically intelligent interaction between humans and computational systems that helps in decision making by way of creating awareness of the situation and perceptions related to changes in the environment. Through Artifical Intelligence (AI), computers can

eventually evolve to operate in unfamiliar environments as well. India is a great example of a country that aims to bring in more use of Artificial Intelligence in their defense systems along the borders. India has started developing defense skills using AI to achieve and build better warfare systems like unmanned aerial vehicles, completely technology based robotic rifles and tanks.

The applications of Artificial Intelligence is spread over these areas specifically [38]:

- Financial Sectors-To reduce fraud and corruption in financial institutions by early detection of damage and remove human errors.
- Healthcare-The healthcare industry relies on AI to fine-tune the precision of medical projections and select an appropriate therapy line.
- Manufacturing-Products will be of better quality and more identical when produced by machines. A larger amount of products would be produced in a shorter period of time.
- Crime detection-Indian authorities are taking the help of AI that is developed from across the world that helps to process cctv feed and detect criminal activities that are about to take place especially in public places.
- Improved Agriculture-Agriculture is still one of the most common methods of income in India, with the help of AI farmers hope to automate their crop yield production and usage of sensors to measure the moisture and temperature of the soil.

Cyber Physical Systems also influence the Control Systems that are computerized electrical devices affecting the functioning of other devices using control loops. These systems are used to improve safety, security, efficiency and production of different fields; some of them include: Nuclear energy plants, mines and agriculture and boiler industries. As said earlier, control loops are enable the functioning of Control Systems that could either be open or closed loops (shown in Fig. 8.1). The open loops are controlled by humans, whereas closed loops are computational. In some cases, loops can be switched between open and closed modes.

Humanoid robots and automated energy saving automated cars are the other applications of Cyber Physical Systems. Automated cars can help in solving problems of traffic. It is done by collecting information in real-time from all traffic conditions on the roads. Automated cars also help in reducing human errors on roads such as crashes due to road rages. These humanoid bots could be used in rescue operations.

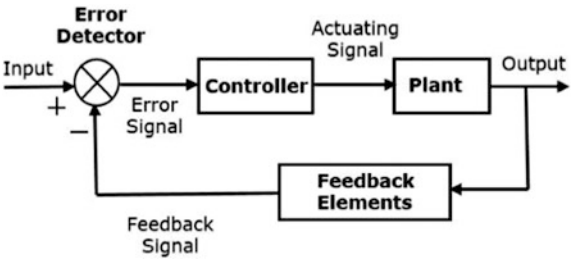


Fig. 8.1 Simplified working of control systems

8.3 Smart Manufacturing

8.3.1 Introduction

Smart manufacturing is known as solution enabler and is a collection of many solutions and technologies used in the manufacturing Industry. This enhances the manufacturing of various products which in turn boosts profits. It is a broad approach and cannot be directly applied in the production sector. Smart manufacturing's main goal is to maximize the use of automation and information analytics to optimize manufacturing sectors output. Smart machines could be included and networked through the Internet of Things (IoTs) and widely implemented in the manufacturing industries across the globe. They are also able to order materials required for production, allocate jobs and prepare the networks. As shown in Fig. 8.2, fusion of manufacturing processes and embedded technology, data engineering, materials, sustainability and networking are the main pillars of smart manufacturing. Developments in this sector can be visualized to business dichotomy and standardization in ten distinct concepts such as production digitization and material-product-process phenomenon.

Smart Manufacturing, along with some difficulties, provides many possibilities. Manufacturers are using smart technology to create new products and improve services to refine their revenue streams. For example, Worcester Bosh manufactures smart boilers are able to detect faults and intimate when they require service or maintenance. It has improved safety for the customers and prevented loss that is often caused due to faulty boilers. The many challenges that are a part of smart manufacturing are [39]:

- Information security is very important as everything that is stored in our systems are vulnerable to attacks that can result in the loss of our information. Smart Manufacturing firms must take measures to keep each component of their systems secure from cyber-attacks.

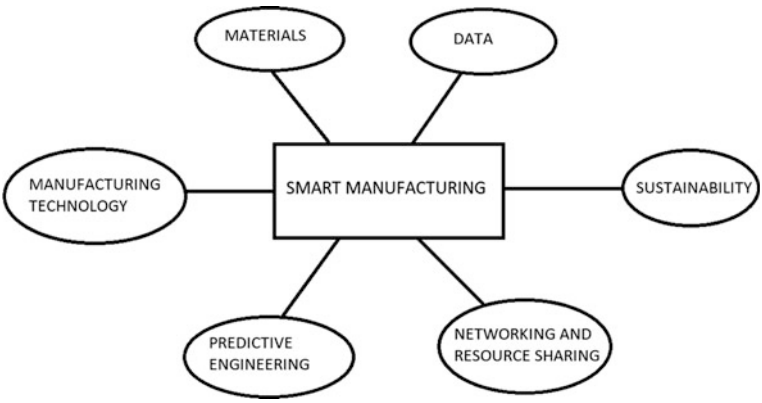


Fig. 8.2 Pillars of smart manufacturing

- Maintenance and repair is yet another challenge faced in the manufacturing industry. Each machine must be maintained as well as enhanced over a period of time. This would cost a lot of money and resources.
- It is a challenge to connect various systems together that will support an end-to-end picture of the supply chain and manufacturing process. The interoperability of these systems and networks is required at operational tier. Moreover, international level technical standards are applied to achieve desired results. The new business processes will have enhanced connectivity that may also subject manufacturers to unknown and new laws and regulations to deal with.

8.3.2 Industry 4.0

Industrial sector plays a vital role in the economic growth of countries [40]. The industrial revolution recognized as the transition from old to new manufacturing processes began in the 18th century. After the third industrial revolution, once again the industry is transforming into new manufacturing trends commonly now known as 4th industrial revolution [41] and considered to be Industry 4.0. It is a name given to support existing trends of automation as well as exchange of data within manufacturing processes and supportive technologies. It is already recognized that Industry 4.0 technologies will affect current and future sectors substantially [42]. It deals with smart digitalized systems and network integration which advances the working environment of an industry by reducing the human involvement in certain tasks [43]. Digitalization, Internet of Things (IoT) and Cyber Physical Systems (CPS) are the terminologies used to describe Industry 4.0. These conditions are labeled as the result of the German high-tech strategy to the manufacturing sector's futuristic industries [44].

The term digitalization is the progression of transforming into a digital business. Using the latest digital technologies, a business model is changed to digital company and fresh income is generated through value-added opportunities [45]. The definition is so wide that it includes relationships and customer interactions between different businesses, and government. It is essential to acknowledge that there is a clear connection between business services and real customer needs [46]. In the business domain, digitalization illuminates many significant company characteristics, such as how to keep track of clients, identifying distinct methods of producing and transporting products effectively, inexpensive and efficient methods of advertising, and where to purchase and sell the products. Similarly, in production domain, digitalization contributes to design and create products virtually before the actual production and also to maintain the relationship between customers and production organizations or service providers. The core of digitalization is Big Data where enormous amounts of data are accessible via the Internet [46]. However, a fully decentralized architecture is one major challenge in big data applications [47].

Decentralization of data and information helps keeping independent management processes and smart objects in Industry 4.0. Nevertheless, throughout the network, these procedures and smart objects are interconnected, thus promoting communication between virtual and real globe, which is a fresh element of production and production processes [48].

Decentralized data and integrated processes stimulate complexity but enhances transmission of data between partners in supply chains. In Industry 4.0, IoT infrastructure provides shared platforms via cloud systems which helps in optimizing the business processes [49]. IoT infrastructure which is comprises on Industrial Wireless Networks (IWN) and Internet of Things (IoT) [50, 51] offers diversified fields including loyalty programs, information for decision making, brand relationship and customer retention [52]. The main purpose of IoT is to connect with physical devices and to collect data which is used to take decision about operations [53]. IoT transfer and integrate knowledge within and across organizations by connecting humans and machines. Specific and personalized products can be offered with the help of IoT infrastructure which can be customized by users via web pages. The data then transmitted to the industrial cloud. In order to produce products efficiently; cloud data is not only used by the manufacturers to optimize the design process but also to manage and monitor the production processes [49]. However, constructing a secure IoT infrastructure for Industry 4.0 is a major challenge due to the involvement of dynamic management processes and human machine interaction. Therefore, cloud engineering structure in Industry 4.0 will be focusing on the characteristics of Cyber Physical Systems in order to optimize the operational efficiency of the infrastructure [54].

Cyber Physical Systems combines the procedures of computing, networking and physical processes [55, 56]. The National Science Foundation (NSF) described CPS as "*systems with profoundly intertwined physical and software parts, each working on different spatial and temporal scales, displaying various and distinct behavioral modalities and interacting with each other in a multitude of ways that alter context*" [57]. CPS key obligations are to improve the industry's efficiency and effectiveness and to meet agile and dynamic manufacturing requirements [49]. CPS helps in monitoring and controlling physical processes. It helps in taking decentralized decisions by creating virtual connection to the physical world. Decentralization and independence of decisions contributes in improving the overall industrial performance [58]. Furthermore, CPS provides real time communication links between physical devices and humans within and across the organization [54].

In their studies, Thames and Schaefer [54] indicated that Industry 4.0's main goal is to attain operational efficiency, productivity and improved automation support. Researchers [58, 59] revealed five primary characteristics of Industry 4.0 including, (i) digitization, optimization and manufacturing customization, (ii) automation and adaptation, (iii) human machine interaction, (iv) value-added services and enterprises, and (v) automatic information exchange and communication. Therefore, Industry 4.0 is a value addition process for improved knowledge management. It provides computerization and connectivity within the outdated industry. Besides many other benefits, Industry 4.0 can improve flexibility, help in reducing

lead times, provide customization, and also reduce costs [60, 61]. There can be different ways to implement Industry 4.0 infrastructure. It is revealed in the literature that there are three known frameworks available to adopt and implement Industry 4.0 i.e. C4ISR, IDABC and ATHENA [62–65].

Originally created by the United States. Defense Department, 1996—C4ISR refers to Command, Control, Communications, Computers, Intelligence, Surveillance and Recognition. C4ISR's aim was to incorporate U.S. military relations, values, and guidelines [64]. The second framework is described as the Interoperable Delivery to Public Administration, Business and Citizens of European eGovernment Services (IDABC). It is derived from the European Interoperability Framework (EIF). EIF aimed at implementing interoperability through organizational, technical and semantic dimensions [65]. Whereas Advanced Technologies for Interoperability of Heterogeneous Enterprise Networks and their Applications (ATHENA) obtained from three multidisciplinary methods known as Enterprise Modeling, Architectures and Platforms and Ontology [62, 63].

8.3.3 Cyber Physical Systems Ecosystem

The CPS/IoT Ecosystem is regarded to be a varied structure consisting of hardware devices and software components scattered across tree intertwined operating scopes: cloud, fog/edge, and sensor/actuator nodes. The cloud offers computing with high efficiency and storage of big capability. These systems are spread globally and are used in different industries in Europe, particularly in many locations. For instance, in Austria, parts of the installed infrastructure is: The CPS Ecosystem Cloud, Custom Built Hardware, Sensor devices and Information Model [66].

- CPS/IoT Ecosystem Cloud: The cloud system is a high-performance computing platform located in a TU Wien server center for general reasons. It provides services to assist handle big amounts of data (e.g., storage, analysis, aggregation).
- CPS/IoT Ecosystem Fog/Edge: the ability to react rapidly and with guaranteed quality of service (QoS) at a factory level or a similar fog/edge implementation plan.
- CPS/IoT Ecosystem Sensor Device: the sensor/actuator nodes are direct physical environment interfaces.
- CPS/IoT Ecosystem Information Model: Three main issues in IoT, as stated above, are management, growth and safety. A functional IoT information model for the CPS/IoT infrastructure is part of the solution to these challenges.

Cyber Physical System Ecosystem is a much studied domain in the IoT. However, there are some pertaining challenges: These systems take up immense amounts of power. Security is a very important field of study since almost

everything is connected to smart devices privacy becomes an issue for everyone. Managing large amounts of data also becomes a major challenge and requires lots of resources and time dedicated to it.

8.3.4 Industry 4.0 and Cyber Physical Systems: Sector-Wise Implications

While, the Internet of Things (IoT) tends to connect "Things" that are object and machines, first to the internet, and eventually to each another, Cyber Physical Systems (CPS) incorporate physical process, networks and computational layers in one unit. Highly networked computers and machines, such as robots, interact with physical world in a highly-integrated and technical environment. With its new found service and application agility, CPS is now rapidly penetrating into the manufacturing process, making it imperative to validate subsequent impacts of CPS on the sector itself.

The Science & Technology Options Assessment (STOA) study "Ethics of Cyber-Physical Systems" recognized main regions where CPS is found to have important impact [66]:

(1) Disabled people and daily life of elderly people.
(2) Healthcare.
(3) Agriculture and food supply.
(4) Manufacturing.
(5) Energy and critical infrastructures.
(6) Logistics and transport.
(7) Security and safety.

Disabled/Elderly: It is estimated that by 2050, adult population (over the age of 85) will triple due to the measures of improved life expectancy. This will have a spillover effect, due to reduced birth rates. An imbalance of young and old generation within societies will emerge, where, relatively lesser younger people will be available to look after and care for elderly and disabled. To address this, CPS will provide smart homes, equipped with sensors for disabled and eldering people. It will include wearable sensors and robotics. The patient care services will improve in quality due to adoption of technologies, leading to shifting from treatment to prevention paradigm. Medical professionals will have access to real-time data, collected on patients through smart home sensors and smaller wearable CPC devices. Eventually, specialized task oriented robots will take over the process. It is expected that impact of patient care treatment will become effective and in the long run, with increasing levels of autonomy associated, there is potential of CPS to be converted into ubiquitous and independent patient care.

Healthcare: In the health care industry, CPS will bring increased accuracy based on real-time media data. It will lead to lesser false warnings and quicker recovery

for patients. With robots taking over smartly, surgical procedures and human enhancement will experience reduced errors. The prognosis and diagnostic process will become highly structured due to CPS and decisions taken, will be based on evidence supported results and treatments. The integration and increased use of CPS will support healthier society with procedures becoming less aggressive in nature, and immensely reducing absenteeism at work. However, there will be environmental pressures to deal with, in addition to reconsidering patient privacy and medical secrecy laws, and meeting the demand of rare and precious materials to support health care industry through implementing CPS.

Agriculture: Agriculture has been revolutionized with CPS, as food sensors will be deployed to probe for diseases, evaluate products' freshness and standardize food safety measures—across the world. Obviously, it will also impact on the hygiene of the food industry. To gather data on accurate farming, sensors, farming machines and drones will be used. Eventually, autonomous CPS machines will pave way for crop establishment, searching, and selective farming. It will encourage progress in the recognition and execution of AI information interpretation, information mining and decision-making patterns. Smart food labels will also provide a holistic overview of the entire production chain, value creation and supply chain to provide insightful information on where and where food is grown. Precision farming will have positive impact on our environment due to resource friendly approach. It will bring about loss of jobs in the agriculture and food production sector, as technologies will replace human workers. But in the context of Industry 4.0, robots will require highly trained, and skilled engineers to manage them. It will create a niche for high-skilled jobs within industries developing autonomous agricultural machines. Also, young individuals will be compelled to work in agriculture sector due to the ease with which they could operate and manage their businesses—remotely and efficiently. It will support their urban lifestyle as well as give them quick access, time and support to engage in agricultural tasks. Additionally, IoT will enable and link information gathered from food production processes and package development to devices such as refrigerators. It may send an alarm and message supermarkets when it is time to replace a product. The fact cannot be ignored is whether it will infringe upon consumers privacy and ethical concerns violation.

Manufacturing: It is widely believed that use of CPS in manufacturing could bring about structural changes to conventional processes that are followed, giving full throttle rise to the 4th Industrial revolution, Industry 4.0. Building onto the foundation of recent technological advancements in the field of nanotechnology, CPS can regulate and facilitate the manufacturing process by way of implementing continuous miniaturization of actuators and sensors. Likewise, as enormous amount of real-time data collected through sensors is required, to enable and function smart manufacturing, therefore, miniaturization of sensors will provide a smooth platform to realize Industry 4.0. New internet protocols, such as IPv6, combined with smaller sensors, will make it possible for the sensors to eventually become part of the Internet of Things. It is where we know, everything is connected and interconnected online—an essential requirement feature of Industry 4.0. New business models will

emerge (like Google and Facebook), that will be use data as an asset to support the evolution radical manufacturing processes. As these advancements in CPS are going to allow for the emergence of highly intelligent machines, that will not only excel in abilities of machine-learning, but would create individualization of modern society. It primarily means that consumers will have the ability to customize and personalize products. As there is a rise in application of additive manufacturing, coupled with CPS, manufacturing will no longer be a difficult concept for a layman to understand. It will be cost-effective, highly personalized and will promote consumerism.

As manufacturing industry happens to have lion share in the creation of jobs and its impact on GDP of an economy, therefore it is undeniable that changes due to CPS integration with additive manufacturing could lead to job shifts in the manufacturing sector. It can be predicted that labor intensity in terms of strength and involvement will reduce and as well may become less important. There will be a likely increase on acquiring digital skills. It is a reported fact that by 2020, ninety percent of all jobs will require some digital skills [67], which is a good omen because it will support healthier life, reduced cost of insurance, better life expectancy and improved age ranges for workers to flourish and contribute in the manufacturing sector.

With its added advantages and benefits for the sector and the people working in the manufacturing sector, CPS also comes with its shear of challenges and ethical concerns. However, CPS in manufacturing will yield more benefits to the economy and society, at large. Development and application of CPS enabled systems will require legislation to look after the risks posed and to ensure citizen feel safe and ethically not compromised in the world shared with CPS.

Energy and Critical Infrastructure: Anticipated changes in infrastructure systems, with respect to CPS and Industry 4.0, will include controlling electricity flow from producers to end-users or consumers. The transition will result in "energy prosumers'—individuals that will consume and produce energy. Smart grids will be required for the new infrastructural setup and to support increasing energy decentralization. Similarly, increasing reliance on smart technologies will also transform usual linear energy grids into intelligent grids via the "IoE-Energy Internet." The smart grids will provide continuous live-data to producers and consumers about energy efficient usage. It will also optimize grid management. Automation will take forward future energy systems that will become a reality through global Internet of Energy. Smaller to larger, self-sustaining communities of prosumers will emerge, creating virtual power plants (VPP). On the other front, we cannot ignore that CPS energy systems will require technical abilities and finances therefore it may lead to digital divide between those who have access to resources and digital skills and those who do not. Moreover, areas involving liability, ownership and data collection also require attention in order to mitigate negative impacts.

Logistics and Transport: Logistics and transportation system will be modernized by CPS with the advent of Industry 4.0. It will have an outward spillover effect with an overall reduction in emissions and efficiency optimization to achieve higher saving in fuel consumption. Automobiles are automated and existing

manufacturers are introducing advanced driver assistance systems that will make cars smarter by providing automated assistance. Robotics and related technologies will effects logistics fundamentally in order to resolve traffic congestion problems. It will monitor loading and unloading areas in urban areas and send information in real-time for processing by the CPS. Likewise, automation of retrieval systems, storage warehouses and manipulation of goods will increase. Materials for autonomous robotic handling systems are being built and very soon, deployment of completely autonomous fleets in transportation and logistics sectors will be a reality. CPS will require regulatory measures, standardized law and redressal of privacy characteristics.

Security and Safety: CPS will in many ways provide foundation to build safe environments, yet it will be highly complex that would require improved understanding of machines and their effects on security safety measures. It is, thus, agreed that CPS will introduce challenges for security and safety, as hackers pose threat to vulnerabilities in systems to corrupt operating systems. In case of prediction failure of machines, a number of safety issues can emerge. Development of quantum 2.0 technologies will reduce potential vulnerabilities. The use of CPS will collect data from potential threats, and identification as well as handling of such data will require specialized skills.

4.0: Hannover Center for Production Engineering (PZH)—Case Studies on Digital Manufacturing/Industry

The Hannover Center for Production Engineering (PZH GmbH) was founded at the University of Leibniz Hannover in 2001. The seven mechanical engineering institutes heads (i.e. IFA, IFUM, IFW, IMPT, match, ITA and IW) established PZH with the primary goal of bringing under one umbrella university research and manufacturing related companies. It was the joint effort of Public Private Partnership Initiative with the State and Federal Government [68].

PZH GmbH is now the subsidiary of Leibniz Universitat Hannover, TEWISS GmbH (Technik und Wissen GmbH). TEWISS emerged in 2013 from the PZH GmbH with the objective to advance and co-finance the facility in Garbsen. The TEWISS serves as a mediator between university and industry to bridge the gap. Now, the TEWISS is comprises on 18 institutes in total to build competence and to increase interaction among universities and companies. Approximately, 250 research associates, 110 non-scientists administrative staff and around 540 research students are part of the research centre. The focus of researchers at TEWISS is twofold. On the one side, for a good interdisciplinary collaboration, they bring together versatile disciplines. On the other side, they make excellent use of the engineering services supplied by TEWISS GmbH and the many smaller manufacturing-related businesses, some of which are even the institute's own by-products [69]. Since 2004 all mechanical institutes of PZH in collaboration were sharing a common address. Therefore, the new manufacturing technology set-up in Garbsen has been built, all of Leibniz Universitat Hannover's mechanical engineering faculties will be united at the "Mechanical Engineering Garbsen" campus with about 4500 staff and students [68]. The research is conducted in the six institutes:

1. IFA—Institute of Manufacturing Systems and Logistics: The Institute analyzes logistic and organizational interactions in manufacturing enterprises and supply chains.
2. IFUM—Institute of Metal Forming and Metal Forming Machines: The research focus is on resource friendly machines technologies and initiatives. It also emphasis on innovative processes of forging and sheet metal forming.
3. IFW—Institute of Production Engineering and Machine Tools: In relation to enhancing current instruments and optimizing the organisation of production, the Institute offers functional surfaces and designs its own instruments.
4. IMPT—Institute of Micro Production Technology: The aim of this institute is the development of high-performance sensors and actuators in an efficient manner.
5. ITA—Institute of Transport and Automation Technology: The Institute's goals are to provide well-organized, secure and smart means of transporting products and raw materials efficiently. It also creates new techniques for optical waveguides.
6. IW—Institute of Materials Sciences: The main goal of the institute is to develop customized high-performance material.

Product manufacturing involves different stages such as planning, design and development etc. The role of researchers at PZH is to examine the complete process of product manufacturing stages. Now a few days, the focus is on developing tailor-made services, developing fresh, customized products, and optimizing manufacturing instruments and systems, particularly in the field of special purpose equipment and prototype building. The results of the universities are transferred to the industry to make a prototype to test the results. Furthermore, to enhance the production capabilities and to ensure the sustainable production technologies and logistics, they make the best use of the machinery and equipment in place. Moreover, they also consider comfort of people-at-work an important element. The productivity of employees can be improved by studying and providing a better working environment [69, 70]. The PZH's primary study fields are:

1. Top-level research in fundamentals and practice

The German Research Foundation promotes interdisciplinary projects. PZH's top level research in fundamentals is documented in the research unit at PZH as well as it is documented by three collaborative research centres. Furthermore, PZH is also known as its unique and rare orientation towards practice. Fast transfer of knowledge from the institutes towards the industry is always given a high priority at PZH. At the same time, learning from experiences and joint development through working groups or through bilateral projects are highly appreciated [68].

2. Computer-aided manufacturing and Industry 4.0

In 2016, PZH set up the first SME 4.0 Competence Center in Germany. The large challenge was how to create Lower Saxony and Bremen small and medium-sized businesses eligible for Industry 4.0? To bridge the divide, the science fundamentals

were needed. Hence, the Collaborative Research Center supplied delicate parts, machine tools and technologies to enhance communication. The scientific foundations have been named "Gentelligent Components" [68].

3. Preserve resources, create sustainable processes

Sustainable production is an essential course in academic education. PZH approved and carried out three important projects in order to map the objectives of sustainable production. The three projects were (a) "dexterous regeneration cell" this provides the concept of repairing turbine components, (b) energy consumption of a machine tool can be reduced by more than one third by cooling lubricants adaption based on actual demand, (c) improve resource efficiency of companies is measured by optimum resource saving during the production process [68].

4. Medical engineering: helping the body heal

Many medical engineering related projects completed in 2015 after a long journey of 12 years under the umbrella of Collaborative Research Centre "Biomedical Engineering" at PZH. Many medical researchers, veterinarians and technicians work in collaborative environments in medical engineering. In addition to many good outputs of the collaborated projects, the most significant innovations were endoprostheses and bioresorbable magnesium alloys. Once a fracture has cured, bioresorbable magnesium alloys can dissolve in the body [68].

5. Back to green field status—Decommissioning nuclear power plants

One of the biggest challenges in nuclear power plants is dismantling reactors without harming the staff and its surrounding environment. The best way is to access and decommission nuclear reactors internally inside their contained environment hence producing a very little waste which is considered to be a tough job. Wire saw technology in particular is used to separate composite products from metal and steel. Researchers at PZH developed methods to access reactors inside their contained environment to dismantle them which includes welding and cutting are methods, electron beam and water jet technologies [68].

6. Technologies for aerospace industries

Aerospace industry is ever growing and requires continues upgradation in technology and systems. PZH provides an international platform for continuous efforts in the field of aerospace engineering under the consortium of "Machining Innovations Conference for Aerospace Industry". Researchers are constantly addressing novel production-related problems in the aerospace industry, such as the processing of combinations of CFRP-titanium materials. CFRP's financial output is covered by "CFK Nord," which is Stade's study branch in the aviation sector neighborhood [68].

There are 550 students of mechanical engineering engaged in separate studies. Besides all studying, teaching and graduating; about 550 learners of mechanical engineering are already engaged in research projects at the PZH. They get to know

of a project as either being student assistant or by organizing status symposia where they make and collaborate with industry experts. Students have to develop a study project in view of their project-oriented bachelor or master dissertation requirements. In addition, they have the opportunity to experience multiple study areas first hand. This practice enables them to find out and sometimes even build new research interests and specialized strengths. Not surprisingly, as a PhD student, many student assistants join "their" institute after completing their studies. Once researcher, under new circumstances now they are accountable for the future of their own developed devices, progress of ongoing study projects and assignments of students assigned to them—many are engaged in teaching duties. Some students are also given management duties such as being Head of a Department.

One major benefit for learners or student assistants at PZH is that the lecture hall is near to the exam areas that provide top-level facilities: state-of-the-art analyzer systems, machine tools, and the Underwater Technology Center providing an excellent study environment along with finest conditions for up-to-date application-oriented training. The students are exposed to full process industrial mapping and provided associated know-how under one umbrella. These are some of the benefits of studying at PZH, which has seven institutes that promotes research and education in all respects. Students as well as scientists benefit from these facilities. Many are able to create direct contact with peers working on project's adjacent elements. PZH allows for large-scale interdisciplinary study projects requiring close collaboration between all parties engaged in the process. Last but not least, businesses can take advantage of study projects and graduates taking a wider perspective of manufacturing and its difficulties.

8.4 Conclusion

In terms of computer systems, we are witnessing significant paradigm changes enabled by Disruptive technologies. The ability to collect Big Data, use it to model physical environments with incredible precision and use it to improve present systems is a main factor behind the upcoming revolution. To move and transform these actual information into mobile information, we use Cyber Physical Systems (CPS)—to track and manipulate our physical world and Internet-of-Things (IoT). Many difficulties must be confronted in this situation. The difficulties, such as concerning the ability to interconnect disparate data sources, such as: providing high connectivity and device interoperability, machines and human operators, in conjunction with handling of big quantities of information originating from them, implementation of tailor-made and proactive methodologies and strategies for managing these new technologies, the need to make use of the effort and know-how from distinct fields and professionals in each industry and the chance of precious and reliable data being accessible. All these difficulties demand intelligent production systems. Smart manufacturing systems are multidisciplinary complex systems that use mechatronic systems regarded as CPSs. This chapter explores the

various domains revolving around CPS, challenges, applications and the ecosystem. Industry 4.0 and the sector wise implication gives an insight to the real world applications. Lastly, some case-studies are discussed to have a better understanding of the domain.

References

1. Jóźwiak, L.: Embedded computing technology for highly-demanding cyber-physical systems. IFAC—PapersOnlLine **48**(4), 019–030 (2015)
2. Sztipanovits, J.: 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS '07), pp. 3–6. IEEE Computer Society (2007)
3. Kramer, B.J.: Evolution of cyber-physical systems: a brief review. In book: Applied Cyber-Physical Systems, Springer (May 2012)
4. Wang, J., Abid, H., Lee, S., Shu, L., Xia, F.: A secured health care application architecture for cyber-physical systems. Control. Eng. Appl. Inform. **13**(3), 101–108 (2011)
5. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Futur. Gener. Comput. Syst. **25**(6), 599–616 (2009)
6. Nithya1 S., Sangeetha M., Apinaya Prethi, K.N.: Role of cyber physical systems in health care and survey on security of medical data. Coimbatore Institute of Technology, India
7. Rawung, R., Putrada, A.: Cyber physical system: paper survey. [online] Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7013187 (2014). Accessed 28 May 2019
8. Available at: http://chess.eecs.berkeley.edu/cps/
9. Song, Z., Chen, Y.Q., Sastry, C.R., Tas, N.C.: Optimal Observation for Cyber-Physical Systems: A Fisher-Information-Matrix-Based Approach. Springer-Verlag, London (2009)
10. Rajkumar, R.: A cyber-physical future. Proc. IEEEE, vol. 100, no. Special Centennial Issue, pp. 1309–1312 (May 2012)
11. Tricaud, C., Chen, Y.Q.: Optimal mobile actuator/sensor network motion strategy for parameter estimation in a class of cyber physical systems. In: Proceedings of the 2009 American Control Conference St. Louis, MO, 2009, pp. 367–372
12. Liu, Y., Peng, Y., Wang, B., Yao, S., Liu, Z.: Review on cyber-physical systems. IEEE/CAA J. Autom. Sin., **4**(1) (January 2017)
13. Zhao, W.: Cyber-physical system research. Mar. 2006. [Online]
14. Available: http://varma.ece.cmu.edu/cps/Presentations/Zhao.pdf
15. Khaitan, S.K., Mccalley, J.: Design techniques and applications of cyber physical systems: a survey. IEEE Syst. J. (2014)
16. Chen, H.: Applications of cyber-physical system: a literature review. J. Ind. Integr. Manag. **2** (3), 1750012 (28 Pages) (2017)
17. Kao, Hung-An, Lee, Jay, Siegel, David: A cyber physical interface for automation systems—methodology and examples. J. Mach. **3**, 93–106 (2015)
18. Akhil, J., Aluvalu, R., Samreen, S.: Cyber physical systems for smart cities development. Int. J. Eng. Technol. **7**(4.6), 36–38 (2018)
19. Ghaemi, A.: A cyber phisical system approach to smart city development. In IEEE International Conference on Smart Grids and Cities, pp. 257–262 (2017)
20. Zanni, A.: Cyber phisical systems and smart cities developer works. IBM (2015)
21. Broy, M., Cengarle, M.A., et.al.: CPS: Imminent Challenges in Large Scale Complex IT Systems, Development Operations and Management. Springer, pp. 1–28 (2012)

22. Frmhold-Eisebith M.: Cyber phisical systems in smart cities mastering technological economics and social challenges smart cities, foundations, principles and applications, 1st edn, pp. 1–21. Wiley (2017)
23. Owen, S., Anil, R.: Ted Dunning, and Ellen Friedman. Mahout in Action. Manning Publications (2011)
24. Ghoting, A., Krishnamurthy, R., Pednault, E., Reinwald, B., Sindhwani, V., Tatikonda, S., … Vaithyanathan, S.: SystemML: declarative machine learning on MapReduce. In: 2011 IEEE 27th International Conference on Data Engineering (ICDE), pp. 231–242. IEEE (2011)
25. Bifet, Albert, Holmes, Geoff, Pfahringer, Bernhard, Kranen, Philipp, Kremer, Hardy, Jansen, Timm, Seidl, Thomas: MOA: massive online analysis, a framework for stream classification and clustering. J. Mach. Learn. Res. Proc. Track **11**, 44–50 (2010)
26. Cesa-Bianchi, N., Lugosi, G.: Prediction, learning, and games. Cambridge University Press (2006)
27. Babcock, B., Babu, S., Datar, M., Motwani, R., & Widom, J. (2002, June). Models and issues in data stream systems. In: Proceedings of the Twenty-first ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (pp. 1–16). ACM
28. Cormode, G., Muthukrishnan, M.: approximating data with the count-min sketch. Software, IEEE **29**(1), 64–69 (2012)
29. Ntarmos, N., Triantafillou, P., Weikum, G.: Distributed hash sketches: scalable, efficient, and accurate cardinality estimation for distributed multisets. ACM Trans. Comput. Syst. (TOCS) **27**(1), 2 (2009)
30. Chabchoub, Y., & Heébrail, G. (2010, December). Sliding hyperloglog: estimating cardinality in a data stream over a sliding window. In: 2010 IEEE international conference on data mining workshops (ICDMW), (pp. 1297–1303). IEEE
31. Matusevych, S., Smola, A., Ahmed, A.: Hokusai-sketching streams in real time. arXiv preprint arXiv:1210.4891 (2012)
32. Heule, S., Nunkesser, M., Hall, A.: HyperLogLog in practice: algorithmic engineering of a state of the art cardinality estimation algorithm (2013)
33. Chawla, N.V.: Data mining for imbalanced datasets: an overview. In: Data Mining and Knowledge Discovery Handbook (pp. 875–886). Springer US (2010)
34. Gama, J., Sebastião, R., Rodrigues, P.P.: Issues in evaluation of stream learning algorithms. In: Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 329–338). ACM (2009, June)
35. Dean, J., Ghemawat, S.: Mapreduce: simplified data processing on large clusters. ACM, Commun (2008)
36. Apache Haddop: http://hadoop.apache.org/ (2014)
37. Apache Spark: http://Spark.apache.org/ (2014)
38. Allam, Z., Dhunny, Z.A.: On big data, artificial intelligence and smart cities. J. Cities, (2018)
39. Zeid, A., Sundaram, S., Moghaddam, M., Kamarthi, S., Marion, Tucker: Interoperability in smart manufacturing: research challenges. J. Mach. **7**, 21 (2019)
40. Santos, B.P., Santos, F.C., Lima, T.M.: Industry 4.0: an overview. [Available on] https://www.researchgate.net/publication/326352993_Industry_40_an_overview (2018)
41. Lasi, H., Fettke, P., Kemper, H.G., Feld, T., Hoffmann, M.: Industry 4.0. Bus. & Inf. Syst. Eng., **6**(4), 4.0; Bus. & Inf. Syst. Eng., **6**(4), 239–242 (2014)
42. Posada, J., Toro, C., Barandiaran, I., Oyarzun, D., Stricker, D., Amicis, R., Pinto, E. B., Eisert, P., Döllner, J., Vallarino, I.: Visual computing as a key enabling technology for industry 4.0 and industrial internet. IEEE Comput. Graph. Appl. **35**(2), 26–40 (2015)
43. Gizem, E.: How To Define Industry 4.0: Main Pillars Of Industry 4.0. Available at: https://www.researchgate.net/profile/Gizem_Erboz/publication/326557388_How_To_Define_Industry_40_Main_Pillars_Of_Industry_40/links/5b55de5545851507a7c19cc4/How-To-Define-Industry-40-Main-Pillars-Of-Industry-40.pdf?origin=publication_detail (2017). Accessed May 4, 2019
44. Hofmann, E., Rüsch, M.: Industry 4.0 and the current status as well as future prospects on logistics. Comput. Ind. **89**, 23–34 (2017)

45. Gartner—IT Glossary. Available at: https://www.gartner.com/it-glossary/digitalization/. Accessed April 21, 2019
46. Gray, J., Rumpe, B.: Models for Digitalization. Softw. Syst. Model. **14**(4), 1319–1320 (2015). https://doi.org/10.1007/s10270-015-0494-9
47. Scardapane, S., Wang, D., Panella, M.: A decentralized training algorithm for echo state networks in distributed big data applications. Neural Netw. **78**, 65–74 (2016)
48. Ungurean, I., Gaitan, V.G.: An IoT architecture for things from industrial environment. In: Communications (COMM), IEEE 2014 10th International Conference, pp. 1–4 (2014)
49. Lu, Y.: Industry 4.0: a survey on technologies, applications and open research issues. J. Ind. Inf. Integr. **6**, 1–10 (2017)
50. Lin, F., Chen, C., Zhang, N., Guan, X., Shen, X.: Autonomous channel switching: towards efficient spectrum sharing for industrial wireless sensor networks. IEEE Internet Things J. **3** (2), 231–243 (2016)
51. Vijaykumar, S., Saravanakumar, S.G., Balamurugan, M.: Unique sense: smart computing prototype for industry 4.0 revolution with IOT and bigdata implementation model. Indian J. Sci. Technol. **8**(5), 1–4 (2015)
52. Geographica.: Trends in digital transformation in the retail sector. Available at: https://geographica.com/en/blog/retail-sector/ (2019) Accessed April 24, 2019
53. Rahman, H., Rahmani, R.: Enabling distributed intelligence assisted future internet of things controller (FITC). Applied Computing and Informatics. Available at: http://linkinghub.elsevier.com/retrieve/pii/S2210832717300364 (2017). Accessed May 4, 2019
54. Thames, L., Schaefer, D.: Software-defined cloud manufacturing for Industry 4.0. Procedia CIRP **52**, 12–17 (2016)
55. Conti, M., Das, S., Bisdikian, C., Kumar, M., Ni, L., Passarella, A., Roussos, G., Tröster, G., Tsudik, G., Zambonelli, F.: Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence. Pervasive Mob. Computing. Val. **8**, 2–21 (2012)
56. Lee, E.: Computing needs time. Commun. ACM **52**(5), 70–79 (2009)
57. National Science Foundation: Cyber Physical Systems, Program Solicitation. NSF 10–515 Available at: https://www.nsf.gov/pubs/2010/nsf10515/nsf10515.htm. Accessed May 4 2019
58. Ivanov, D., Sokolov, B., Ivanova, M.: Schedule coordination in cyber-physical supply networks Industry 4.0, IFAC-PapersOnLine Vol.49, **12**, 839–844 (2016)
59. Posada, J., Toro, C., Barandiaran, I., Oyarzun, D., Stricker, D. Amicis, R., Vallarino, I.:Visual computing as a key enabling technology for Industry 4.0 and industrial internet. IEEE Comput. Graphics Appl. **35**(2), 26–40 (2015)
60. Roblek, V., Meško, M., and Krapež, A.: A complex view of Industry 4.0, SAGE Open **6**(2) (2016)
61. Shafiq, S.I., Sanin, C., Toro, C., Szczerbicki, E.: Virtual engineering object (VEO): toward experience-based design and manufacturing for Industry 4.0, Cybern. Syst. **46**(1–2), 35–50 (2015)
62. Shafiq, S.I., Sanin, C., Szczerbicki, E., Toro, C.: Virtual engineering factory: creating experience base for Industry 4.0, Cybern. Syst. **47**(1–2), 32–47 (2016)
63. Berre, A.J., Elvesæter, B., Figay, N., Guglielmina, C., Johnsen, S.G., Karlsen, D., Lippe, S.: The ATHENA interoperability framework. Enterprise Interoperability II, pp. 569–580. Springer, London (2007)
64. Ruggaber, R.: Athena-advanced technologies for interoperability of heterogeneous enterprise networks and their applications. Interoperability Enterp. Software Appl. SAP Research, pp. 459–460 (2006)
65. Sowell, P.K.: The C4ISR architecture framework: history, status, and plans for evolution. Mitre Corp, Mclean, VA (2006)
66. Synergy, European interoperability framework v 1.0, The IDABC Q. (2005) 01 (January), 2005
67. Science and Technology Options Assessment (STOA): Annual report for 2015, http://www.europarl.europa.eu/RegData/etudes/STUD/2016/563507/EPRS_STU(2016)563507_EN.pdf

68. https://ec.europa.eu/digital-single-market/en/news/new-report-shows-digital-skills-are-required-all-types-jobs
69. https://www.pzh.uni-hannover.de/fileadmin/PZH/_downloads/2016/WhatisthePZH_160219_2.pdf
70. https://ec.europa.eu/growth/tools-databases/regional-innovation-monitor/organisation/hannover-centre-production-technology-pzh

Chapter 9
Towards Integration of Cloud Computing with Internet of Things

Junaid Latief Shah and Heena Farooq Bhat

Abstract The "Internet of Things" refers to a novel technological innovation that enables pervasive communication of things with "physical or virtual world" via internet. As sensor devices and RFID communication have seen an exponential surge in recent years, humongous amounts of data gets generated, which becomes difficult to handle with limited processing and storage available in these sensor nodes. To overcome this, Cloud and IoT amalgamation also known as CloudIoT provides an efficient solution for bridging communication between heterogeneous devices and handling ever increasing data demands. CloudIoT framework permits seamless application deployment and service rendering using Cloud service based models. In this chapter, we review the available CloudIoT literature and present a holistic vision on the CloudIoT integration components. The chapter also presents seamless applications dispensed by CloudIoT platform and contemplates discussion on factors driving CloudIoT integration. The work in this chapter also highlights security issues affecting IoT layered architecture including vulnerabilities inherent in the Cloud. Also a brief discussion on some potential mitigation measures will be provided. The chapter also elaborates discussion on various CloudIoT platforms that aim at solving heterogeneity issue between the Cloud and Things. Finally, the chapter concludes by identifying some open research issues and challenges hampering Cloud and IoT integration.

Keywords Cloud · Things · Sensor · IoT · RFID

J. L. Shah (✉)
Department of Information Technology, Sri Pratap College, Cluster University Srinagar, Srinagar, India
e-mail: junaidlatiefshah@gmail.com

H. F. Bhat
Department of Computer Science, University of Kashmir, Srinagar, India
e-mail: heenafarooq14@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_9

9.1 Introduction

Evolution in technology and radio data transmission has allowed real time monitoring, efficient management and reliable transmission of mission critical data over internet [61]. Since the year 2012, the number of internetworking objects has outnumbered the global population. From the year 2020, "Cisco" predicts that more than 50 billion interconnected things will be communicating over internet that include sensor devices, mini tablet computers, smart phones and GPS enabled devices and related technologies [38]. The "Internet of Things" or "IoT" proves to be rudimentary step in digital evolution providing varied applications and dispensing wireless connectivity and accessibility in our lives. The IoT consists of small sensor objects or things having the ability to sense the environment and capture the data. As these devices are interconnected with each other via a wireless medium, they transmit the data collected into powerful storage platform called Cloud [13]. For communication and data transmission, these sensor devices use heterogeneous technologies and protocols which include "Bluetooth", "Zigbee", "Near Field Communication (NFC)", and "Radio Frequency Identification (RFID)". To transmit information over large geographical distances, IoT's employ mobile data transmission services which include "GPRS-Edge", "3G" and "4G over LTE" [15]. These sensor objects work autonomously without any human involvement, often referred to as "Machine-to-Machine communication (M2M)". IoT finds application in diverse areas ranging from developing smart home systems, smart city, environment surveillance, power management and healthcare management. These application areas generate humongous amount of data which demand real time processing [45]. This however requires flexible network architecture that would underpin high traffic volume that gets generated by heterogeneous devices. With the exponential rise of these heterogeneous devices, performance of IoT decreases substantially [9]. The reason being constrained power and limited bandwidth available in these devices. Thus, migrating data and computation from real world environment to virtual platform i.e. from "IoT to Cloud" seems to be a coherent solution. The Cloud dispenses a feasible, on-demand, pliable and agile platform for application deployment and provides access to virtually unlimited networked computing infrastructure [14]. These computing infrastructures offer extensive processing power and substantial virtual storage that augment the constrained resources in IoT devices, hence providing robust platform for pervasive communications [2]. To define correlation and integration between heterogeneous IoT devices and Cloud platform, the concept of CloudIoT or "Cloud of Things" (CoTs) evolved at MIT's Auto-ID labs [17]. The IoT's are small internet ready devices that are distinctly pervasive and ubiquitous; however suffer from limited computational power and storage. These drawbacks contribute to performance bottlenecks, security flaws and privacy affairs in IoT nodes [39]. Contrary to this, Cloud offers robust, flexible and agile platform for IoT application deployment. With CloudIoT, it is envisioned that two heterogeneous technologies will integrate for dispensing efficient power and resource management, and for developing

innovative solutions that cater diverse application areas [2]. This technological framework can serve delay sensitive as well as real time applications in a reliable and secure manner. With CloudIoT platform, the virtual resources are dispensed like a service on subscription or "pay-per-use" basis to the client users. CloudIoT framework permits seamless application deployment and service rendering using Cloud service based models which are "Infrastructure as a Service (IaaS)", "Platform as a Service (PaaS)" and "Software as a Service (SaaS)". Also, the framework ensures that end-to-end "Quality of Service (QoS)" is sustained in the network [49]. As an example, when service load request from client increases, the cloud must automatically augment itself to satisfy the request. Again when client request load reduces, the cloud must automatically adjust itself to accommodate the change [24, 26].

Some of the principal characteristics of CloudIoT implementation include virtually unlimited storage space and computational power for IoT nodes, pervasive and ubiquitous service model for users, cross platform support for applications, efficient resource management and end-to-end "Quality of Service (QoS)". However, with numerous tangible benefits of CloudIoT platform, the integration process is somewhat arduous and not that simple [2]. The integration framework must address issues related to economic and business perspective of service providers. Other issues contemplating CloudIoT platform involves reliable as well as secure communication and data storage [14]. As CloudIoT also involves financial and business transactions, the platform as such is vulnerable to attacks from malevolent systems. The problem becomes more convoluted in case of hybrid clouds where the main focus should be on safeguarding confidentiality, availability and data privacy including identity protection [49]. This entails employing cryptographic techniques for data encryption and authentication. Also, to avoid any physical damage to deployed IoT nodes, tamper proof mechanisms should be designed and regular on-site monitoring check should be carried out [48]. Integrating two heterogeneous technologies i.e. Cloud and IoT involves interconnection and data exchange between divergent networks. These disparate networks should be flexible, unrestricted and should underpin heterogeneous data and services [33, 35].

In this chapter, we review the available CloudIoT literature and present a holistic vision on the CloudIoT integration components. The chapter also presents seamless applications dispensed by CloudIoT platform and contemplates discussion on factors driving CloudIoT integration. The work in this chapter also highlights security issues affecting IoT layered architecture including vulnerabilities inherent in the Cloud. Also a brief discussion on some potential mitigation measures will be provided. The chapter also elaborates discussion on various CloudIoT platforms that aim at solving heterogeneity issue between the Cloud and Things. Finally, the chapter concludes by identifying some open research issues and challenges hampering Cloud and IoT integration.

The entire chapter is segregated into ten sections. Section 9.2 presents background and related work that has been carried in the integration process of Cloud and IoT. Section 9.3 discusses "Internet of Things" model and its hierarchical architecture. Section 9.4 presents discussion on Cloud Computing and its

deployment and service models. Section 9.5 introduces CloudIoT and presents a holistic vision on the CloudIoT integration components including its diverse applications. Section 9.6 highlights security issues affecting IoT layered architecture including vulnerabilities inherent in the Cloud. Section 9.7 presents related work on the study of security issues that has been carried over a period of time including potential measures for mitigation. Section 9.8 contemplates discussion on some existing CloudIoT platforms that try to bridge the gap between two heterogeneous components by implementing a middleware between the Cloud and IoT. Section 9.9 highlights some open research challenges and issues in this research area. Finally, Sect. 9.10 presents the chapter conclusion.

9.2 Related Work

The Cloud and IoT have seen an exponential and myriad rise in recent years with scientists working tirelessly for their flawless integration. However, CloudIoT which is in its genesis lacks established framework architecture guiding data communication, reliable storage and powerful computation [2]. As IoT supports disparate technology protocols, attribute features such as adaptability, reliability, accessibility and authenticity are very arduous to attain. Also as "IoT" suffers from constrained energy sources and computational capability, its amalgamation with "Cloud" platform will assist in vanquishing inherent bottlenecks. On the other hand, "Cloud empowers IoT" by extending its capabilities to interconnect with real world objects [10, 30]. The research papers available online on "Cloud and IoT" integration presents a very precise and summarized view of the concept, however in this chapter; we try to bridge this gap by surveying the latest available literature and highlighting the key motivating factors for integration.

In [10], a detailed review on Cloud and IoT integration is presented. The work identifies diverse characteristics of Cloud and IoT and the prime factors responsible for CloudIoT integration. Also detailed overview of research challenges has been presented. The paper also highlights some of the well known CloudIoT platforms including services. Finally the work concludes by underlining potential future research areas. Authors in [39] have attempted a similar work by emphasizing on viability of services dispensed by CloudIoT integration. The work in [17] elaborates discussion on steps needed to perceive and practically implement the CloudIoT concept. An abstract architecture of CloudIoT is also presented; however some significant issues have not been highlighted. To manage physical sensors on cloud framework, authors in [54] propose Sensor-cloud based infrastructure and discuss its architecture and implementation. However, the proposed implementation focuses only on transforming a "physical sensor into virtual sensor" on the cloud framework. In [23], authors have attempted a similar work and propose "Pub-Sub model" for flawless amalgamation of sensor objects with powerful cloud platform.

Even though a number of research constraints have been underlined, however, the work fails to address the key inherent issue in sensor-cloud integration. Although IoT and Cloud based applications has witnessed a surge in recent years, however no significant work has been done on the integration of disparate and distributed sensors in a realistic and feasible approach. In [19], researchers propose cloud based open source communication platform called "IoTCloud" that allows developers to write flexible and smart sensor compatible IoT applications. The underlying programming language used is Java and applications are hinged on an open platform like "Apache Active MQ" including "JBoss Netty". For empirical evaluation and performance analysis, authors employ "Future-Grid" Cloud test bed. Another open source platform presented in [44] known as "OpenIoT" project allows immaculate interaction between IoT interface and Cloud platform. The "OpenIoT" offers a platform for data collection from any geographically distributed sensor nodes and also concurrently assures their complete monitoring. The project also provides varied number of visual tools that permit seamless application deployment. Authors in [21] present current principal notation for Inter-cloud architecture. The authors also contemplate discussion regarding current "Inter-Cloud" frameworks that help management of pervasive and diverse range of applications on heterogeneous cloud platforms with focus on their non functional requirements. The authors also present an overview of the current available literature and highlight some open research issues in this area. However; the paper fails to define its relationship with IoT. Similarly works in [11, 50] also do not discuss any relationship with IoT. Today, IoT devices supporting multimedia operations require robust multimedia processing systems for seamless data transfer. To achieve this, "Media Cloud" proves to be a coherent panacea that can fulfill ever increasing demand towards multimedia data transmission using underlying IoT network. However, the challenging task would be to maintain tolerable QoS in the network. To underpin this, the use of IPv6 is highly recommended that offers Flow Label and Traffic Class for maintaining end-to-end QoS in the network. To further improve the performance and lower propagation delay in streaming of multimedia, improving QoS using queuing techniques needs to be implemented. The work in [59] presents a "Media-Edge Cloud" (MEC) framework that combines storage space, "Central Processing Unit (CPU)", and "Graphics Processing Unit (GPU)". The "Media-Edge Cloud" efficiently accomplishes concurrent and pervasive computing and also providing simultaneous services for maintaining tolerable QoS. However, the empirical cost analysis incurred is not deliberated. Most of work discussed above reviews Cloud and IoT separately without discussing any substantial relationship between the two. However, this chapter takes a profound insight into CloudIoT paradigm and underlines its integration components. The Chapter also highlights some of the potential issues inherent in CloudIoT framework with their feasible and viable solutions.

9.3 Internet of Things Model

The title "Internet of Things (IoT)" or "Internet of Objects" evolved originally in "Future of Internet and Ubiquitous Computing" and was conceived by a British scientist "Kevin Ashton" [53]. Kevin envisioned a system where the real world environment can be mapped or connected to virtual world using internet enabled sensor objects. This technological evolution varies from conventional internetworks and represents the future of ubiquitous computing. The IoT operates in an environment involving heterogeneous devices that communicate using divergent protocols [28]. The "things" in IoT represents any object or device that interconnects with other objects or devices in the network. For communication with other devices, IoT employs short range data transmission and lower power dissipation devices which include "Radio Frequency Identification (RFID)", "Bluetooth" and "Zigbee" etc. The IoT offers a flexible and convenient framework for humans to interact with the environment around us. Although the popularity of IoT has surged over the years, however no standard definition is yet available for the technology. In basic terms, IoT represents an internetwork of small connected devices or objects. These devices use sensors to perceive the environment around them, capture the data and transmit or share this data over the internet for additional tasks [32].

9.3.1 Hierarchical Architecture

Due to global popularity and promising future, "Intel" labeled IoT as "Embedded Internet". This is due to the fact that today, embedded devices used in everyday appliances have the ability to connect and transmit information over the Internet. As depicted in Fig. 9.1, the IoT principal architecture is segregated into four layers in a given hierarchy: "Perception or Physical layer", "Network or Transport layer", "Middleware layer" and "Application or Service layer". Every hierarchical layer performs a defined function and services the layer above it.

"*Perception Layer*"

This represents first layer in the hierarchy and involves the use of small physical sensors, "RFID's", "Barcode tags" etc. The principal functionality assigned to this layer is to sense and capture information and transmit this information to the remote server node. Analogous to OSI model, the information captured by this layer is transmitted to upper layers for further operation.

"*Network Layer*"

This layer is composed of networking protocols that assist in data transfer from intended source to destination or sink node. The source and sink are usually assigned distinct IP addresses.

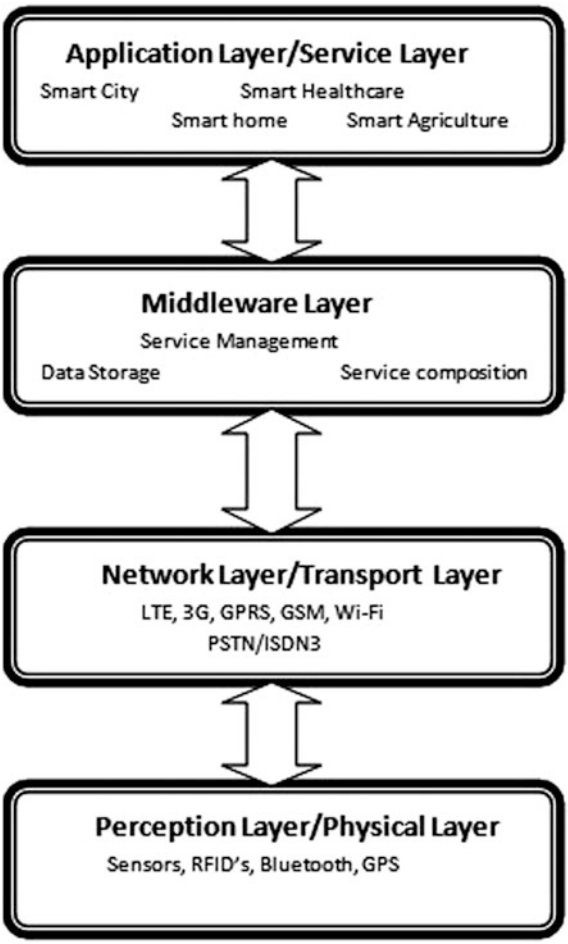


Fig. 9.1 Hierarchical IoT architecture

"*Middleware Layer*"

This is an intermediate layer between network and application layer. This layer offers varied data management services that preprocess the data and output it to next layer.

"*Application Layer*"

This represents the uppermost layer in the hierarchy and presents application interface for user data. The layer dispenses various user application functions underpinned by below middleware layer. These services promote diverse range of application areas like industrial automation systems, automated e-healthcare, smart city, smart traffic etc.

9.4 Cloud Computing Model

Cloud Computing offers an on-demand service platform that dispenses seamless access to infinite warehouse of pervasive and distributed infrastructure which include computational power, humongous database, software and business data analytics. The approach involves storing data on a remote database server and performing computation and processing using powerful remote virtual servers, thus reducing the management tasks on account of its client users [36]. The adaptation of Cloud platform for IoT has been favored for a number of reasons which include: being economically feasible, reliability and performance, rapid elasticity, scalability and robust security [36]. The Cloud Computing model offers four distinct features that differentiate it from traditional processing systems. First; it offers an "on-demand service model" which allows a client to utilize server storage and processing as per his convenience and time. Second, it provides a "broader network access" by employing varied devices like smart phones, tablet computers and also desktop machines. Third, it "pools various resources" and combines them to build a large warehouse repository which are distributed to clients on demand. Fourth, it promotes "rapid elasticity" of resources that permits a server to adjust to client request as per load and demand.

As illustrated in Fig. 9.2, the Cloud platform offers service to the clients at three distinct levels: "Infrastructure as a Service (IaaS)", "Software as a Service (SaaS)" and "Platform as a Service (PaaS)".

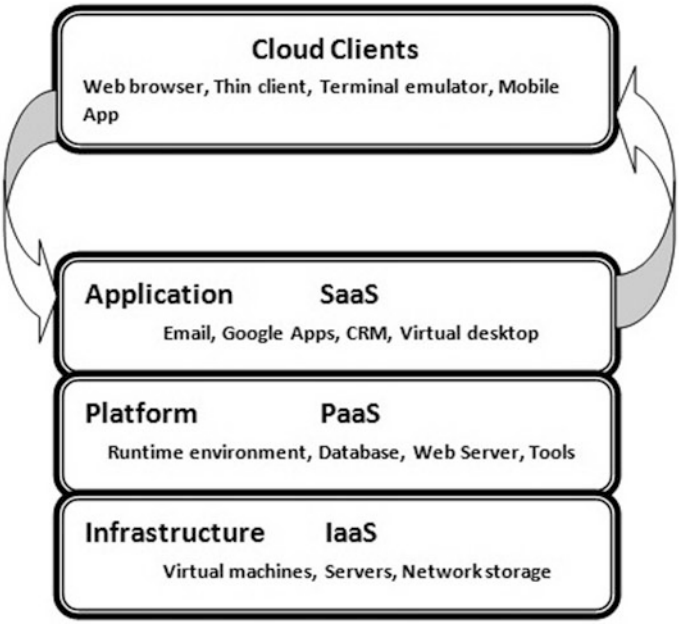


Fig. 9.2 Cloud service models

"*Infrastructure as a Service (IaaS)*"

The IaaS platform dispenses a virtual environment to the clients in which infrastructure resources which include virtual machines, storage and networking are provided on subscription basis. The platform provides a billing system wherein the users pay for Infrastructure on demand. The hired infrastructure is highly scalable depending on user's processing and storage requirements.

"*Software as a Service (SaaS)*"

The SaaS model dispenses a seamless access to cloud software and database on subscription basis. The installation, up-gradation and troubleshooting of software is managed by the SaaS platform. The user data remains secured in the cloud and failure of infrastructure hardware does not result in data loss. The applications installed on the cloud can be run remotely via internet from anywhere in the world.

"*Platform as a Service (PaaS)*"

The "PaaS" platform offers users an integrated software development and management interface. The users can manage, develop, test and deliver applications using this interface in addition to software and database design tools that allow direct web application deployment. The platform also provides an efficient collaborative work environment in which different users work together remotely.

In addition to cloud service models, the technology offers four distinct deployment platforms which are discussed below and are depicted in Fig. 9.3.

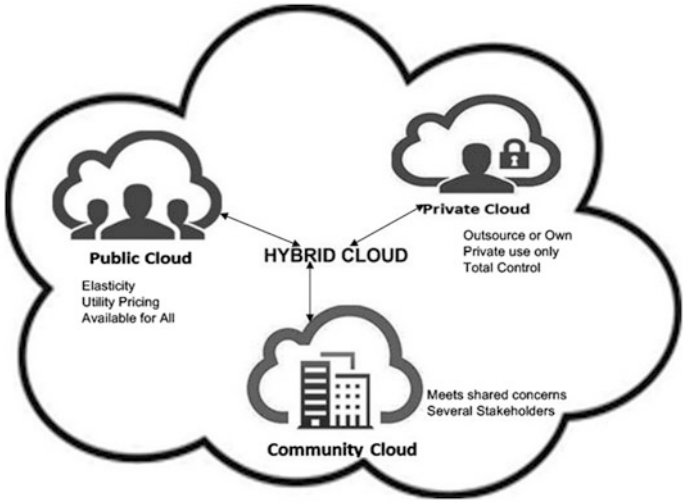


Fig. 9.3 Cloud deployment models

"*Public/External Cloud*"

The "Public or External Cloud" offers unrestricted or public access to the cloud platform. The service provider owns the platform resources and clients pay as per service usage.

"*Private/Internal Cloud*"

The "Private or Internal Cloud" is generally owned or hired by a company or business organization for its personalized usage. The organizations usually deploy business critical applications on this cloud model.

"*Community Cloud*"

The "Community Cloud" is owned by a community of business enterprises having related interests and activities.

"*Hybrid/Virtual Private Cloud*"

This deployment platform offers a blend of private/public/community clouds.

9.5 CloudIoT: Integrating Cloud with IoT

The popularity of Internet based computation has increased the number of objects or things getting interconnected with each other. This in turn has led to increased data generation rate by things or objects. As IoT devices have constrained storage space, it is not thus possible to store this data locally on interim storage devices. Earlier; the sensors would transmit data to mainframe computers which had the required computing infrastructure and resources. However, this approach had some drawbacks. First, running applications and storing data on mainframes was costly and time consuming. Second, in case of failure, the entire system would shut down. Another approach was distributed computing wherein nodes were equipped with minimal storage and processing. However, this approach too had limitations which include cost of IoT node replacement in case of failure and cost for providing the backup power. Recent times have seen an increased demand for low cost IoT devices with efficient computational power. As such technological evolution of CloudIoT seems to provide a potential solution that is tangible, robust, less convoluted and cost effective [1, 8]. The IoT component functionality involves sensing the environment, capturing data and transmitting this data to outside world via internet while as Cloud platform provides a systematic and a flexible computing resource [58]. Figure 9.4 illustrates the working operation of CloudIoT communication. As illustrated, the data from the sensor nodes is passed to various IoT layers which further transmit the data to the cloud where it is stored and processed. Although "Cloud and IoT" are two divergent technological platforms, the current research data presents their corresponding features and attributes that underline the rationale for their amalgamation. These features and characteristics as obtained

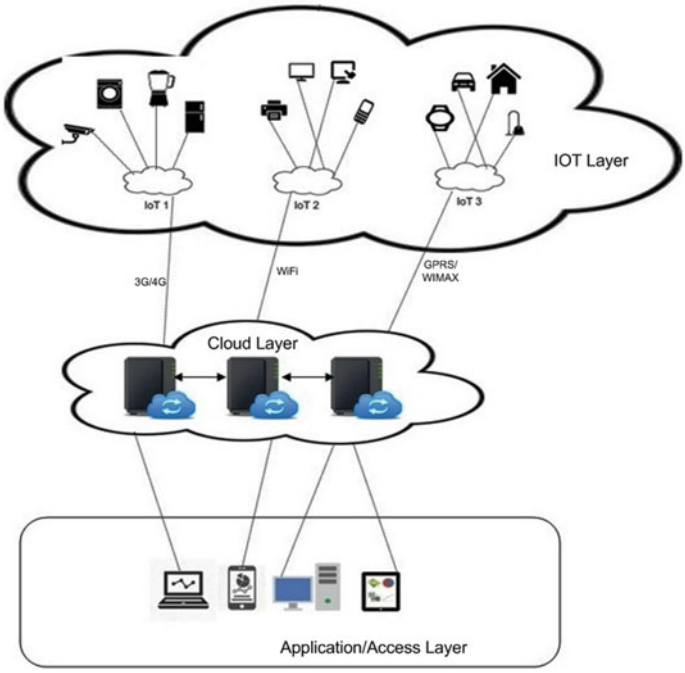


Fig. 9.4 CloudIoT operational scenario

Table 9.1 Comparison of IoT and cloud characteristics

Characteristic	IoT	Cloud
"Displacement"	Pervasive (things are everywhere)	Centralized and condensed service
Availability	Restricted	Distributed (remote access to resources)
Device nature	Things are real world objects	Virtual infrastructure available via internet
Computational power	Limited computational capacity	Virtually limitless processing power
Memory space	Sparse in nature	Scalable as per demand
Role of internet	Uses internet as convergence place	Employs internet for delivery of service
Big data	Contributes as prime source for big data	Big data processing and management is supported

from available research papers are reported in Table 9.1. With CloudIoT architecture, Cloud layer connects underlying IoT sensor objects and end user services at the access layer. The cloud also conceals complex operations and algorithms from the client user.

The motivating features driving the integration and adoption of CloudIoT framework are:

"*Storage*": The sensor nodes in "IoT" produce large volume of data by exploiting various information generation sources. This data is usually called as Big data and is classified as either semi-structured or non-structured [5]. This Big data has three well known properties [60]: which include "volume" (i.e. quantity of data), "variety" (i.e. data type heterogeneity) and "velocity" (i.e. rate of production of data). To capture, store, organize and examine such sizeable amount of data is infeasible for resource constrained sensor nodes. Thus Cloud offers an efficient and pliable choice to manage IoT data [40].

Once the data has been preserved in cloud storage, data analytics and data mining techniques can be applied to extract useful information and policy making. Also robust cryptographic procedures can be employed to secure sensitive data from malicious users.

"*Computing capabilities*": Nearly all IoT nodes have limited processing capacity that restricts their ability to perform complex data processing operations online. The feasible solution is to transfer the strenuous computational part to powerful and scalable server machines. The on-demand cloud service platform presents virtually infinite processing power and implementing flexible and instant policy making for sensor based services [46].

"*Communication*": Among the principal goals of IoT is to permit application data sharing and provide reliable communication among nodes over the internet. To supplement such communication incurs greater financial cost and as such is not feasible. Therefore cloud offers an effective and feasible economic solution for interconnecting, managing and personalizing applications remotely from anywhere [40]. To assist in remote administration and management of data, the cloud communications are underpinned by high speed optical fiber internet [46]. Although Cloud considerably improves Quality of Service (QoS) in communication with IoT nodes, however in certain situations still acts as a bottleneck which limits down its computational capacity. Thus feasible and realistic solutions need to be developed to enable large volume of data transfer between IoT and the Cloud.

"*New Capabilities and Paradigms*": The disparity between "IoT" objects and underlying protocols make adaptability, validity, accessibility and authenticity very arduous to attain. To resolve this issue, the Cloud offers easy resource access, robust and strong platform for applications and economically feasible deployment [13, 55]. The amalgamation of Cloud and IoT enabled smart devices and services manage contemporary real life situations. Table 9.2 (extracted from [10]) reports summary of new design models and standards evolved from this integration. Due to the lack of any standard terminology, the acronyms differ in various cases and have no coherent variance.

Table 9.2 Innovative services and models envisioned with CloudIoT

"Acronym"	Expanded form	Description of service
SaaS	"Sensing as a Service"	To dispense seamless access to sensor data
SAaaS	"Sensing and actuation as a Service"	To support automated control logistics with cloud implementation
SEaaS	"Sensor Event as a Service"	Transmitting real time messages triggered by events perceived by a sensor
SenaaS	"Sensor as a Service"	To enable Remote management of distributed remote sensors
DBaaS	"Database as a Service"	To enable Remote database administration
DaaS	"Data as a Service"	To support pervasive access to any data type
EaaS	"Ethernet as a Service"	Enabling distributed layer-II access for remotely distributed devices
IPMaaS	"Identity and Policy management as a Service"	Dispensing ubiquitous access to management of identity and policy
VSaaS	"Video Surveillance"	To enable remote video recording and performing examination and analysis on it

Source [10]

9.5.1 CloudIoT Applications

Integrating two heterogeneous platforms i.e. Cloud and IoT has created numerous opportunities that fully channelize the power of pervasive and distributed computing. In CloudIoT environment, the nodes/objects communicate using three different ways [14]. First, using "Machine-to-Machine (M2M)" interactions e.g. deployed sensor nodes triggering an interrupt when some anticipated event occurs. Second, using "Human-to-Machine (H2M)" interactions, e.g. humans commanding machines over voice identification systems. Third, using "Machine-to-Human (M2H)" interactions e.g. recognizing human characteristics by employing biometric devices. The seamless amalgamation of Cloud and IoT underpins the varied real world applications as shown in Fig. 9.5.

Healthcare: Healthcare represents an important application area of CloudIoT. In general terms; Healthcare monitoring using CloudIoT consists of (i) Set of sensors for recording physiological data of patients; (ii) "Wireless Body Area Network (WBAN)" that enables doctors to communicate with cloud server remotely; and (iii) Cloud server for data archival, computation, and mining. The healthcare generates humongous patient data that is archived by healthcare institutions within Cloud platform. Later, data mining and analytics techniques are employed for decision and policy making. To dispense cost effective and efficient healthcare solutions, employing smart objects and cloud applications is highly recommended that persistently contributes towards innovation and novel ideas in healthcare area. As smart phones have seen a surge in recent years, thus demand for robust security and acceptable Quality of Service (QoS) becomes apparent.

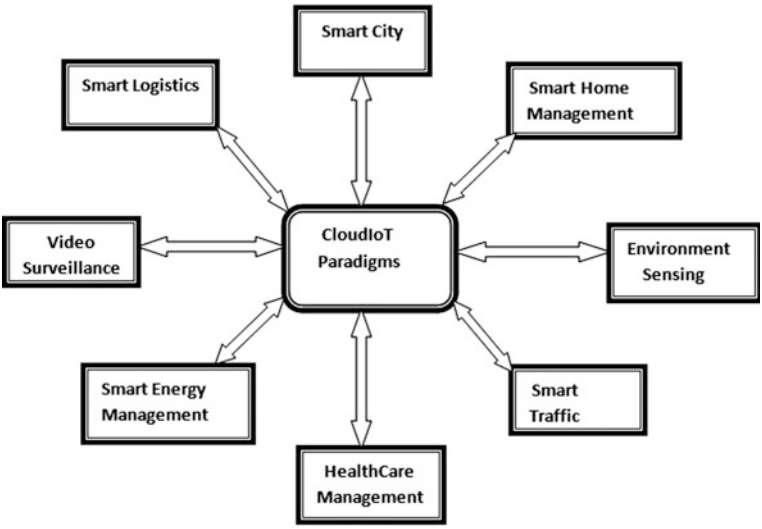


Fig. 9.5 CloudIoT applications

Smart City: CloudIoT forms an essential part in developing smart city infrastructure that aims to control issues related to traffic, environment, power, public lighting etc. The main focus is to refine and revamp the urban city life by providing better facilities and applications. For example, installing smart meters can improve detection of leaks in pipes. The customers can get real time access to information about their water consumption. Another application could be efficient management of city and traffic lights during the night.

Smart Home: The concept of smart home involves employing internet enabled devices to remotely monitor and control applications such as lighting bulbs, Geysers, heating appliances, energy consumption etc. Integration of Cloud with IoT dispenses a wide framework for management of home appliances having embedded sensors in devices [45].

Remote Video Surveillance: With respect to security, this is one of the important applications areas of CloudIoT that assists in achieving remote surveillance and monitoring. The deployed sensor objects capture data using video cameras and transfer this information to cloud servers. The cloud on the other hand provides sufficient storage space and computational power which wasn't previously possible.

Environment Observation: The CloudIoT also finds its application in observing and studying the behavior of changing environment around us. For example, in industries as well as in water bodies, the deployed sensors could detect the rise in the amount of pollution levels on real time basis. Similarly, monitoring air quality to check percentage composition of gases such as carbon-dioxide, carbon-monoxide, smog etc. Also, monitoring and checking degree of snowfall at mountain areas for weather updates and forestalling avalanches. The gathered data can later be transmitted to research labs for scientists to study and policy making.

9.6 CloudIoT Security Threats and Issues

The "CloudIoT" involves internetwork of connected things that drive common services ranging from smart city and homes, intelligent traffic monitoring, environment monitoring, industrial management machines as well as how these things interact with each other [22]. The Cloud presents an efficient service platform for things and supports easy access to shared infrastructure which includes computational power, humongous storage space, robust applications and seamless data analytics and mining capabilities [7]. Although CloudIoT has proven to be beneficial in ameliorating our daily life; however, there has been no security contemplation to its practical deployment scenario [25, 27]. In case of any vulnerability abuse in CloudIoT network, the services can be rendered non functional and critical information can be abused by malevolent users. The integration of Cloud and IoT will further aggravate the situation and as such will uncover concealed issues and vulnerabilities. The security flaws could be misused by malevolent actors to exploit CloudIoT network rendering billions of interconnected nodes vulnerable. Thus, loopholes in CloudIoT network will override its number of benefits. Also, it's not practical that deployed sensor nodes can be replaced periodically owing to its cost implications. The fundamental security architecture needs to be robust and persistent enough to work for substantial period of time without replacement and maintenance.

9.6.1 Security Features and Goals

CloudIoT supports data transmission between connected things and users to achieve precise goals. In order to safeguard communication in such a pervasive environment, it's essential that parameters such as authenticity, privacy and control need to be fortified. However, given the limitations imposed by constrained infrastructure (processing capability and storage) of nodes, the framework demands fine tuning in existing security methods in order to meet apparent security goals as shown in Fig. 9.6 [43].

"*Confidentiality*"

The confidentiality feature ensures authorized retrieval of the sensitive data and safeguards it from illegal access. The CloudIoT network relies on sensor nodes including RFID's that capture and store data and this information needs to be fortified from hostile nodes as well as malevolent users. To safeguard data and preserve confidentiality, cryptographic techniques and security protocols should be designed and employed [12].

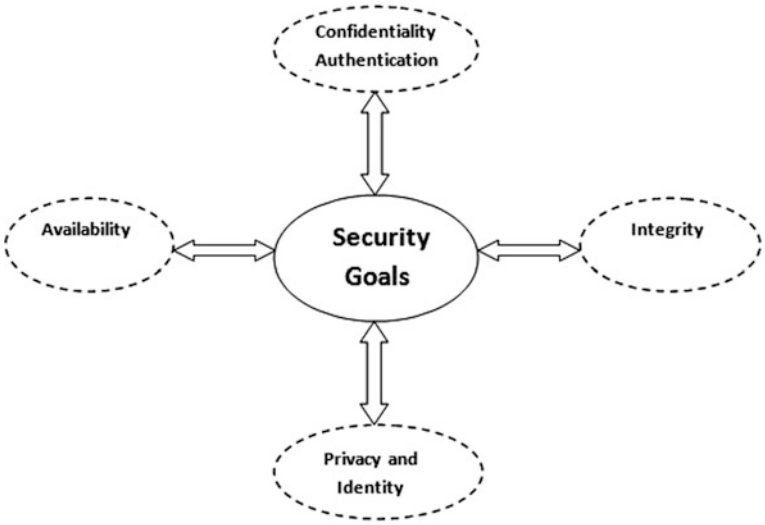


Fig. 9.6 CloudIoT security goals

"*Integrity*"

Data Integrity warrants that accuracy, consistency and reliability of data are preserved over entire duration of data transmission. During transit between legitimate nodes, the data cannot undergo any change and steps need to taken to prevent data fiddling or tampering. The integrity feature ensures that authentic and valid data is received by legitimate users. To enforce integrity principle, end-to-end security protocols need to be employed in data transit and reception.

"*Availability*"

The availability feature warrants that information and services are accessible to authorized users when required. The objects in CloudIoT network transact data in real time with minimal delays. However; failure to safeguard availability principle would result in unnecessary processing delays which would result in shutdown of network.

"*Identity and Authentication*"

The Identification and Authentication ratifies that valid information is transacted in CloudIoT network by authorized nodes. Though given the heterogeneity of the whole system and sensor nodes, the process becomes quite complicated [42]. The feasible and optimal solution would be enforcing strict authentication policies and protocols between the permissible entities of the internetwork.

"*Privacy*"

The privacy feature corroborates restricted information retrieval limited only to valid users. In contrast to confidentiality principle which employs encryption procedures to avert data tampering, the privacy factor permits restricted access without abstracting any other specific details.

9.6.2 Security Vulnerabilities

The CloudIoT security vulnerabilities include issues in both IoT network as well as those inherent in Cloud data model. In this section, we first discuss vulnerabilities in each layer of IoT architecture and then underline security loopholes in Cloud data model.

9.6.2.1 IoT Issues and Limitations

The IoT's hierarchical architecture is susceptible to various attack vectors from malevolent actors. The attack vectors are primarily classified into two categories i.e. active and passive based on their operative signature. The active attack directly impacts normal behavior of node, thus being more hostile in nature. The passive attack works covertly in the background like a Trojan Virus [4]. The expounded security review of each IoT layer is discussed below:

Issues in Perception Layer

As the primary goal of "Perception or Physical layer" is to perceive and capture sensitive information from surrounding physical network, the malicious attack vectors are aimed towards node tinkering or tampering of gathered data. These sensor objects are deployed in a hostile and remote operating environment; as such remain susceptible to "Node Capturing Attacks" in which an attacker leverages physical damage and tinkering of hardware sensors [57]. If an attacker succeeds in compromising a deployed sensor node, it therefore ensue revealing sensitive information such as cryptographic keys and authentication procedures. Also, an attacker can clone a sensor node by copying information parameters in order to authenticate itself with the IoT network. A similar attack vector known as Code Injection Attack inserts malicious scripts into working software code of a sensor node, thereby altering its otherwise standard operating procedures. The malicious script permits attacker to control IoT network which further downgrades its normal working. Additionally, the attackers for trust exploitation can leverage Replay attack in which compromised sensor node transfers sensitive information to illegitimate destination [37]. Once trust is established, the attacker revamps authentication procedures employed in IoT system. To drain battery and deplete the operating power of sensor nodes, the attacker sometimes leverages Sleep

Deprivation attacks. As IoT nodes are battery powered, therefore in order to run for longer durations, they employ programmed sleep timers in order to save power utilization. The Sleep deprivation attack alters sleep timers and makes nodes work continuously even when otherwise idle. This results in power loss and device shutdown [6].

Issues at Network Layer

The IoT network layer is most susceptible to abuse as most of the collected data through sensors gets transmitted at this layer. Most of the security schemes focus on accessibility of the available resources [31]. The security measures also aim at preserving node integrity as well as authentic information data that is communicated over the deployed internetwork. Some inherent vulnerabilities are highlighted below.

"Eavesdropping and Interference": As underlying communication medium used by IoT devices is wireless, security threat lies in the fact that transmission medium could be intercepted by malicious actors. The quality of data exchanged between IoT nodes over wireless medium could be degraded by superimposing jamming signals [22]. Secure encryption and cryptographic procedures need to be put into place in order to uphold data accuracy.

"Denial of Service (DoS) attack": This is one of the commonly executed network attack directed to render computing infrastructure in a network inaccessible to its legitimate client users. In this attack, large amount of network data traffic is redirected towards the victim node which it cannot process simultaneously, resulting in shutting down or unavailability of a server or controller node. Common attacks which gobble up resources including bandwidth, storage, node memory and processing time include attack vectors such as "Ping of death", "Flooding UDP data", "ICMP Flooding" etc. Common mitigation strategies implemented for thwarting the attack include implementing robust firewall rules and gateway policies.

"Spoofing attacks": These attacks are categorized into two categories: IP spoofing and RFID spoofing. Both type of attacks target and spoof control system of IoT in order to transmit malicious scripts across network [31].

"Routing Attacks": In IoT architecture, routing function is performed at the network layer; therefore these attacks fiddle with routing policy including protocols with the main aim of creating route loops that result in increased packet drop rate. This further result in increased traffic congestion and latency in network [6].

Additionally, other attacks that are directed towards network layer include "Sink Hole attack", "Sybil Attack", "Worm Hole attack" and "Illegal node access attack".

Issues at Application Layer

As application layer provides interface for client requests, therefore most of the security issues in this layer are directed towards software routines. The IoT architecture is yet to be standardized; therefore the issues related to security at application level are supreme and demand robust solutions. Diverse applications entail varied authentication and verification procedures and to homogenize these

approaches is an arduous task. Application privacy and node authentication should be the primary design goal of security protocols. Some common application level security threats include script injections such as "SQL Injections", inept coding which provide platform to XSS vulnerability, password stealing techniques such as Fishing and many more [6].

9.6.2.2 Cloud Service Issues

The security vulnerabilities present in traditional cloud computing systems are also inherent in CloudIoT; however the integration between two heterogeneous technologies introduces complex attack vectors that are effortless to initiate [20]. As client requests computation and data storage from cloud services, it's important that data confidentiality and data privacy is preserved. The client should be well aware about storage location of their data and its access policies offered by the service

Table 9.3 Vulnerabilities in CloudIoT layers

	Attack/threat	Security issue	Potential solution
"Perception layer"	"Node capture attack"	Control the deployed sensor node by physical damage or change in its software routines	Effective physical site monitoring and detection of malicious script
	"Malicious code/ data Injection"	Inserting malevolent script into software routines of sensor node to change its working behavior	Secure code writing practices and code testing including malicious script filtering need to be developed
	"Replay attack"	Counterfeiting certification keys to gain trust of sensor device	Employing secure timestamp procedures in digital certification of keys
	"Side channel attacks/ Cryptanalysis"	From plain-text/cipher text, extract or gain illegal access to encryption keys	Secure and robust key generation and encryption procedures need to be employed
	"Signal Interference"	Superimpose noise signal or data to corrupt and interfere with wireless transmissions	Robust and efficient noise removal techniques to for repairing original signal need to be designed
	"Sleep deprivation attack"	Forcibly shutdown sensor devices by altering their programmed sleep routines in order to keep them running when not required	Exploit wind, solar and other forms of energy Secure code writing practices and code testing while designing sleep routines and procedures

(continued)

Table 9.3 (continued)

	Attack/threat	Security issue	Potential solution
"Network layer"	"Denial of service"	Directing massive traffic towards victim node to render it non-functional and non-serviceable	Designing robust firewall and packet examination routines in network routers and gateway
	"Spoofing attack"	Spoofs identity (IP or RFID spoofing) of legitimate user to gain illegal access to the system	Designing secure and robust authentication and authorization access procedures
	"Sinkhole attack"	To control data forwarding or routing, the victim node assets unusual or extraordinary power and processing capacity	Designing secure routing and data forwarding protocols and techniques
	"Man-in-the-middle"	The malevolent actor places itself between two victim nodes. Impersonates them and gains access to information without their knowledge	Designing secure and robust authentication and authorization access procedures. Also employing authentication and encryption certificates
	"Routing attacks"	This attack aims to create route loops and high congestion in the network	Designing secure routing and data forwarding protocols and techniques
"Application layer"	"Phishing attack"	To obtain authentication and authorization credentials including passwords by flooding spam mails and creating fake websites/forums	Employing robust spam filters in emails. Creating awareness among web application clients
	"Malicious-worm attack"	Infects and Injects the sensor network with Worms, Viruses and Trojans etc. Obtains or deletes confidential data	Designing robust firewall and packet examination routines for virus detection
	"Cross site scripting"	To steal privileged and validation information including passwords by injecting network applications with malevolent scripts	Secure code writing practices and code testing including malicious script filtering need to be developed

provider who manage their data. The client also demands service providers block illegitimate and unlawful access to their data. Given the on-demand cloud service model, an efficient management platform should be provided to the clients and unsanctioned and unauthorized access to this management platform needs to be

blocked. The platform if left vulnerable could contribute for further attack definitions [47]. The cloud also faces security threats to communication protocols at the network layer. As Cloud services are distributed and pervasive in nature, most of the clients access this platform using various internetworking protocols. As majority of these interworking protocols are stateless in nature, thus security threats such "Denial of Service" attack, "Man-in-the-Middle" attack, Eavesdropping are possible [20]. In addition to these, vulnerabilities also exist in how cloud interface is accessed. E.g. Mediocre authentication policies and injection attacks like "SQL injection" which directly aims at Cloud system database. Also web user interface which is accessed through a client web browser is susceptible XSS attacks. Table 9.3 lists some common CloudIoT vulnerabilities.

9.7 Related Research on Security

For a secure integration, CloudIoT paradigm requires security measures in the IoT network as well as on Cloud layer. In this regard, a substantial research with focus on meeting security goals like authentication, authentication and integrity has been carried. The section below describes the prominent security methods and state-of-art security measures that tackle distinct security issues.

A brief analysis of security and privacy issues have been discussed in [42, 51]. It has been established that data privacy and integrity are one of the prime issues with regard to IoT and Cloud. It is also important to achieve confidentiality of data which will be one of the driving factors for the success of CloudIoT integration. In [41], authors stress on addressing open issues and challenges in IoT, some of which include developing better cryptographic techniques, design of network protocols, user privacy and identity management. A similar work has been presented in [47] whereby authors discuss current state of research and challenges.

To address authentication measures, authors in [56] present an innovative mutual identity authentication technique for IoT. In their work, authors propose "Asymmetric Mutual Authentication Technique" between the platform and the sink node rooted on "Secure Hash Algorithm (SHA)", feature selection and "Elliptic Curve Cryptography (ECC)". Although; authors claim improved security with light computation and communication cost, the concept is only theoretical with no empirical evidence. Another novel technique for ID validation between the nodes in IoT is presented in [52]. The technique is a "One-Time Cipher" approach hinged on a request-reply method and applied by employing a pre shared key matrix. The authors claim its encryption and decryption process to be lightweight and use valid timestamps for communication between two parties. For large scale implementation of technique in IoT devices, the installation of pre shared matrix needs to be secured. Ensuring controlled access is the backbone for security authentication and these two features work together for securing IoT and cloud. To address these functions, authors in [34] propose the "Identity Authentication and Capability based Access Control" (IACAC) framework for IoT. The framework exhibits an

integrated technique of authentication and authorization for IoT nodes and offers protection against network based attacks. The proposed method is put to evaluation using security protocol verification tool and results obtained are quite promising.

The physical elements of IoT's perception layer are composed of sensors and RFID's. As highlighted previously, these small devices have constrained computational capacity; as such, use of complex cryptographic procedures is not feasible. To overcome this, authors in [29] propose a light weight validation technique for "RFID" tags. The technique uses encryption process based on a XOR computation instead of traditional encryption procedures. The protocol safeguards mutual authentication procedure in a classic RFID system without involving complex issues. The review of the current research and literature on CloudIoT security shows that although different solutions are available; majority of them focus on enforcing authentication, establishment of identity management, privacy and node authorization. As such, the demand for seamless software and hardware solutions to address currently open issues on CloudIoT security is mushrooming.

9.7.1 Potential Defense Strategies

It is quite obvious that amalgamation between two heterogeneous platforms i.e. Cloud and IoT will surge up security threats substantially, therefore inviolable defense strategies need to be enforced so that vulnerabilities could be averted [31]. The defense security architecture should address both the security in IoT layers as well as in the deployed cloud model. For example, to avoid illegitimate node access in IoT perception layer, node authentication should be mandatory. Also, secure encryption techniques need to be enforced to ensure data confidentiality. To achieve this, Lightweight encryption techniques and protocols like "Elliptic curve cryptography (ECC)" supplemented with effective key exchange procedures should be implemented [43]. Since Sensor nodes in IoT consume battery power, therefore energy saving procedures such as sleep routines should be implemented to increase their working life span. In addition to this, providing optimal energy generation techniques, such as channelizing renewable power sources such as solar, air and wind should be explored. To minimize physical damage to deployed sensor nodes, periodic monitoring checks and analysis should be done at the remote site. In order to avoid attacks such as "Denial of Service (DoS)", "Distributed Denial of Service (DDoS)", "Man-in-the-Middle" directed at IoT's network layer, the defense strategy would be to implement strong firewall policies and filtering rules. Also to avoid replay attacks, secure timestamp techniques need to be developed and employed. It is highly encouraged that cryptographic network protocols that ensure end-to-end encryption such as TLS/SSL and IPsec should be implemented. This would help in maintaining the integrity and authenticity of legitimate data [47]. To secure Application layer against malicious script insertion attacks such as "Cross Site Scripting (XSS)" and malicious worm attack, the defense strategy would be to practice efficient code writing and script detection techniques. This also includes

re-writing the vulnerable code for sanitization. To protect cloud data, access policies and strict authentication protocols needs to be designed and implemented. To prevent data leakage and theft, cloud data and files should be properly encrypted. Since cloud platform is distributed and pervasive in nature with multiple clients accessing its interface, a certain degree of concurrency control measures need to be implemented to avoid race conditions and data redundancy. Tracking cyber crimes directed at CloudIoT interface becomes arduous for forensic investigators as the data sources are heterogeneous and pervasive in nature. To detect and scan for any anomaly, the standard protocol would be that all operations on CloudIoT interface should be logged and stored in a secure file. The cyber forensic investigators can check this file at a later point in time so that appropriate corrective measures are taken. As Cloud and IoT represent two disparate heterogeneous platforms, providing optimal security is a challenging task for security experts and thus requires robust security protocols.

9.8 Platforms and Services

This section discusses about various available commercial as well as open source platforms that underpin and support CloudIoT vision and applications. The platforms discussed in this section are selected according to their suitability in distinct application domains and information about them has been obtained from the platform website as well as from surveying the available literature.

9.8.1 Available Platforms

According to www.ionos.com, more than 50 CloudIoT platforms are available that cater diverse users including applications varying from healthcare, agriculture, engineering, manufacturing and transportation. However, due to knowledge deficit about these platforms, users are unable to choose and exploit their full potential [10]. Most of these platforms focus on minimizing heterogeneity between the Cloud and IoT by implementing a middleware between the two for processing and hoarding sensor data and also by dispensing an API towards applications [2].The driving factors for the development of CloudIoT platforms include the need for facilitating machine-to-machine (M2M) communication which has seen an exponential rise in current times. Machina Research [3] forecasts that machine-to-machine (M2M) connections are anticipated to rise from one billion in 2010 to nearly 12 billion in 2020. Given such an unprecedented rise, cross platform operation and reuse is starting to evolve [54]. Some of the existing platforms including services are discussed below.

KAA Project (https://www.kaaproject.org/) is a flexible open source IoT middleware interface for designing robust and smart IoT solutions. It enables data

exchange between connected things including data analytics and visualization services. It dispenses back end operations for IoT by employing SDK's that come pre-fabricated with current data processing solutions which include Hadoop, mongoDB and others. Complete implementations already exist for platforms such as IoS, Android and Raspberry Pi.

Sensor Cloud (https://www.sensorcloud.com/) is a private IoT cloud platform dispensing platform as a service for data acquisition, visualization, monitoring and analytics. Sensor cloud is a robust tool supporting easy data upload using open data API and csv uploader. It receives data from Lord Microstrain's wireless and wired sensors and provides efficient data encryption and security. The platform also provides efficient data visualization and mathematical tools including reminder alerts for data threshold values.

Etherios (https://www.etherios.com) is a pliable public cloud platform based on platform as a service model supporting device management, application messaging and data storage. In addition to data visualization tools, the platform also provides API's for time series data storage and analytics. It also provides real time monitoring and management control of all connected devices using a single door interface.

Exosite (https://www.exosite.com/) is cloud based software as a service platform dispensing machine-to-machine connectivity and offering real time data monitoring and analytics service to the users. The platform supports various development kits for designing IoT based solutions. e.g. Arduino, Microchip, Renesas boards are well supported on Exosite platform. The system also provides open API for further data processing and interoperability with enterprise based applications.

Arkessa (https://www.arkessa.com) facilitates management, monitoring and control of remote devices using desktop computers and smart phones. The platform provides mobile internet as well as data services for system integrators and enterprise users to command and operate remote devices and systems for users across geographical lines and applications. Arkessa follows Platform as a Service model to serve security, healthcare, energy and transportation industries across Europe and America. This platform also provides Emport portal for viewing and monitoring machine-to-machine (M2M) connections with inbuilt assistance for troubleshooting and performance measurement analysis.

Axeda (http://www.axeda.com/) is a cloud based middleware for management of connected things and machine-to-machine (M2M) applications. The platform offers Axeda machine cloud to convert machine data into precious knowledge, develop and run machine-to-machine (M2M) including IoT applications and thus optimize varied business processes by machine data integration. API's such as REST and SOAP further drive Axeda to initiate cloud to cloud communication using cellular as well as satellite medium. Tracking of assets, management including push notifications and alerts are some its proficient features.

Nimbits (http://www.nimbits.com/) offers "Platform as a Service" model to design software as well as hardware solutions that effortlessly integrate with the cloud and with each other. Nimbits server offers "REST Web Services" for data logging and access and also rule engine platform for ensuring machine-to-machine

(M2M) connectivity. The server is driven by robust cloud platforms which include "Google App Engine" to the small Raspberry Pi device. It's capable of recording incoming data including value calculation based on which events like an alert or a push message could be triggered. The new values calculated based on the captured data can be archived to other channel triggering more cascading computations and alerts.

ThingWorx (http://www.thingworx.com/) provides an absolute end-to-end technology platform designed for enterprise IoT and offers quick and seamless development including deployment of smart objects. The platform provides integrated development tools that drive communication, connectivity, analysis, developing applications and monitoring characteristics of IoT framework. These tools contain the "Composer", the "Mashup Builder", "Storage" and a "Search Engine". Its search engine also called as "SQUEAL (Search, Query, and Analysis)" is employed for analyzing, searching and filtering data. The tools also facilitate rapid business development and empowerment.

9.8.2 Available Services

In addition to above discussed platforms, number of services are available that facilitate data collection from connected things and archiving this data on the service providers cloud. These services typically present an API for data collection and sample applications to operate on such data. Xively (https://www.xively.com/) is one such platform owned by Google which offers product enterprises to connect and manage products including data and incorporate that data in other systems. Xively is based on Platform as a Service model and includes directory as well as data services, a trust service for security and web user interface. Its messaging system is based on MQTT which is publish-subscribe protocol. REST, MQTT and WebSockets are supported by the API.

ThingSpeak (https://www.thingspeak.com/) is yet another platform with features very much similar to Xively and based on public cloud technology. ThingSpeak provides real time data collection and transmits data privately to the cloud. This data could be examined and inspected using various toolkits (e.g. Matlab, Arduino) and a reaction could be triggered based on certain events. Using ThingSpeak, a user can create a sensor-logging app, track live location of objects and establish a novel social network of things. The platform API also allows mathematical processing on data such as calculating average, median, summation and rounding.

Table 9.4 provides summarized view of some of the existing platforms/services including their advantages and limitations.

Table 9.4 Summary of existing platforms

	Platform/ service	URL	Advantages	Limitation
1	KAA project	www.kaaproject.org	• Applications using Bigdata and NoSQL are supported • Open Source Middleware	• Low number of Hardware modules supported
2	Sensor cloud	www.sensorcloud.com	• Efficient Management of large number of sensor devices	• Private cloud • Issues with open source devices
3	Etherios	www.etherios.com	• Cloud service for devices including third party software are enabled • Trail usage period provided	• Restrictions imposed on developers by some devices
4	Exosite	www.exosite.com	• Easy system development • Supports Arduino, Microchip, Renesas boards	• Big Data support lacking
5	Arkessa	www.arkessa.com	• Suitable for enterprises	• Doesn't have good visualization tools
6	Axeda	www.axeda.com	• Robust M2M data management • Supports REST and SOAP API	• Hinges on third party web services
7	Nimbits	www.nimbits.com	• Easy platform for developers • Supports REST API and Google app engine	• Query processing occurs in real time
8	ThingWorx	www.thingworx.com	• Supports design of data intensive apps • Offers SQUEAL for Search, Query, and Analysis	• Supports limited number of devices
9	Xively	www.xively.com	• Direct support from Google • Easy integration with devices using RESTful API's	• Lacks/less support for notifications
10	ThingSpeak	www.thingspeak.com	• Public cloud access • API's for storing and analyzing data • Mathematical operations supported	• Less support for simultaneous connection for devices

9.9 Integration Challenges and Open Issues

It is quite evident that amalgamation of Cloud and IoT will add tangible benefits in our daily life; however the integration also lays genesis to some perilous issues that demand robust solutions and need to be overlooked by security researchers [16].

Security and Privacy

As Cloud and IoT are distributed and pervasive in nature, ameliorating underlying Security and Privacy infrastructure play a major role in its successful integration.

To ensure authenticity, data Integrity and data availability, optimal measure need to be designed so that critical data in cloud is preserved [14]. Failure to safeguard these security principles could lead to data pilferage or exploitation of personal data. The issue becomes more complicated if data gets exposed to third party vendors which could propagate it further for illegitimate activities. Thus; efficient security framework needs to be developed for heterogeneous device communication between IoT nodes as well as for protecting privacy on Cloud platform.

Protocol support and Need for Standards

As no standard architecture for IoT is yet available, disparate protocols need to communicate and transact information with each other. Even if homogeneous sensor nodes are deployed in the network, the underlying communication protocols are still heterogeneous in nature which includes 6LOWPAN, CoAP, Zigbee, IEEE 802.15.4 etc. There is also possibility that data aggregation gateway would not support all of these protocols leading to incompatibility issues. The problem becomes more severe once these devices are integrated with the cloud platform. Thus, scientific community needs to develop standardized protocols and scalable platforms so that seamless integration of CloudIoT services is achieved.

Efficient Power Usage

The ubiquitous communication between Cloud and IoT generates prodigious amount of data that drains battery of power constrained sensor nodes. The problem becomes more severe if visual data (e.g. surveillance video) is involved. As sensor nodes are battery powered, periodic and frequent replacement with silicon batteries is not feasible. The solution could be to exploit alternate forms of energy generation models such as wind and solar power [18]. Another efficient technique would be to program periodic sleep routines for the sensor nodes. The devices could go in a sleep mode if no observable perception action occurs during a fixed time frame.

Delay and Limited Bandwidth

The distributed platform such as Cloud presents limitless computing resources and varied services, however utilizing these services with minimum latency and delay is not guaranteed. One of the prime components in achieving optimal performance is ensuring high bandwidth for data transmission. To minimize delay, a middleware layer known as “Fog Computing” is to be placed between Cloud and IoT. The “Fog computing” will achieve low latency for applications that are sensitive to delay. [8, 14].

Quality of Service (QoS)

The “Quality of Service (QoS)” is the dominant parameter in governing aggregate performance of the internetwork. Given the large volume of data that is being produced and interchanged in CloudIoT, maintaining QoS in services provided by the platform is of supreme importance. Also, considerable number of client requests demand efficient management by the Cloud platform some which may be sensitive to delay. Thus, to avoid packet loss, employing QoS improvement techniques and

prioritizing data packets seem to be a flawless solution. Thus utilizing next generation IP protocol (IPv6) which offers tangible features for ensuring QoS in the network is optimal choice for CloudIoT environment.

9.10 Discussion and Conclusion

The evolution and growing popularity of Cloud and IoT has become the prime factor for enabling seamless applications influencing our everyday life. Amalgamation of Cloud and IoT is highly motivated by requirement for efficient computing infrastructures, limitless warehouse for data logging, optimal network performance and availability. Also, "Cloud" provides an efficient platform and solution to overcome several inherent issues (heterogeneity and resource constraints) faced by IoT systems. Majority of available research papers have surveyed Cloud and IoT separately, focusing on architecture, underlying technology and affairs, however shortfall from detailed examination and in-depth exploration. To fill this research gap, this chapter carried a deep and profound review of the available research papers and presented a holistic vision on the CloudIoT integration components. The chapter presented seamless applications dispensed by CloudIoT platform and contemplated discussion on factors driving CloudIoT integration. The work in this chapter also highlighted security issues affecting IoT layered architecture including vulnerabilities inherent in the Cloud. Also a brief discussion on some potential mitigation measures has been provided. A summarized discussion on CloudIoT platforms is also presented that aim at solving heterogeneity issue between the Cloud and things. Finally, the chapter concludes by identifying some open research issues and challenges hampering Cloud and IoT integration. From the reviewed literature, it is quite apparent that additional research steps need to be taken to accomplish flawless and impeccable convergence of Cloud and IoT. More work needs to be done on designing secure algorithms and encryption procedures so that only legitimate devices and nodes are authorized to access the sensitive data in IoT network and Cloud. Also data privacy in CloudIoT systems needs to be augmented so that integrity of the system is maintained. As sensor nodes have constrained power backup, the designed encryption protocols should be computationally light and consume minimal power. To conserve energy, the solution could be to exploit alternate forms of energy generation models. Another efficient technique would be to program periodic sleep routines for the sensor nodes. The devices could go in a sleep mode if no observable sensing activity occurs in a given time frame. For applications that are sensitive to delay, decentralizing Cloud operations also called "Fog Computing" would ensure minimal latency and low transmission delays between Cloud and IoT. Also to assure that QoS in data transmission is preserved, employing IPv6 characteristic attributes like Traffic class and Flow label are highly recommended.

References

1. Aazam, M., Huh, E.N.: Fog computing and smart gateway based communication for cloud of things. In: International Conference on Future Internet of Things and Cloud (FiCloud), pp. 464–470. IEEE, 2014 Aug
2. Aazam, M., Huh, E.N., St-Hilaire, M., Lung, C.H., Lambadaris, I.: Cloud of things: integration of IoT with cloud computing. In: Robots and Sensor Clouds, pp. 77–94. Springer, Cham (2016)
3. Aazam, M., Hung, P.P., Huh, E.N.: Smart gateway based communication for cloud of things. In: 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), pp. 1–6. IEEE, April 2014
4. Abomhara, M., Køien, G.M.: Security and privacy in the internet of things: current status and open issues. In: 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), pp. 1–8. IEEE, May 2014
5. Aguzzi, S., Bradshaw, D., Canning, M., Cansfield, M., Carter, P., Cattaneo, G., Stevens, R.: Definition of a research and innovation policy leveraging cloud computing and IoT combination. Final report, European Commission, SMART, 37 (2013)
6. Andrea, I., Chrysostomou, C., Hadjichristofi, G.: Internet of things: security vulnerabilities and challenges. In: IEEE Symposium on Computers and Communication (ISCC), pp. 180–187. IEEE, July 2015
7. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Zaharia, M.: Above the clouds: a berkeley view of cloud computing, vol. 4, pp. 506–522. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley (2009)
8. Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, pp. 13–16. ACM, Aug 2012
9. Botta, A., De Donato, W., Persico, V., Pescapé, A.: On the integration of cloud computing and internet of things. In: 2014 International Conference on Future Internet of Things and Cloud (FiCloud), pp. 23–30. IEEE, Aug 2014
10. Botta, A., De Donato, W., Persico, V., Pescapé, A.: Integration of cloud computing and internet of things: a survey. Future Gener. Comput. Syst. **56**, 684–700 (2016)
11. Buyya, R., Ranjan, R., Calheiros, R.N.: Intercloud: utility-oriented federation of cloud computing environments for scaling of application services. In: International Conference on Algorithms and Architectures for Parallel Processing, pp. 13–31. Springer, Berlin, May 2010
12. Capkun, S., Buttyán, L., Hubaux, J.P.: Self-organized public-key management for mobile ad hoc networks. IEEE Trans. Mob. Comput. **2**(1), 52–64 (2003)
13. Chen, S., Xu, H., Liu, D., Hu, B., Wang, H.: A vision of IoT: applications, challenges, and opportunities with china perspective. IEEE Internet Things J. **1**(4), 349–359 (2014)
14. Cook, A., Robinson, M., Ferrag, M.A., Maglaras, L.A., He, Y., Jones, K., Janicke, H.: Internet of cloud: security and privacy issues. In: Cloud Computing for Optimization: Foundations, Applications, and Challenges, pp. 271–301. Springer, Cham (2018)
15. Devipriya, S.: Contribution of internet of things: a survey. J. Web Develop. Web Design. **1**(1–3) (2017)
16. Díaz, M., Martín, C., Rubio, B.: State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. J. Netw. Comput. Appl. **67**, 99–117 (2016)
17. Distefano, S., Merlino, G., Puliafito, A.: Enabling the cloud of things. In: 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 858–863. IEEE, July 2012
18. Evans, D.: The internet of things: how the next evolution of the internet is changing everything. CISCO White Paper **1**(2011), 1–11 (2011)
19. Fox, G.C., Kamburugamuve, S., Hartman, R.D.: Architecture and measured characteristics of a cloud based internet of things. In: 2012 International Conference on Collaboration Technologies and Systems (CTS), pp. 6–12. IEEE, May 2012

20. Grobauer, B., Walloschek, T., Stocker, E.: Understanding cloud computing vulnerabilities. IEEE Secur. Priv. **9**(2), 50–57 (2011)
21. Grozev, N., Buyya, R.: Inter-cloud architectures and application brokering: taxonomy and survey. Software Practice Exper. **44**(3), 369–390
22. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
23. Hassan, M.M., Song, B., Huh, E.N.: A framework of sensor-cloud integration opportunities and challenges. In: Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, pp. 618–626. ACM, Feb 2009
24. Jeffery, K.: Keynote: CLOUDs: a large virtualisation of small things. In: The 2nd International Conference on Future Internet of Things and Cloud (FiCloud-2014) (2014)
25. Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D.: Security of the internet of things: perspectives and challenges. Wirel. Netw. **20**(8), 2481–2501 (2014)
26. Khodkari, H., Maghrebi, S.G., Branch, R.: Necessity of the integration Internet of Things and cloud services with quality of service assurance approach. Bulletin de la Société Royale des Sciences de Liège **85**(1), 434–445 (2016)
27. Khorshed, M.T., Ali, A.S., Wasimi, S.A.: A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener. Comput. Syst. **28**(6), 833–851 (2012)
28. Kovatsch, M., Mayer, S., Ostermaier, B.: Moving application logic from the firmware to the cloud: towards the thin server architecture for the internet of things. In: 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 751–756. IEEE, July 2012
29. Lee, J.Y., Lin, W.C., Huang, Y.H.: A lightweight authentication protocol for internet of things. In: 2014 International Symposium on Next-Generation Electronics (ISNE), pp. 1–2. IEEE, May 2014
30. Lee, K., Murray, D., Hughes, D., Joosen, W.: Extending sensor networks into the cloud using amazon web services. In: 2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications (NESEA), pp. 1–7. IEEE, Nov 2010
31. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. **4**(5), 1125–1142 (2017)
32. Liu, W., Zhao, X., Xiao, J., Wu, Y.: Automatic vehicle classification instrument based on multiple sensor information fusion. In: Third International Conference on Information Technology and Applications (ICITA 2005), vol. 1, pp. 379–382. IEEE, July 2005
33. Machine-to-Machine connections to hit 12 billion in 2020, generating EUR714 billion revenue. https://machinaresearch.com/static/media/uploads/machina_research_press_release_m2m_global_forecast_analysis_2010_20.pdf
34. Mahalle, P.N., Anggorojati, B., Prasad, N.R., Prasad, R.: Identity authentication and capability based access control (iacac) for the internet of things. J. Cyber Secur. Mobility **1**(4), 309–348 (2013)
35. Meingast, M., King, J., Mulligan, D.K.: Embedded RFID and everyday things: a case study of the security and privacy risks of the US e-passport. In: IEEE International Conference on RFID 2007, pp. 7–14. IEEE, Mar 2007
36. Mell, P., Grance, T.: The NIST definition of cloud computing (2011)
37. Mo, Y., Sinopoli, B.: Secure control against replay attacks. In: 47th Annual Allerton Conference on Communication, Control, and Computing. Allerton 2009, pp. 911–918. IEEE, Sept 2009
38. Nordrum, A.: Popular internet of things forecast of 50 billion devices by 2020 is outdated. IEEE Spectrum **18** (2016)
39. Parwekar, P.: From internet of things towards cloud of things. In: 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp. 329–333. IEEE, Sept 2011

40. Rao, B.P., Saluia, P., Sharma, N., Mittal, A., Sharma, S.V.: Cloud computing for Internet of things & sensing based applications. In: 2012 Sixth International Conference on Sensing Technology (ICST), pp. 374–380. IEEE, Dec 2012
41. Roman, R., Najera, P., Lopez, J.: Securing the internet of things. Computer **44**(9), 51–58 (2011)
42. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. **57**(10), 2266–2279 (2013)
43. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in internet of things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
44. Soldatos, J., Kefalakis, N., Hauswirth, M., Serrano, M., Calbimonte, J. P., Riahi, M., Aberer, K., Jayaraman, P.P., Zaslavsky, A., Žarko, I.P., Herzog, R.: Openiot: Open source internet-of-things in the cloud. In: Interoperability and Open-Source Solutions for the Internet of Things, pp. 13–25. Springer, Cham (2015)
45. Soliman, M., Abiodun, T., Hamouda, T., Zhou, J., Lung, C.H.: Smart home: integrating internet of things with web services and cloud computing. In: 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), vol. 2, pp. 317–320. IEEE, Dec 2013
46. Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G., Suciu, V.: Smart cities built on resilient cloud computing and secure internet of things. In: 2013 19th International Conference on Control Systems and Computer Science (CSCS), pp. 513–518. IEEE, May 2013
47. Suo, H., Wan, J., Zou, C., Liu, J.: Security in the internet of things: a review. In: 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 3, pp. 648–651. IEEE, Mar 2012
48. Thepparat, T., Harnprasarnkit, A., Thippayawong, D., Boonjing, V., Chanvarasuth, P.: A virtualization approach to auto-scaling problem. In: 2011 Eighth International Conference on Information Technology: New Generations (ITNG), pp. 169–173. IEEE, April 2011
49. Velte, A.T., Velte, T.J., Elsenpeter, R.C., Elsenpeter, R.C.: Cloud Computing: A Practical Approach, p. 44. McGraw-Hill, New York (2010)
50. Villegas, D., Bobroff, N., Rodero, I., Delgado, J., Liu, Y., Devarakonda, A., Fong, L., Masoud Sadjadi, S., Parashar, M.: Cloud federation in a layered service model. J. Comput. Syst. Sci. **78**(5), 1330–1344 (2012)
51. Weber, R.H.: Internet of things-new security and privacy challenges. Comput. Law Secur. Rev. **26**(1), 23–30 (2010)
52. Wen, Q., Dong, X., Zhang, R.: Application of dynamic variable cipher security certificate in internet of things. In: 2012 IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS), vol. 3, pp. 1062–1066. IEEE, Oct 2012
53. Wu, M., Lu, T.J., Ling, F.Y., Sun, J., Du, H.Y.: Research on the architecture of Internet of things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol. 5, p. V5-484. IEEE, Aug 2010
54. Yuriyama, M., Kushida, T.: Sensor-cloud infrastructure-physical sensor management with virtualized sensors on cloud computing. In: 2010 13th International Conference on Network-Based Information Systems (NBiS), pp. 1–8. IEEE, Sept 2010
55. Zaslavsky, A., Perera, C., Georgakopoulos, D.: Sensing as a service and big data (2013). arXiv preprint arXiv:1301.0159
56. Zhao, G., Si, X., Wang, J., Long, X., Hu, T.: A novel mutual authentication scheme for internet of things. In: Proceedings of 2011 International Conference on Modelling, Identification and Control (ICMIC), pp. 563–566. IEEE, June 2011
57. Zhao, K., Ge, L.: A survey on the internet of things security. In: 2013 9th International Conference onComputational Intelligence and Security (CIS), pp. 663–667. IEEE, Dec 2013
58. Zhou, J., Leppanen, T., Harjula, E., Ylianttila, M., Ojala, T., Yu, C., Yang, L.T.: Cloudthings: A common architecture for integrating the internet of things with cloud computing. In: IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 651–657. IEEE, June 2013

59. Zhu, W., Luo, C., Wang, J., Li, S.: Multimedia cloud computing. IEEE Signal Process. Mag. **28**(3), 59–69 (2011)
60. Zikopoulos, P., Eaton, C.: Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data. McGraw-Hill Osborne Media, New York
61. Zorzi, M., Gluhak, A., Lange, S., Bassi, A.: From today's intranet of things to a future internet of things: a wireless-and mobility-related view. IEEE Wirel. Commun. **17**(6) (2010)

Part III
IoT in Healthcare Paradigm

Chapter 10
Application of IoT in Healthcare

Pranati Rakshit, Ira Nath and Souvik Pal

Abstract The IoT has broad application in the field of medical care as well as health care. It has potential to provide ascend to numerous medical services and applications like remote or distant health monitoring, information tracking, improved drug usage, device, emergency care, healthcare charting etc. The IoT has a variety of application area which includes health care. The modern health care is becoming sophisticated and redesigned by the IoT revolution. Promising technological, economic, and social prospects promote the revolution in IoT. The IoT is likely to enable a range of healthcare solutions. In the context of healthcare, service and application cannot be differentiated objectively and both are interdependent. So, both IoT services and IoT applications ought to have closer attention. This chapter addresses various healthcare applications which are IoT-based, along with some healthcare technologies. Many promising and enabling technologies are nowadays working for IoT-based healthcare solutions, and thus it is important to put some lights on those technologies. In this respect, the following analysis focuses on some core technologies which have the prospective to revolutionize IoT enabled healthcare services.

Keywords Remote health monitoring · Information tracking · Improved drug usage · Device · Emergency care · Healthcare charting

10.1 Introduction

With the advent of modern mobile devices and increase in different feature in the mobile technology remote health caring is becoming easier nowadays. People at home can communicate with doctor or any concerned person of nursing home or

P. Rakshit (✉) · I. Nath
CSE Department, JIS College of Engineering, Kalyani, Nadia, West Bengal, India
e-mail: pranati.rakshit@jiscollege.ac.in

S. Pal
CSE Department, Brainware University, Barasat, Kolkata, West Bengal, India

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_10

hospital very easily with the help of IoT (Internet of Things) and mobile technologies. These technologies make it simple to control the sick's fitness situation by exchanging the data of health to physicians, nurses and specialists. If any guardian or patient party is busy with other job and cannot go to the nursing home or hospital to get the information of the patient, then he also gets the patient's information remotely.

As nowadays sensor has been made as miniaturized, it can be used in many areas which can improve the quality of human life. So, it can be easily used in places which are related to health care. Basically, for a developing country the heath care services cost seems to be expensive sometimes. Extra money is also needed to take the information about the patients by the relatives. The knowledge of IoT have been rapidly utilized to interrelate the existing medical resources and supply smart, dependable, and actual healthcare facilities to the sick persons. IoT based health controlling systems can be advantageous to improve the patient's lifestyle.

The IoT based health monitoring systems generally gather the information for sensor data through Arduino microcontroller and transmit it to the cloud where it is developed and evaluated for distant sighting. Feedback achievements depended on the scrutinized information can be directed to the physicians or custodian through Email and/or alerts through SMS in the situation of any crises.

10.2 IoT in Healthcare—Benefits and Challenges

The healthcare industry is in a situation of immense desolation. Healthcare facilities are expensive and the numbers of chronic diseases are growing day by day. In this situation the initial healthcare will not be reachable to most of the people of the society and will be suffered from chronic diseases for a long duration. So, the only solution of the above-mentioned problem is the construction and growth of IoT app. The technology can not prevent the inhabitants from becoming old enough or eliminate chronic diseases instantly. But the availability of healthcare remedies will be in our pocket always.

Medical diagnosis requires a huge amount of money to pay for the hospital. Technology can transfer the practices of regular medical diagnosis from a hospital (hospital-oriented) to the patient's home (home-oriented). The actual analysis will diminish the necessity of taken admission at hospital frequently.

An innovative and current technology which is familiar as the IoT has a widespread application in various expanses, with healthcare. The whole utilization of this technology in healthcare zone is a joint expectation as it permits medical centers to work more proficiently on sick persons to get treatment satisfactorily.

With the utilization of this technology-oriented healthcare technique, there are unequal advantages which could progress the grade and effectiveness of medical care and accordingly upgrade the physical fitness of the victims.

10.2.1 Benefits

(a) **Simultaneous reporting and monitoring**

Actual controlling through attached resources can save lives at the time of a medical emergency like heart failure, diabetes, asthma attacks, etc. A smart medical resources attached to a smart phone app is always ready to control any arising situation. The attached resources can gather medical and additional necessary health information connected to the smart phone to deliver gathered data to a doctor.

Midpoint of Associated Health Strategies survey to focus that a 50% discount is there in 30-day readmission charge for distant sick person suffering from heart failure.

The IoT resources gather and transmit health data: blood pressure, oxygen and blood sugar levels, weight, and ECGs. These huge amount of data are accumulated in the cloud and can be exchanged with a third party, who might be a doctor, your insurance company, a participating health firm or an external physician, to permit them to see at the gathered information without considering their location, time, or resources.

(b) **End-to-end connectivity and affordability**

IoT can systematize treatment of sick person with the support of healthcare flexibility result and other innovative technologies, and healthcare services for new generations. IoT allows exchange of data, machine-to-machine transmission, sharing of data, and motion of information that creates healthcare facility operative.

Connectivity protocols: Bluetooth LE, Wi-Fi, Z-wave, Zig-Bee, and other recent protocols, healthcare employees can alter the way they identify diseases in sick persons and can also invent innovative ways for treatment and caring.

Subsequently, technology-driven setup reduces the expenditure by lessening the needless appointments, utilizing improved class devices and increasing the allotment and lessens the expenditure, by reducing needless appointments, using improved class devices, and enhancing the allotment and scheduling.

(c) **Data assortment and analysis**

A huge quantity of information that a healthcare machine transmits during a small interval for actual implementation, is complex to keep and control, if the entree to cloud is inaccessible. Even for healthcare transmitters to accumulate information generating from more than one resource and evaluate it physically is a complicated task.

IoT resources can gather reports and evaluate the information at present and reduce the necessity to gather the original information. These all can occur through cloud with the supplier only achieving entree to ultimate descriptions with diagrams and charts.

Moreover, IoT healthcare activities permit private and govt. sectors to achieve indispensable healthcare methodical and information-oriented visions which speeds up taking decisions and is fewer susceptible to faults.

(d) **Tracking and alerts**

On-time warning is crucial in the occasion of life-fatal situations. IoT permits resources to accumulate vigorous data and transmit that data to physicians for actual follow up instantly, while reducing announcements to mankind about crucial areas via mobile apps and other attached resources.

Statements and warnings provide a bold decision about a situation of a sick person without thinking about place and time. It also assists to create an experienced opinion and provide proper treatment and caring instantly.

So, IoT empowers actual warning, tracking, and controlling, which allows real caring, better correctness, involvement by physicians and improve entire caring and treatment of sick persons for providing positive outcomes.

(e) **Remote medical assistance**

In the occasion of an emergency condition, sick persons can communicate with a physician who is located far away with a smart mobile app. The doctors can instantly examine the sick persons and recognize the illnesses immediately for further treatment with motion resolutions in healthcare.

Also, various healthcare distributions combine those which are predicting to construct devices that can allot medicines based upon the sufferer's prescription and the information depends upon the diseases exist via linked machines.

IoT will be more efficient in the field of the sick person's care in hospital. This will reduce the expenditure of the mankind during the treatment.

10.2.2 Challenges

(a) **Data safety and confidentiality**

The information related with safety and confidentiality is one of the most important issue that IoT has. IoT resources seize and communicate information in actual-time. However, most of the IoT resources have deficiency of information protocols and standards.

Furthermore, there is an important uncertainty regarding information possession and guideline. All these issues create the information extremely vulnerable to hackers who can cope with the organization and negotiation for Personal Health Information (PHI) of both sick persons and physicians.

Hackers can abuse victim's information to generate false IDs to purchase medicines and clinical apparatus which they can retail in future. Cybercriminals can also submit for a fake Insurance claim in sick person's name.

(b) **Integration: multiple devices and protocols**

Accumulation of various resources creates disruption in the execution of IoT in the healthcare field. The purpose for this burden is that reproducer of resources hasn't achieved an agreement considering transmission protocols and standard.

So, even if the dissimilarity of resources is linked; the alteration in their transmission protocol confuses and delays the method of information accumulation. This non-uniformity of the attached resource's protocols reduces the entire method and diminishes the possibility of adaptability of IoT in healthcare.

(c) **Data overload and accuracy**

Accumulation of information is problematic for the utilization of various transmission protocols and standards. However, IoT resources keep a huge amount of information. The information gathered by IoT resources are used to achieve vigorous visions.

However, the ton of information is so marvelous that analyzing visions from it are appearing tremendously problematic for physicians which, finally influences upon the superiority of creating determination. Moreover, this anxiety is growing as more resources are attached which accumulate a huge amount of information.

(d) **Cost**

IoT has not created the healthcare facilities inexpensive to the ordinary mankind so far. The thriving in the Healthcare expenditures is a symbol of anxiety for everyone particularly the progressed territories.

The condition is such that it provides growth to "Medical Tourism" in which sick persons with crucial situations acquire healthcare services of the progressing countries which reduces prices. IoT in healthcare as an idea is an engrossing and pledging concept.

However, it hasn't resolved the expenditure problems as of now. To fruitful accomplishment of optimized IoT, the stakeholders must create its expenditure effective, otherwise it will be inaccessible to everybody excluding the rich people.

10.3 Different Application Areas of IoT in Healthcare

10.3.1 Dropping Emergency Room Waiting Time

Waiting in the emergency room is one of the boring things in the healthcare system. Apart from the different medical demands and expenditure, big amount of time are wasted for emergency room visits. With the help of IoT some hospital or medical organization reduces this waiting time. One example which can be shared is that 50% of waiting time of patients who needs urgent care in emergency room is slashed down at Mt. Sinai Medical Center in New York City. It's made possible with their partnership with GE Healthcare and one IoT-driven software, which is known as AutoBed that tracks occupancy among 1200 units and factors in 15 different metrics to assess the needs of individual patients.

It's a highly efficient system that highlights the more inventive and electrifying uses of the IoT.

10.3.2 Telehealth

With the advent of telehealth or remote health monitoring system, sometimes patients don't have to go to an emergency room or even hospital. It minimizes costs and eliminates the visitation expenditure. By discarding the travel which is sometimes very inconvenient, it helps the patients to improve their living quality.

If mobility is the limitation for a patient or he is dependent on public transport, simply telehealth can make a lot of difference.

10.3.3 Ensuring the Risk Management of Critical Hardware

As our society is moving very fast with new technologies, modern hospitals need different software and hardware which are capable to perform with next generation's demands. Some of these IOT driven solution even helped to save or prolong human life. Like all electronic devices, this equipment is also prone to frequent risks—from power outages to system failures—that could be a matter of life or death. But different IoT driven solution are being invented to solve this type of problem. For example, Philips has designed a solution, called e-Alert which aims to solve that problem.

Instead of waiting for a device to fail, Philips' new system takes a proactive approach by virtually monitoring medical hardware and alerting hospital staff members if there's a problem.

10.3.4 Information Tracking

Safety and security are the extreme concern of each healthcare organization—or at least it should be. So it's very important to track assets—staff members, patients and hardware—throughout the building or campus. It is very hard to maintain the maximum amount of security without the ability to track the resource.

In smaller organization this task can be easily achieved. But if there are multiple structures and campuses with large number of patients as well as staff members then it is a matter of concern.

For asset tracking many organizations are moving towards the IoT based and real-time location systems. It is a cutting-edge technology which is very effective and inexpensive.

10.3.5 Improved Drug Usage

One of the most exciting breakthroughs regarding healthcare and IoT comes in new forms of prescription for medication.

It uses pills which contains microscopic sensors that are of the size of a grain of rice, can send a signal to an external device, usually a patch worn on the body, to ensure proper dosage and usage.

10.3.6 Devices

Devices are not beyond the good fortune of IoT. They normally offer fewer benefits and qualities that an IoT system offers. But current devices are improving in their power, precision, and availability. IoT has a great potential to unlock existing technology, and lead us towards better healthcare and medical device solutions.

10.3.6.1 Hearables

New-age hearing aids are called hearables with which people who suffered from audible range loss can interact with the world in a better way than before. It has completely transformed the interaction methods. Nowadays, hearables are compatible with Bluetooth which syncs your smart phone with it. Real-world sounds can be filtered, equalized and added with layered features.

10.3.6.2 Ingestible Sensors

These sensors are also a fortunate thing for a diabetic patient as it would help in curbing symptoms and provide with an early warning for diseases. Proteus Digital Health is one such example.

10.3.6.3 Moodables

Moodables are most interesting devices which can enhance our mood. This mood enhancing devices can help in improving our mood throughout the day. It may sound like science fiction, but it's not far from reality.

10.3.6.4 Drones

Computer vision technology along with AI has given rise to drone technology which aims to mimic visual perception and hence decision making based on it.

Drones like Skydio use computer vision technology to detect obstacles and to navigate around them. This technology can also be used for visually impaired people to navigate efficiently.

10.3.7 Healthcare Charting

Patient charting is one of the important works of doctor which takes a lot of time. IoT devices can reduce this charting time by discarding manual work which a doctor has to do. It is powered by voice commands and captures the patient's data. It makes the patient's data readily accessible for review. It saves around 15 h per week of doctor's job. One such a device is Audemix.

10.3.8 Emergency Care

Limited resources are one of the reasons for having problem in the emergency support services. Sometimes, this is also disconnected from the base facility. The advanced automation and analytics of IoT cater to this problem in the healthcare sector. From a far distance places or rather miles away an emergent situation in healthcare can be analyzed. The service providers get hold of access to the patient's profiles way before their arrival and that is the reason they can deliver indispensable care to the patients on right time. In this way, associated losses are reduced, and emergency health care is improved.

10.4 Related Technologies

10.4.1 Role of IoT and Cloud in Healthcare

Internet of Things is the set of resources that are attached to the internet to accomplish the service that help our initial necessities, finances, fitness and atmosphere [1–4]. Cloud computing is an epitome, in which dynamical, accessible and virtualized supplies are provided as assistances via internet. Cloud computing in addition with the IoT will improve the ability to perform well and capacity to store highest resources. So, cloud computing is utilized as a forward-facing terminal to entree IoT. The healthcare industry is growing quickly which enables mankind to reside better living by utilizing associated and linked resources such as tablets, wearables and hand-held resources. IoT is a fast-growing skill that bonds the interoperation among various provocations to totally alteration of the technique in which healthcare will be transmitted, providing better results, improving effectiveness and creating healthcare inexpensive. IoT provides mankind essential and fundamental technology to supply improved outcomes. The healthcare industry is rapidly growing in the direction of cheap, reachable and standard health services. All private and govt. sectors are endeavoring scarcely to construct transmission affinity among the wide range of devices that have handled separately. IoT and adopt IoT driven methods have the capability to model this type of healthcare,

which depends upon active involvement of sick persons. This will thereafter enhance the healthcare which is being supplied. IoT is here to reside, and will endure to grow quick, conducting to effective and improved alterations for all stakeholders in the area of healthcare. The innovative ideas of the IoT are rapidly finding out its path to solve problems in our present life, pointing out to improve the excellence of livings by attaching with various smart devices, technologies, and resources. Moreover, the IoT would permit for the computerization of the whole surrounding with us. Presently scientists have searched out that there is a possible implementation of IoT to the healthcare trade. We can use a prototype that operates upon the difficulties of sick persons using essential gathering of collected information by facilitating the physicians to identify and notice the matters related with sick persons.

10.4.2 Role of IoT and Grid Computing in Healthcare

A novel context-conscious information and sufferer-oriented technique for global healthcare is essential to supply individual healthcare treatments to the old and the disabled persons. However, this innovative technique needs real-time in the area of development and gather vigorous symbols utilizing intrinsically through complicated biological replicas and study of the processed data (resultant biological parameters) underneath framework (e.g., site, ambient conditions, present physical condition) to bring out proficiency about the fitness disorder of victims. As the executional abilities for biomedical sensor nodes are inadequate to route these models, a new device providing outline that attaches the computing abilities of under-used electronic resources in the locality for arrangement of a mobile computing grid. The outline of the model is conveyed with self-optimization and self-healing abilities for effectiveness and steadiness beneath lack of certainty etc. The suggested model based on mobile grid management works as a clue permitting skill for IoT based future-generation global healthcare outcomes.

10.4.3 Role of IoT and Big Data in Healthcare

The innovative view points for fitness care controlling is given rise to the expansion of IoT and Big data, and the abundant quality of small bio sensors [5]. Several challenges have yet to be presented to make a reliable and stretchy scheme for health care controlling. IoT based health care controlling scheme consist of "Internet of health sensor things". These belongings generate a large volume of information that could not be monitored by the doctors. The vital anxiety of a doctor is that they require to create crucial choices about their sick's problems related with diseases from these large amount of health data. He/she has to separate the data about one specific sick person from the large amount of health care data

collected from the gigantic count of sick persons. Intel Galileo Gen 2 is performing as IoT representative and is utilized to organize the data about sick person's health into the Cloud. The Cloud could handle the growing amount of health information, ingeniously exchange the data through the healthcare models and supply capability for Big data analytics. The warning of data related with bad health of a sick person at proper time is a crucial effort in Big data which is very important. The Big health sensor are evaluated using the Hadoop model.

Ambient Intelligence with IoT systems is a developing research area and there is normally a shortage to realize the appropriate methods to take care in this area. The achievement of IoT systems relays on the effective combination of its resources, sensors and information management methods. Ambient Intelligence (AmI) is an innovative method in information technology focused at permitting mankind's abilities using the modern digital techniques those are adjustable and responsive to necessities, practices, motions, and feelings of mankind. This innovative idea of every day's need will empower us with new mankind-machine interactions characterized by prevalent, unremarkable and preventive transmissions. Such new interaction models create ambient intelligence technology an appropriate applicant for constructing different real-life explanations, together with the area of health care technology. We deliberate the importance of AmI technology in the health care area, with the aim to supply the researchers with the required circumstantial. We evaluate the setup and techniques needed for receiving the idea of ambient intelligence, such as smart surroundings and costumery pharmaceutical resources. We review the advanced techniques based on AI (Artificial Intelligence) utilized for constructing AmI scheme in the health care area with different studying methods (for studying from customer communication), cognitive methods (for thinking and understanding about customers' achievements and wishes) and drafting methods (for designing operations and communications). We deliberate how AmI techniques may help mankind who are suffering from different physical or mental inabilities or long-lasting sickness.

10.4.4 Role of Augmented Reality and IoT in Healthcare

Augmented reality (AR) improves your opinion to the real world by covering and showing digital content [6, 7]. Except marketing and entertaining objectives, AR is also achieving importance in the healthcare area. This growing technology is assisting this field in acquiring innovative schemes that returns back to the invention to existing health care systems, nourishment of the sick persons, apparatus conservation and helping doctors in their training and exercise daily.

Google Glass is one of the widespread platforms in supplying AR solutions in healthcare. Although it fails miserably in the mainstream market, this wearable technology is searching customers in healthcare. There are many companies whose objectives are to supply innovative AR solutions to healthcare.

(a) **Advantages of AR in Healthcare**

i. **How AR Benefits Patients?**

Augmented reality supports to enhance the quality of treatment of an admitted sick person. It supplies an improved way to the sick persons to define their symptoms. AR apps are accessible to teach the sufferer and the household members of the victims about the effect of specific illnesses for supplying superior treatment and anticipation. This data supports the sick persons in creating proper healthcare resolutions.

ii. **How AR Benefits Doctors?**

Augmented reality accomplishes as a visualization and training tool for physicians. Accuracy is very vital when performing complex surgeries. The correctness of this highly new and novel technology will support the surgeons to be more effective at surgeries. AR permits the few skilled surgeons to search for the distant supervision and control of veteran surgeons while executing complex methods. This technology provides the physician's admission to sufferer's data quickly and in real time thereby empowering the capability of the physicians to detect and start treatment quickly.

iii. **Locating Veins Using AR**

Augmented reality supports to generate easy methods such as pulling blood. A handheld scanner called AccuVein is now in utilize that usage augmented authenticity to irradiate the veins on a victim's skin thereby helping nurses in tracing the veins. This capability is very helpful for cosmetic surgeries too.

iv. **Support Blind People Navigate**

Augmented reality glasses are obtainable that provides the blind to be conscious of their surrounds. Depth sensors and the software in these smart glasses supports to highpoint the frameworks and make simpler the characteristics of adjacent mankind and entities.

v. **Helps People in the Autism Spectrum**

Wearable technology which characters AR environment permit the children and grownups in autism spectrum to explain themselves about serious life skills.

vi. **Training with AR**

Medical students are required to have a moral realizing of human anatomy, sickness pathology and surgical methods along with the real time implications. AR creates medical training more collaborative. Few AR apps are existing which when positioned over an exact page in the book will condense a 3-D illustration of the 2-D image. This way the students can read a specific subject thoroughly. AR can be used in many fields in this area that can give advantage in all related with it. Most of the professionals in the area of healthcare are unconscious of this innovative technology too. Consciousness has to be generated among them for AR and more novel innovations are required in this area so that they can accept this technology in their daily exercise.

10.5 Future of IoT in Healthcare

Just a few years ago, medical practitioners were closely watching the development of IoT and thinking to make it a part of their future. Today, it's not only a reality, but also making life easier for healthcare providers and patients also.

Now it is the most important question that how far we have come with IoT and where will IoT go in future? The increasing development in AI and interface of AI and IoT [8–16] is likely to acquire more intelligent IoT devices which can have the ability to perform activities autonomously in the healthcare sector. This could include medical devices that react to triggers or recognize the patient and interact with them based on their treatment plan. And also the use of autonomous drones to deliver drugs and other facilities in need are the near future of IOT in healthcare. It is almost in use but not in full bloom.

Artificial intelligence is the most vital area which can be explored more and more in this field. Healthcare robots are being used today but it will be used more in near future than today. To be futuristic, It may seem that, there will be a 50% increase in the use of robots by 2020. In fact, these robots perform simple, automated tasks such as delivering medications, food and lab results. Internet of medical things (IoMT) devices can also directly feed data into larger AI-driven healthcare analytics systems. These systems can diagnose heart disease, and detect blood infections and even certain types of cancer. These IoMT devices are being more improved and will be able to diagnose more diseases in future.

Next-generation IoT devices will bring intelligent services as part of their offering, allowing for real-time data which enables some actions to be executed by the device if necessary, and then send back data to the patient and their clinical teams.

Future Uses of IoT in Healthcare

- **Remote Monitoring**

Real time medical card reader devices and customized software will read data of patients and help doctors to conduct a better analysis of patient's health.

- **Wearables**

Several types of gadgets are obtainable in the market that can constantly monitor daily activities of the patients and store the data. These devices notify patients regarding their physical activities. They can also assist in preventing emergency, as patient's information would be sent to the doctor without delay.

- **Asset Monitoring**

IoT can help in providing functions and controllers to various essential equipments in the hospital. As the equipments are vital while treatment, any defect in them can be fatal. Connecting these devices will enable the staff to monitor their working easily. It can reduce the possibility of inappropriate treatment by figuring out the defects in the devices in real time.

Future Benefits of IoT in Healthcare

- **Better Supervision and Reporting**

Emergencies of patients of asthma attacks, heart failures like diseases can be saved by real-time supervision of IoT devices. The associated device can accumulate critical data of patient's health and convey it to the physician in real time. A survey conducted by Centre for Connected Health policy suggests that due to remote supervision, re-admission rate of patients was reduced by 50%.

- **End-to-End Connectivity**

The workflow of patient care can be automated by IoT with the help of healthcare mobility solutions. It enables interoperability, machine-to-machine communication, data movement and information exchange while making healthcare delivery more productive. Different connectivity protocols in the devices allow hospital personnel to spot early signs of illness in the patients.

- **Data Analysis**

IoT devices can gather report and assess the extensive data collected in short time, reducing the need of its storage. This helps healthcare providers in focusing on relevant data and speed up the decision-making process of the physician.

- **Alerts and Tracking**

Timely alerts can be crucial in case of life-threatening circumstances. IoT allows medical devices to gather essential data and transfer it to doctors in real time. The reports provide perfect opinion on the patient's condition, irrespective of location or time.

- **Lower Costs**

The connected devices and wearables will allow patients to connect with doctors from their homes. The regular visit for different tests and checkups will be minimized. This will save cost and time of patients on a daily basis.

- **Medication Management**

Time of medication can be tracked and can be remembered by the patients with the help of smart wireless pill bottles. The IoT enabled medication management processes will also provide doctors with analytics for offering better care to the patients.

Future Challenges of IoT in Healthcare

The challenges are also increasing with the increase of the IoT market in healthcare. Storing mountains of data collected by many devices will front a challenge to the healthcare organization. As this data will also be exchanged amongst other devices, the security issues will also rise. Unauthorized access to connected devices can cause harm to the patient's safety. Thus, proper authentication and authorization will be necessary to achieve success with IoT.

Applications that IoT has to offer are not fully developed yet. The widespread of connected devices in the healthcare structure is also incomplete. IoT and healthcare together will radically change the service offerings in the hospitals. The digitalization in healthcare will be brought by the IoT.

10.6 Conclusion

IoT changes the approach of the facilities which are designed and delivered to the healthcare industry. These technologies improve the product, causing a larger effect by bringing together minor changes. Rather than just creating tools, IoT tries and fills gaps between the way we deliver healthcare and the equipment by creating a system.

IoT tools and devices are revolutionizing medical care. Notably, remote patient monitoring devices enable innovative new ways of tracking a patient's health. Devices like glucose monitors, pulse oximeters and blood pressure monitors are fueling growth expected to reach a compound annual growth rate of 17%. Cloud computing and virtual infrastructure also provide caregivers real-time information and enable evidence-based treatment.

In this chapter benefit, challenges, technologies, different healthcare applications and future of IoT are covered and how IoT is beneficial for healthcare is explored.

References

1. https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html
2. Babu, R., Jayashree, K.: A survey on the role of IoT and cloud in health care. Int. J. Sci. Eng. Technol. Res. **4**(12), 2217–2219 (2015)
3. Jaiswal, K., Sobhanayak, S., Turuk, A.K., Bibhudatta, S. L., Mohanta, B.K., Jena, D.: An IoT-Cloud based smart healthcare monitoring system using container based virtual environment in Edge device. In: 2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR), pp. 1–7. IEEE, July 2018
4. Viswanathan, H., Lee, E.K., Pompili, D.: Mobile grid computing for data-and patient-centric ubiquitous healthcare. In: 2012 The First IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things (ETSIoT), pp. 36–41. IEEE, June 2012
5. Dineshkumar, P., SenthilKumar, R., Sujatha, K., Ponmagal, R.S., Rajavarman, V.N.: Big data analytics of IoT based Health care monitoring system. In: 2016 IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics Engineering (UPCON), pp. 55–60. IEEE, Dec 2016
6. Acampora, G., Cook, D.J., Rashidi, P., Vasilakos, A.V.: A survey on ambient intelligence in healthcare. Proc. IEEE **101**(12), 2470–2494 (2013)
7. https://smacar.com/augmented-reality-for-healthcare/
8. Rohokale, V.M., Prasad, N.R., Prasad, R.: A cooperative internet of things (IoT) for rural healthcare monitoring and control. In: 2011 2nd International Conference on Wireless

Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), pp. 1–6. IEEE, Feb 2011
9. Yuehong, Y.I.N., Zeng, Y., Chen, X., Fan, Y.: The internet of things in healthcare: an overview. J. Ind. Inform. Integr. **1**, 3–13 (2016)
10. Vicini, S., Bellini, S., Rosi, A., Sanna, A.: An internet of things enabled interactive totem for children in a living lab setting. In: 2012 18th International ICE Conference on Engineering, Technology and Innovation, pp. 1–10. IEEE, June 2012
11. Chung, W.Y., Lee, Y.D., Jung, S.J.: A wireless sensor network compatible wearable u-healthcare monitoring system using integrated ECG, accelerometer and SpO_2. In: 2008 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 1529–1532. IEEE, Aug 2008
12. Castillejo, P., Martinez, J.F., Rodriguez-Molina, J., Cuerva, A.: Integration of wearable devices in a wireless sensor network for an E-health application. IEEE Wirel. Commun. **20**(4), 38–49 (2013)
13. Sebestyen, G., Hangan, A., Oniga, S., Gál, Z.: eHealth solutions in the context of Internet of Things. In: 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, pp. 1–6. IEEE, May 2014
14. Burgun, A., Botti, G., Fieschi, M., Le Beux, P.: Sharing knowledge in medicine: semantic and ontologic facets of medical concepts. In: IEEE SMC'99 Conference Proceedings. 1999 IEEE International Conference on Systems, Man, and Cybernetics (Cat. No. 99CH37028), vol. 6, pp. 300–305. IEEE, Oct 1999
15. Liu, J., Yang, L.: Application of internet of things in the community security management. In: 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks, pp. 314–318. IEEE, July 2011
16. Xiao, Y., Chen, X., Li, W., Liu, B., Fang, D.: An immune theory based health monitoring and risk evaluation of earthen sites with internet of things. In: 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, pp. 378–382. IEEE, Aug 2013

Chapter 11
Research Perspectives on Applications of Internet-of-Things Technology in Healthcare WIBSN (Wearable and Implantable Body Sensor Network)

R. Dhaya, R. Kanthavel and Fahad Algarni

Abstract Dealing, managing clinical operations and tracing e-health importance of hospitalized patients have been the research oriented one. The advancement in knowledge sensors, microelectronics and coordinated circuit, system on-chip structure and low power wireless communications presented the advancement of scaled down and independent sensor hubs which can be sent to build up a proactive Body Sensor Network (BSN). The fast headway in ultra-low power RF (Radio Frequency) innovation encourages intrusive and non-obtrusive gadgets to deliver the biological information to a remote station. Moreover, the adoption of Internet of Things (IoT) may fetch remarkable alterations in the functioning efficacy to clinical centers. In addition, the Internet of Things (IoT) has control over the functioning process with minimized time to deliver improved care for mankind. The vital tasks to be focused are security and privacy in healthcare WIBSN, wearable and implantable imaging system, applications of Bio-implantable systems, wearable and implanted technology in health care applications and challenges of future directions in healthcare. By applying the Internet of Things (IoT) technology in healthcare applications must also look after the cost effectiveness, reliability, and safety. In this context, it is apparent to grasp that the study of applicability of Internet of Things (IoT) on e-health care sector is indeed a need of present time. Particularly, the characteristic of attached wearable's and their uprightness with Internet of Things

R. Dhaya (✉)
Department of Computer Science, King Khalid University,
Sarat Abida Campus, Abha, Kingdom of Saudi Arabia
e-mail: dhayavel2005@gmail.com

R. Kanthavel
Department of Computer Engineering, King Khalid University,
Abha, Kingdom of Saudi Arabia
e-mail: kanthavel2005@gmail.com

F. Algarni
Department of Computing and Information Technology,
University of Bisha, Bisha, Kingdom of Saudi Arabia
e-mail: fahad.a.algarni@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_11

(IoT) empowered technologies is unquestionably the greatest significant substance of learning. In summary, this chapter adds the following things namely Learning and evaluation of IoT supported parameters such as hardware and cloud platforms to determine the suitability for e-health care services, Analysis of existing IoT based wearable's solutions for e-healthcare Identification of encounters related with IoT aware e-health care domain, Analysis of integration of WIBST and IoT attained from this arduous study. The challenges and benefits of IoT based applications for healthcare have also been outlined later in the Chapter.

Keywords IoT · Healthcare · Wearable and implantable body sensor network · Radio frequency

11.1 Introduction

The Internet of Things (IoT) has extended its opportunities in medicine to the conventional medical devices that can gather precious supplementary data, provide further understanding into indications and developments, permit inaccessible care by means of offering patients mechanism over their breathes and management [1]. For many recent years, Micro-electro-mechanical systems (MEMS) expertise has been a boon for the edifice of a low-powered and small-sized sensor knobs to create a wireless sensor network (WSN) which do not need infrastructure or need very little infrastructure for surveillance purpose. On the other hand, WBASN plays a significant role to permit healthcare observing process that might be completed remotely as one of the most distinguished request areas of WBASN which comprises two types of sensors namely invasive and non-invasive categories for observing and determining humanoid biological strictures. These devices can be used with an intention not to intrude the individual's commotion but could platter the biological strictures at the time of human action like for the blood pressure, heartbeat or temperature and during daily routine works. Due to its tiny size and flexibility, these sensors carry out mainly three tasks in the form of sensing, processing, and communication which are responsible to sense the data to processing purpose before sending that to the communication task in the form of processing. WBASNs could also render help to the injured people as a significant impact on the medical field. Consequently, the Internet of Things (IoT) technology is seemingly being applied in the healthcare industry successfully since healthcare services are expensive and the number of chronic diseases is on ascending mode. The main applications of IoT in the field of intelligent medicine carry the perception and conception of material management, digitization of medical information and processes. Medical diagnostic may go through a Technology that can change the procedure of medical appraisal from a clinic to the patient's home without hospitalization by a novel pattern, recognized as the Internet of Things (IoT). The healthcare data like blood pressure, oxygen and blood sugar levels, weight, and ECGs from the IoT Based body sensor networks from the patients remotely are stored in the cloud which could be united with a physician or an external consultant no matter of

their place, time, or device [2]. This kind of Real-time surveillance can spare lives on medicinal crisis like heart disappointment, diabetes, asthma assaults, and so forth by methods for a brilliant therapeutic gadget associated with application to exchange gathered data to a doctor. IoT can adjust understanding consideration progression with the guide of cutting edge social insurance offices to empower interoperability, machine-to-machine correspondence, data trade, and medicinal services administration conveyance compelling. Bluetooth, Wi-Fi, Z-wave, ZigBee, and other present day conventions have been the communication protocol choices in healthcare personnel by reducing unwanted visits, utilizing and better quality resources to speed up decision-making with no errors. Thus, IoT creates timely alerts on emergency care and routine follow-ups for the patients through tracking, and monitoring, which allows hands-on treatments accurately to improve absolute patient concern outcomes instantly. The advancements of IoT in healthcare is exciting owing to its various scope of use in mainly reducing crisis time, trailing patients, staff, and inventory, intensify drug management and guarantee of critical hardware. This Chapter incorporates preliminary studies as its first section which elaborates the relevant literature survey in healthcare WSBN applications using IoT technologies and the rest of the sections focus on the IoT supported parameters such as hardware and cloud platforms to determine the suitability for e-health care services followed by analysis of existing IoT based wearable's solutions for e-healthcare and finally identification of encounters related with IoT aware e-health care domain along with IoT in cloud platform for e-healthcare have been discussed.

11.2 Preliminary Studies

The relevant researches in healthcare WIBSN (wearable and implantable body sensor network) using IOTS have been surveyed in various streams of applications.

Anu Rathee et al. [3] examined the various conceptions related to the wireless sensor wearable devices in health care with an overall perspective of the entire ecosystem of the IoT. Ashraf Darwish and Aboul Ella Hassanien [4] delivered numerous examples of state of the art expertise composed with the strategy deliberations like unobtrusiveness, scalability, power competence, safety, numerous profits and downsides of the structures. While contributing important profits, the domain of wearable and implantable body sensor networks quiet looks at main challenges and vulnerable investigation difficulties which are examined beside with resolutions. Sana Ullah, Henry Higgin, M. Arif Siddiqui1, and Kyung Sup Kwak presented in-body and on-body communication networks on the procedures of wireless communication amid implanted medical devices with exterior observing apparatus on Body sensor network in healthcare applications. S. N. Mohamed Hamdi, Noureddine Boudriga, Habtamu Abie [5] introduced a lightweight identity based encryption protocol suitable for body smart sensor systems along with the experimented results. Sanaz Rahim iMoosavia Tuan, NguyenGiaaAmir Mohammad, Rahmania bethiopia Nigussie SeppoVirtanena [6] presented an well-organized

verification and validation architecture for a secure IoT based health care. Their projected architecture trusts on the certificate-based DTLS handshake protocol as it is the key IP safety resolution for IoT which authenticates and authorizes architecture. Nathalie Marcela Cerón Hurtado, Mohammad Hossein Zarifi, Mojgan Daneshmand, Jordi Aguiló Ll [7] presented a flexible wearable cum implantable bio-compatible sensor using wireless passive detection scheme as a dynamics to an implanted abdominal mesh. Yangzhe Liao, Mark S. Leeson, Matthew D. Higgins, Chenyao Bai [8] proposed an analytical cum accurate in-to-out (I2O) human body path loss (PL) model at 2.45 GHz based on a 3D heterogeneous human body prototypical below security restraints. Revathi Pulichintha Harshitha, Prashanthi Narramneni and Raghavee [9] talked about the troublesome linked to the usage of wearable and implantable sensors for distributed mobile computing. Nadeen R. Rishani, Hadeel Elayan, Raed M. Shubair, and Asimina Kiourti [10] surveyed the current state of art in the area of wireless sensors for medical applications to specifically focus on presenting the recent advancements in wearable, epidermal and implantable technologies. Furthermore, they addressed the challenges that exist in the various Open Systems Interconnection (OSI) layers to depict the future research areas concerning the utilization of wireless sensors in health care applications. Though lots of survey papers undergone here are about IoT in healthcare applications using wearable body area sensor network in a detailed manner but those need further attention and requirement in analyzing the same. The next section presents about the parameters related with IoT that is suitable for E-Healthcare services.

11.3 Learning and Evaluation of IoT Supported Parameters Such as Hardware and Cloud Platforms to Determine the Suitability for E-Health Care Services

The study of Internet of Things (IoT) is to provide seamless and pervasive support to e-health care which has a list of five checks to be performed.

Firstly, a thorough review of the nine different resource constraints through less amount of memory, processor speed, capacity, bus width, and size hardware platforms have been carried away in order to perform comparison on operating voltage, clock speed (MHz), bus size (bits), system memory, flash memory, Electrically Erasable Programmable Read-Only Memory (EEPROM), communication supported, development environments, programming language, and Input/output (I/O) connectivity. Primarily, two types of processor families have been sought for the purpose such as, RISC (Reduced Instruction Set Computer) e.g., Arduino Mega 2560, Arduino Yun, Beagle Bone Black, Kinetics K 53, MSP 430, Marvel 88 MZ 100, Raspberry Pi 3, and Kinetics K 53; CISC (Complex Instruction Set Computer) e.g., Intel Galileo Gen 2, and Intel Edison.

Secondly, various communication technologies have been compared based on their standards, frequency band, data rate transmission range, energy consumption,

and cost for application towards e- health applications [11]. It has also been focused to facilitate Internet of Things (IoT) formulated resources be it hardware, wearable's, or cloud [12]. Main priority has been given to Wi-Fi, LR-WPAN (Low-Rate Wireless Personal Area Networks), Bluetooth Low Energy (BLTE), NFC (Near Field Communication), Mobile Communication (2G, 3G, 4G), WBAN (Wireless Body Area Network) and nano-scale communication [13].

Thirdly, the existing IoT cloud platforms have been investigated based on real time access, data visualization, data capture, data analytic, cloud service type and cost. In this context, a cloud can be viewed as a service to deliver the on demand computing properties from efficacies to data cores on a wage as go base or free. Basically, IoT cloud stands are meant to provide numerous solutions for developers to build and deploy powerful IoT applications (e.g., medical, hospital, and emergency services), utensils for system producers to rapidly incorporate newly linked facilities to the yields and perform actions between machines social networks, and much more [14].

Fourthly, different wearable's e-health solutions have been tracked down in this work to study about usability of sensors, applicability among several genres of population, and detecting parameter (e.g., baby monitor, women e-health, elderly, cardiac, fitness etc.).

Finally, after gathering of required amount of information on hardware platform, communication technologies, cloud solutions, and wearable's, the rest of its task is to analyses the data to seek valuable answers about few tasks such as,

- The hardware platform which is suitable for the development of Internet of Things (IoT) based e-healthcare products.
- The network technologies that pave crucial role in Internet of Things (IoT) supported e-healthcare communications.
- The percentages of owner-ships among e-health care based Internet of Things (IoT) cloud platforms where cost and analytics tools are heavily involved.
- The dissemination percentages of Wi-Fi, Cloud, APP, and BLE (Bluetooth Low Energy) in Internet of Things (IoT) based wearable's.
- The usage pattern of wearable sensors.
- The deployment percentage of area specific Internet of Things (IoT) based wearables.

Hence, it is much needed task to analyze the existing wearable solutions for Healthcare using IoT which follows in the next section.

11.4 Analysis of Existing IoT Based Wearable's Solutions for E-Healthcare

The IoT has opened among people of predictions in medicine when identified with the internet; customary medical utensils can amass significant supporting data in order to give further appreciation into signs and movement. The following are some examples of IoT in social protection that develop the remedial measure to accomplish.

11.4.1 Cancer Treatment

The patients who rehearsed the knowledge checking structure to surely understand as CYCORE with experienced less extreme indications identified with both the malicious growth and its treatment of patients who continued with normal week after week doctor visits. The examination shows the potential advantages of practicality innovation with regards to improve patient interact with doctors, and checking of patients' circumstances, such that origins insignificant obstruction with their day by day lives. Technology makes the relationship with therapeutic expert that significantly important and puts more in control.

11.4.2 Smart Continuous Glucose Monitoring (CGM) and Insulin Pens

- Diabetes partakes ended up being a ready pulverized for the progression of splendid maneuvers as a situation that impacts around one out of ten adults and one that needs perpetual checking and association of treatment. A Continuous Glucose Monitor (CGM) is a contraption that urges diabetics to continually screen the blood glucose levels for a couple of days on end by enchanting readings at typical between time. Adroit CGMs like Ever sense and Freestyle Libre send data on blood glucose levels to an application on iPhone, Android or Apple Watch, empowering the wearer to successfully check their information and recognize designs [15]. The FreeStyle LibreLink application furthermore mulls over remote checking by means of watchmen, which could consolidate the gatekeepers of diabetic youths or the relatives of old patients.

11.4.3 Ever Sense Diabetes

Another powerful tool accurate now enlightening the lives of diabetes patients is the savvy insulin pen. Savvy insulin pens or pen tops like InPen and Esysta can naturally record the time; sum and kind of insulin infused in a portion and suggest the right category of insulin infusion at the perfect time [16]. This utensils interface with a cell phone application that can store long haul information in helping out diabetes patients figure their insulin portion, and even enable patients to record their suppers and glucose levels in order to perceive how their nourishment and insulin admission are influencing their glucose.

11.4.4 Closed-Loop (Automated) Insulin Delivery

A standout amongst the most intriguing zones in IoT medication is the open-source activity OpenAPS, which represents Open Artificial Pancreas System. OpenAPS is

a sort of computerized insulin conveyance framework, which contrasts from a CGM in assessing the measure of glucose in a patient's circulation system. It additionally conveys insulin in shutting the circle [17]. Utilizing the information feed from the CGM and a Raspberry Pi PC, their own product finishes the circle and ceaselessly adjusts the measure of insulin Dana's siphon conveys. Robotizing insulin conveyance offers various advantages that can change the lives of diabetics. By observing a person's blood glucose levels and consequently modifying the measure of insulin conveyed into their framework, the APS keeps blood glucose inside a protected range in anticipating extraordinary highs and lows (hyperglycaemia high glucose and hypoglycemia low glucose). The programmed conveyance of insulin additionally enables diabetics to stay asleep from sundown to sunset without the threat of their glucose dropping. Despite the fact that OpenAPS isn't an "out of the crate" arrangement and expects individuals to be eager to assemble their very own framework. It is pulling in a developing network of diabetics for utilizing its free and open-source innovation to hack their insulin conveyance.

11.4.5 Connected Inhalers

Asthma is a condition that influences the lives of countless individuals over the world. Keen innovation is starting to give them expanded knowledge into and command over their side effects and treatment, on account of associated inhalers. The greatest maker of shrewd inhaler innovation is Propeller Health. As opposed to delivering whole inhalers, Propeller has prepared a sensor that links to an inhaler or Bluetooth spirometer. It relates up to an application and helps people with asthma and COPD (Chronic Obstructive Pulmonary Disease, which incorporates emphysema and endless bronchitis) comprehend what may cause their side effects to track employments of salvage medicine [18]. One of the advantages of utilizing an associated inhaler is improved adherence. At the end of the day, drug is taken all the more reliably and all the more regularly. The Propeller sensor produces stretches an account of inhaler utilizes that can be imparted to a patient's specialist.

11.4.6 Ingestible Sensors

Proteus Digital Health and its ingestible sensors are another instance of how sharp medicine can screen adherence. The gathering has made pills that separate in the stomach and produce a little banner that is snatched by a sensor worn on the body. The data is then exchanged to a PDA application in confirming that the patient has acknowledged their solution as composed. Proteus has so far trialed the structure with pills for treating uncontrolled hypertension and Type 2 Diabetes, and antipsychotic medication [19]. Also as with related inhalers, ingestible sensors can pursue and improve how typically patients take their medicine, similarly as

empowering them to have an undeniably instructed talk with their specialist about treatment. While taking pills with a sensor that may seem, by all accounts, to be prominent, the structure is great in regarding patients and they can stop sharing a couple of sorts of information or quit the program completely, at whatever point.

11.4.7 Linked Contact Lenses

Medicinal rude contact focal points are a decided use of the IoTs in a human services circumstance. While the idea has a lot of potential up until this point, the science has not generally figured out how to satisfy desires. The other therapeutic applications for savvy contact focal points may demonstrate progressively fruitful. Verily is as yet chipping away at two savvy focal point programs with Alcon, which plan to treat presbyopia and waterfall medical procedure recuperation. Swiss organization Sensimed has additionally built up a noninvasive savvy contact point of convergence or focal point called Triggerfish, which normally enlists the varieties in eye measurements that can quick glaucoma [20].

11.4.8 Depression Monitoring Tool

To investigate the utilization of an Apple Watch application for checking and evaluating patients is done with Major Depressive Disorder (MDD) [21]. The analysis found an exceptionally abnormal state of consistence with the application, which members utilized day by day to screen their disposition and discernment [22]. The application's every day evaluations were additionally found to relate with additional top to bottom and target perception tests and patient-detailed results in appearing psychological tests conveyed by means of an application can even now be forceful and dependable. While the analysis is just an exploratory model which has shown the potential for wearable tech to be utilized to evaluate the impacts of gloom progressively. Like other brilliant medicinal gadgets that assemble information, the Apple Watch application could likewise give patients and human services professionals more knowledge into their condition and empower progressively educated discussions about consideration.

11.4.9 Clotting Testing

Bluetooth -enabled clotting system that enables patients to check how rapidly their blood coagulation. This tool is a type of utensil for aggressive to coagulated patients with self-testing appeared to enable patients to remain inside their restorative range and lower the danger of stroke or dying [23]. This device additionally enables

patients to add remarks to their outcomes, reminds them to test, and banners the outcomes in connection to the objective range.

11.4.10 Research Equipment and Parkinson's Disease

Usually Parkinson's disease side effects are observed by a doctor at a facility through physical effusive tests. In addition, patients are urged to maintain a periodical in control to give a more wide familiarity into signs after some time. The Apple incorporated alternative 'Development Disorder API' which permits Apple Watches to monitor Parkinson's disease side effects [24]. This Apple API proposes to make that procedure programmed and ceaseless. An application on an related iPhone can display the information in a diagram, spring every day and hourly analyses, just as moment by-minute indication modification.

11.4.11 Asthma Monitoring System

It shakes to tell the individual exhausting it of a looming asthma attack and can likewise send an instant message to an assigned ability in the meantime. Different high points of the devices incorporate inhaler identification, the gadget can recognize and follow inhaler usage, if the patient cannot recall whether they've utilized one and voice to record belongings like variations, sentiments and practices. It additionally has a calculation modernization that understands what ordinary is for the wearer after some time, enabling it to all the more likely comprehend when something has changed. It works related to an application and online interface, assisting asthma patients with setting prescription updates, see information from the gadget, and help them to remember their treatment plan.

The next section elaborates the vital things that involve in creating awareness in healthcare domain using IoT.

11.5 Identification of Encounters Related with IoT Aware E-Health Care Domain

The important explanations on the IoT based e-healthcare are given as follows.

- Raspberry Pi 3 and Beagle Bone Black devices are the hardware phases where scalable applications and e-healthcare based researches might be accomplished. Intel, Arduin, and Kinetics modules are in processing speed and memory limit than the stated ones.
- Blue Tooth Low Energy (BTLE) and Wireless Body Area Network (WBAN) correspondence technologies seem to necessitate the IoT intrusion into the

healthcare through their low energy efficiency, cost, and high band width and information transmission rate. However these are short range correspondence especially great when to deploy for wearable's. In the event that information must be transmitted to remote places or far off areas, then mobile correspondence (e.g., 2G, 3G, and 4G) and LR-WPAN ought to be used (i.e., remote health observing etc.) [25]. Wi-Fi is a wireless technology for short range that has ability of energy utilization and information rate only in between of Blue Tooth Low Energy (BTLE), Wireless Body Area Network (WBAN) and mobile correspondences. Hence, restriction based applications (e.g., denture X-beam, post exercise ECG, EMG, child movement checking etc.) might be developed utilizing Wi-Fi. Nano scale correspondence may also be used for diagnosing purposes for in vitro circumstances (e.g., Camera capsule, Lab-on-Chip serum testing etc.)

- Axeda, Exosute, Neosoft, E-health Saas, Cleadata etc. cloud stages are made in such design that they are perfect for dealing with healthcare services. Others are likewise capable to hold the IoT healthcare however does need more capabilities to persuade urgent applications. Thing Worx, Ployly, and Thing Speak are best for the development phase before genuine deployment offend item due to free of expense. Carriots, Connecterra, Aekessa etc. IoT mists would be chosen for structure applications where real-time automated response and activation are required (e.g., advising relatives about the sudden fall of an elderly, sudden rise of body temperature of a child etc.)
- Accelerometer, ECG, pressure, Body temperature, step check sensors are the currently being for the most part deployed sensors in the surveyed wearables. SPO2, Doppler probe, movement sensor, and pulse sensor are among the other most encouraging technologies that are increasing subsequent prevalence to measure vitals of human body.
- A matter of concern that is found in the investigation is the expense of the wearable's [26]. Around 41% of these are sold in the range of 51–200 $ per unit which is very high to manage the cost of in poor people and low income countries, for example, India, Bangladesh and other pieces of Asia and Africa.
- At the same time, great trends are being observed that elderly checking, children care, women health and regular life style management related items are steadily up coming into the Internet of Things (IoT) market for benefit of human society converting the mindset towards a smarter world.

Though the awareness of E-healthcare domain studies by facing a lots of challenges to overcome are anal zed in the following section.

11.6 Identification of Challenges Associated with IoT Aware E-Health Care Domain

Whereas IoT health accompanies the guarantees and dreams of consistent network over the physically inaccessible areas where patients, centers and medical clinics could participate, arrange and coordinate the human services forms. There are a few

research difficulties that IoT health needs to defeat before it could turn into a standard platform [15]. However concentrating the results of IoT in brilliant e-social insurance a few difficulties have been recognized as beneath.

- **Regulation**: IoT based e-health services arrangements are still in early phase of improvement and current arrangements do not adjust to explicit principle and guidelines. This raises interoperability issues that need to take care of by scientists by teaming up e.g., unique team in IoT e-wellbeing.
- **Quality of Service (QoS)**: By way of e-health services, administrations require thorough unwavering quality and viability of the framework. It ought to be captured that no postponement, association or information misfortune to be happened by improving the nature of administration. If there should be an occurrence of framework disappointment, excess administrations ought to instantly be benefited by the patient.
- **Environmental Features**: Undeniable IoT e-health care services will need minimal effort bio medical sensors that are easily implantable into human body. Theses sensors might be utilizing rare earth metal or any kind of dangerous elements. This indeed has essential yet unfavorable effects on environment. Government and regulatory bodies e.g., WHO (World Health Organization) ought to prepare a guideline to provide way of assembling of sensors, usage pattern, and transfer practices [27].
- **Information management**: Information management encounters for IoT health is like folks confronted by IoT in additional areas. Though, the health information originates from medical sensors devoted to people. The humanoid frame is a lively structure that vicissitudes its state constantly. Henceforth, as understood in IoT health presentations, there will be a consistent transition of information originating from edge sensors by means of mist registering nodes. The cost of sensors and figuring is declining and henceforth, it has turned out to be less expensive to gather the gigantic data in a short time span. In other presence, IoT wellbeing needs to deal with the intricacy of the data as far as their assortment, volume and speed. There are many data positions relying upon the social insurance end client applications. For instance, ECG data could be imparted in XML plan, while recognizing skin ailments using camera-based IoT gadget need to deal with picture positions. The data configuration support for edge PCs is subject to the makers and their objective clients. Despite edge data position, the data model on the cloud in like manner shifts and in this way, requests regulation. The difficulties of data volume and speed are more connected with the abilities of fog hub equipment to get, procedure, store and convey the high-loyalty, high-goals data starting from restorative gadgets that could be with patients or in crisis centers or offices. Accordingly, there will be a need of fog executives who could supervise the data movement between the fogs and conveyed figuring.
- **Scalability**: To manufacture a littler size of IoT, sensors on versatile gadgets for data gathering and secure focal servers for preparing clients' solicitations are utilized to guarantee all clients that can legitimately get to restorative

administrations by methods for compact gadgets, for instance, advanced mobile phones. This office can be scaled up to the whole facility with the objective that patients in the crisis center which can utilize medicinal administrations check updates and wellbeing status seeing by their advanced mobile phones. This wellbeing model can be scaled up to the whole city, if there are sensors and reception apparatus in the city to gather data, astute tremendous data counts. Advantages of flexibility to an adroit city level can incorporate improvement in effectiveness, saving quality time for delaying and building direct relationship and trust between restorative staff and patients.

- **Interoperability, standardization and regulatory relationships**: When all is said in done, IoT has brought worries up in the territory of organization. All makers, specialist organizations, and end clients look for standards for operability both inside and between the spaces focused by IoT applications. The organization unpredictability lies in the manner that IoT expects to catch a wide scope of controls that are, when all is said in done, directed by various administrative issues. By virtue of IoT wellbeing, the multifaceted nature even increments because of the serious guidelines commanded by medicinal rules.
- **Interfaces and human-issues engineering**: Exceptional key issues in IoT wellbeing is the interface of the front-end advancements sensors, cell phones, tablets, PCs, and different sorts of associations. At the point when IoT medicinal gadgets are structured and given to the patients who have no involvement of using front line instruments, it turns out to be exceptionally imperative that end-clients would most likely self-train themselves with these gadgets. When all is said in done, end-clients have constrained information about the remote systems administration, sensor altering and different activities of the gadget. In addition, when the gadgets will go in remote situations, setting up the wellbeing frameworks ought to be immediate and self-overseeing. For instance, older people will be one of the biggest partners of IoT wellbeing. Subsequently, gadget interfaces should be client (quiet) amicable and to require least inclusion of specialists [28]. One of the fruitful practices in human-factors building is a participatory structure, in which partners or end-clients of IoT wellbeing gadgets could turn into a bit of the plan group to give constant input of their preferences, abhorrence's, and comforts.
- **Security and confidentiality**: Each unmistakable IoT gadget conceivably will endure a conceivable peril that could be misused to either outraged the end-clients or imperil the security of them. Moreover, this can prompt making threats to individual security. Security and insurance of IoT wellbeing ranges the entire lifecycle of the framework starting from particular age to execution and organization. Be that as it may, securing IoT wellbeing biological system is an advanced and testing errand. In order to push IoT wellbeing, these difficulties must be overwhelmed by embracing a complete multi-layer technique. In addition to the awareness and challenges faced in IoT based healthcare WBSN domain, there have been a high demand of advanced applications as explained below.

11.7 Advanced IoT Applications in Healthcare

Some of the advanced IoT Applications in healthcare [29] are listed in Fig. 11.1:

- **Following real-time position**: Uses of IoT in medicinal services administrations are making it useful for experts/specialists to pursue the gadgets used by patients for treating them using continuous area administrations. Medicinal contraptions and mechanical get together like wheelchairs, scales, nebulizers, defibrillators, monitoring gadgets, or siphons can be fixed with sensors and put adequately with IoT. Beside ongoing area administrations, there are furthermore other IoT devices that help with watching nature as well.
- **Watching hand tidiness**: Watching hand tidiness has advanced toward getting to be reality with the continuous usages of IoT in medicinal services administrations. IoT contraptions at present can recognize the tidiness dimension of any restorative administrations worker or social insurance laborer. A progressing outline presented that one out of every 20 patients gets a sickness owing to nonattendance of proper hand tidiness in open crisis facilities. There are various patients who make certifiable disorders out of such restorative center infections and in the long astounding. New usages of IoT in human services administrations have made it easy to harden every one of the information of a social protection authority.
- **Remote health monitoring**: One of the basic employments of IoT in human services is checking wellbeing in remote regions. If the social insurance workplaces are not nonsensically settled in the remote zones, the all-inclusive community living in these locales can be given satisfactory help through IoT. People are losing lives every day because of the inadequacy of lucky and fast

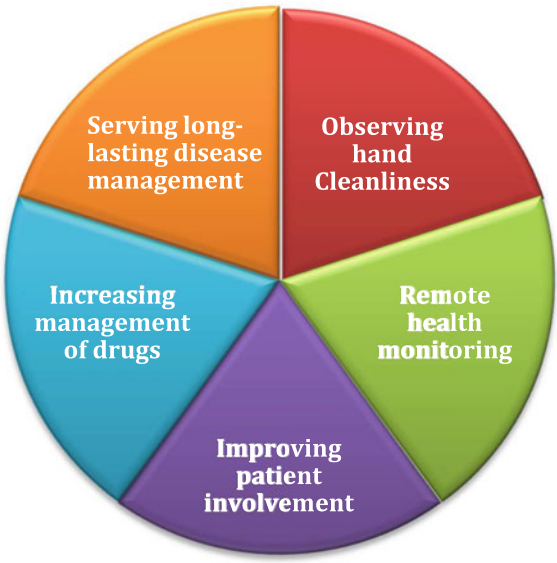


Fig. 11.1 Advanced IoT Applications in Healthcare

remedial help. Uses of IoT in social insurance have made it practical to fit contraptions with sensors that alert the able pros if there ought to be an event of any modification in the condition of a patient. With the help of remote observing, there can be a huge abatement in the length of medicinal facility stays and moreover in the re-confirmation rates. This kind of headway by IoT is a gift to mankind, particularly for developed people.

- **Improving patient involvement**: IoT applications in social insurance have helped in improving the experience of patients. It has now ended up being straightforward for the patients to control the temperature and lightning of their live with the help of the predictable relationship among them and gadgets. Similarly, by and by it isn't any all the more debilitating for the patients to stay for long in the facility bed as late IoT applications in social insurance have made it straightforward for them to talk with their friends and family. They can in like manner team up with medicinal attenders or attendants through radio or telephone for any need. Such IoT applications moreover give basic access to tolerant information by the restorative staff from the cloud by helpful staff.
- **Increasing management of drugs**: Doctor supported remedy is a champion among the most jump forward improvements of IoT in social insurance. It seems, by all accounts, to be very Sci-fi, yet there are little sensors in the pills that are grain assessed and can send signs to outside devices. This ensures genuine usage and estimation of drugs. Advantageous mobile phone applications in like manner help patients get to the information and track their own execution.
- **Serving long-lasting disease management**: Most recent IoT applications in social insurance have influenced immense accomplishments concerning to treating the patients with steady conditions. Today, a single device can never oblige the treatment needs of the 21st century yet it is the blend of wearable development, flexible system, and front line examination that new IoT applications in medicinal services have brought into limit. Contraptions like Fit-piece have helped in redoing the human services and have given stimulating results.

These days, IoT has the rich forthcoming to accomplish every individual all-around at a lone time. More state-of-the-art IoT applications in human services are changing the section and the market will continue advancing with the persistently improving advancement yet how far it will take the world is one of the simple to invalidate centers for everyone. The Wireless Implantable Body Sensor Network is explained in the next section.

11.8 So Far on WIBST (Wireless Implantable Body Sensor Network)

Body sensor network frameworks can help individuals by giving social insurance executives, for example, medicinal checking, memory upgrade, control of home machines, medicinal information access, and correspondence in predicament

circumstances Continuous observing with wearable and implantable body sensor networks will increment initial location of crisis circumstances and illnesses in danger patients. Furthermore it gives an extensive scope of human facilities administrations for individuals with different degrees of intellectual and physical inabilities. Specialists in different interdisciplinary fields, for example, registering, building, and prescription fields are cooperating to guarantee that the wide apparition of wearable and implantable body sensor networks (WIBSNs) for brilliant human services, as showed in Fig. 11.2, can be satisfied.

The significance of coordinating extensive gauge of Wireless communication technologies, for example, 3G, Wi-Fi, and Wi-MAX, with tele-medicine has just been inclined to by certain scientists(1). The scope of wearable and implantable biomedical utensils will increment fundamentally in the following years, because of the upgrades in Micro Electro Mechanical Systems (MEMS) innovation, Wireless Communications, and computerized hardware, accomplished as of late. These advances have permitted the improvement of ease, low power, multi-useful sensor centers that are little in size and can impart over short separations, small sensor hubs, which comprise of detecting, information handling. Sensor networks in this manner speak to a critical improvement contrasted with customary sensors.

The following section focus on the wearable Healthcare applications using IoT in a detailed manner.

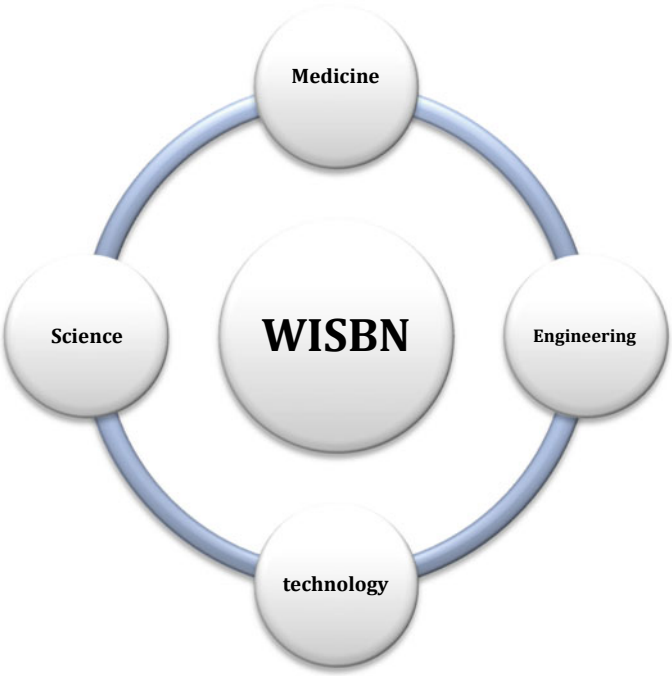


Fig. 11.2 Interdisciplinary for the future of WIBSN

11.9 IOT Based E Healthcare Domain

Medical care and healthcare intend one of the enchanting applications domains for the IoT. Also, different correspondence innovations have been looked at dependent on the device models, recurrence band, information rate transmission run, vitality utilization, and cost for application towards e-wellbeing applications. In this pursuit, it has been engaged to encourage Internet of Things (IoT) detailed assets be it equipment, wearable's, or cloud. Figure 11.3 analyses the IoT based e healthcare domain. Fundamental need is given to Wi-Fi, LR-WPAN (Low-Rate Wireless Personal Area Networks), Bluetooth Low Energy (BLTE), NFC (Near Field Communication), Mobile Communication (2G, 3G, 4G), WBAN (Wireless Body Area Network), and Nano scale correspondence [30]. Essentially, Internet of Things (IoT) cloud stages are intended to give various answers for designers to fabricate and convey ground-breaking Internet of Things (IoT) applications (e.g., therapeutic, clinic, and crisis administrations), devices for gadget makers to rapidly consolidate recently associated administrations to the items and perform activities between machines (gadgets/things) and informal communities, and substantially more.

11.10 IOT Based Wearable Solutions for E-Healthcare

Wearable innovation has jumped on like rapidly spreading fire. Individuals don't appear to grow sufficient of what their astute wristband combined with their Health application can do. Likewise, it is simply profitable to become all the more outstanding. An examination overview expresses that over 75% of plaintiffs feel that wearable medicinal services monitoring gadgets should wind up inescapable with the objective that it propels them to lead more advantageous lives [31].

Wearable gadgets can be characterized as innovation injected gadgets that could be damaged on the humanoid physique. They might be canny wristbands, wristwatches, shoes, shirts, tops, pieces of jewelry, headbands, eyeglasses, and so on.

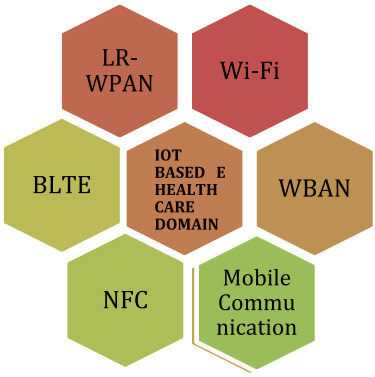


Fig. 11.3 IOT Based E Healthcare Domain

These splendid gadgets cover certain kind of devices that assistance in social occasion/meeting unrefined data and handing-off it into a record or programming. Over this product, we can assemble encounters and investigate our wellbeing.

The bit of learning or examination that is acquired is commonly receptive. The bits of information can alarm the individual exhausting the astute gadget or a specialist who might then have the capacity to take restorative movement. All the while, nutritionists can see the data and guidance a superior eating regimen plan, in view of development level and aliments. Basically, web of things in medicinal services is unwinding various difficulties. IoT affected various enterprises, and the innovation left its engraving wherever it went. Organizations that have neglected to incorporate IoT gadgets into their procedures hazard being deserted. One of the advantages of IoT in human services is that it considers customized consideration from restorative experts [32] gets the customized consideration from therapeutic experts. With IoT gadgets furthermore help in calculating calories, check beat levels, help patients to remember their arrangements, and so on. Figure 11.4 shows the Personalized attention from medical professionals in below points.

Location-Dependent Real-Time Amenities

Over IoT, medicinal services experts can pursue the patient's location. This is mainly helpful once a harmed individual is pending in for a pressing restorative help. Likewise, inside the center therapeutic mechanical gathering, for instance, defibrillators, scales, wheelchairs, other monitoring gadgets, and so forth can be labeled with IoT sensors to find them effectively. IoT gadgets assistance progressively ecological monitoring additionally, for instance, testing room temperature.

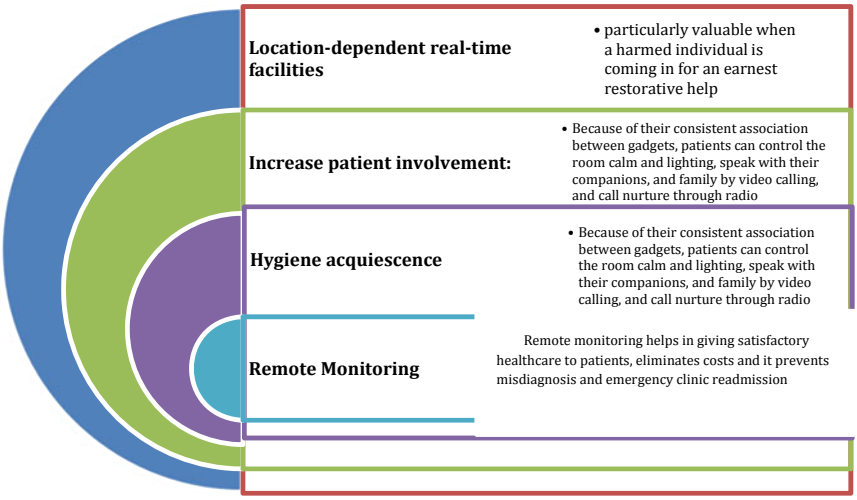


Fig. 11.4 Personalized attention from medical professionals

Increase Patient Participation
IoT gadgets support in purifying the patient contribution. Because of their consistent association between gadgets, patients can regulate the room calm and lighting, speak with their companions and family by methods for video calling, and call nurture through radio. IoT also contemplates simple contact tolerant data from the cloud by therapeutic staff gave they are put away there in any case.

Hygiene Assent For crisis or emergency centers, counteracting contamination is basic. Additionally, given that countless out and contaminated patients walk around consistently, how do crisis centers seek after demanding cleanliness. Practicing hand cleanliness is a standout amongst the best strategies for forestalling contaminations. Hand cleanliness monitoring frameworks aid in background and recognizing a level of neatness among human services and restorative staff. The least complex limit of hand cleanliness IoT gadgets is to signal at whatever point medicinal staff approaches in closeness of a patient bed without washing their hands. The correspondence between these hand cleanliness monitoring frameworks is progressively, henceforth there would not be some mistakes.

Remote Monitoring
Remote monitoring of wellbeing is an indispensable usage of IoT. Enduring observing supports in stretching satisfactory human services to patients. Extensively, various persons kick the bucket as they don't get opportune restorative consideration. IoT gadgets can relate multifaceted estimations and investigate them which helps in giving better medicinal consideration and care to patients in distant territories as a general rule places where authorities can not physically go [33].

Monitoring in like manner dispenses with expenses and it anticipates misdiagnosis and crisis facility readmission is leeway for senior natives. Besides, as IoT gadgets and wearable's are easy to utilize, where patients can approach their step by step routine missing much inconvenience. IoT in human services is required to assist the extent of research. IoT gadgets streamline work forms through legitimate examination. IoT gives cutting edge customized game plans and finding to patients dependent on their signs. Applications can be utilized to remind patients to take their drug. They moreover help and increment medicinal consistence.

Hazards of IoT in Healthcare
Regardless of the way that IoT and wearable's are viewed as a safe house for the human services business. There are various difficulties that organizations should report. The principal and perchance the utmost genuine of difficulties is assurance. As by far most of the records is actuality enthused to the cloud, it would not yield extended for secluded and delicate documents to decrease into the incorrect indicators [34].

IoT gadgets and wearable's work by talking with different gadgets. If this correspondence isn't verify which can lead and cause data spillage. Industry benchmarks should be pursued while making a wellbeing application.

The following thing is to associate the WBSN gadgets among hubs in cloud where bunches of challenges as security and protection that must be allowed foremost significance which is clarified as pursues.

11.11 IOT in Cloud Platform for E-Healthcare

A patient possibly will need the facilities of different healthcare sources like medical clinics/facilities, doctors, dentists, optometrists, radiologists, cardiologists, drug specialists, insurance, etc. A wide range of electronic organisms could be used, for example, modalities like MRI machines, etc., data systems like emergency clinic, radiology, lab, etc. and disparate conventions and messaging groups, used by the devices and Information Systems. In what way we efficiently and professionally offer complete and combined electronic health/medical/patient histories in the existence of such desperateness. Figure 11.5 defines the Collaboration amongst IoT and Healthcare Services.

The field of e-health is extended by telemedicine for lengthy expanse patient attention done by Metropolitan Area Network or Wide Area Network with independently wearable or mobile IoT expedients for home-based or in mobile checking of vigorous information [35]. Telemedicine and IoT require fresh compeers of communiqué resolutions, arrangements for the service layer and interoperability guidelines.

The procedure of Cloud has become practically universal in normal life. Numerous everyday actions of finale employers and facilities related to those actions are aided from anywhere in the Cloud ended the network, open or private, Internet or intranet. The efficiency of healthcare facilities can be importantly enhanced if e-health facilities are deployed in Clouds. While there are rewards, opportunities and many Cloud related challenges which are aggravated by the absence of Cloud connected norms at different stratums of Cloud organization and amenities [36].

Protection and security are progressively dynamic disquiets also. The secure dispensation of personal information in the Cloud signifies a giant experiment. Reception of protection augmenting tools to assistance such actions will be contingent upon the survival of unchanging methods for taking care of personal information and on methodological guidelines which could assistance to confirm compliance with legal and monitoring structures or frames.

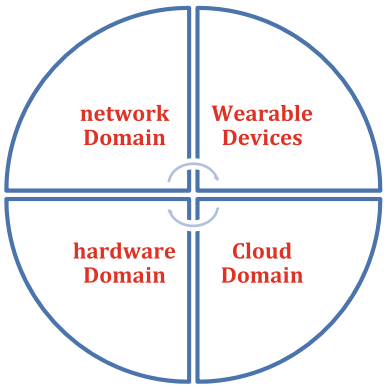


Fig. 11.5 Collaboration amongst IoT and Healthcare Services

The difficult part in E-healthcare applications is that on the integration of wearable devices and IoT which more technical issues to be sorted out are illustrated as follows.

11.12 Analysis of Integration of WIBST and IoT Attained from This Arduous Study

Wearable And Implantable Body Sensor Network is a mingling of remarkably low-power and wireless hubs of a sensor that are basically used to administrate the human body functionalists and the earth around the patient. Since WIBSN hubs are utilized to gather touchy (life-basic) data and may work in unfriendly situations, in like manner, they require exacting security instruments to counteract pernicious collaboration with the framework [37]. And so as to maintain a strategic distance from mistakes severe systems to execute security conventions are made accessible.

11.12.1 Security Requirements

Security is the utmost imperious features of several systems. In broad way, security is a perception related to protection measurements. Currently, the communication in sensor network solicitations healthcare are frequently addressed in wireless mode [38]. In this section, some of the key security requirements in IoT based healthcare system using WIBSN have been described.

- **Data confidentiality**: Like Wireless Sensor Network, data security is supposed to be the greatest authoritative problem in WIBSN. It is mandatory to safeguard the data from coverage. WIBSN should not to discharge patient's imperative information to external or neighboring frameworks. In IoT-based human administrations application, the sensor centers assemble and propel fragile data to a coordinator. An adversary can listen stealthily on the correspondence, and can get essential information. This listening stealthily may make outrageous mischief the patient since the adversary can use the got data for some unlawful purposes.
- **Data consistency**: Retaining data arranged does not defend it from external changes. The aim of the opponent can just alter the data by including a couple of parts or by controlling the data inside a group. This balanced data can be sent to the facilitator. Non-appearance of unwavering quality instrument is a portion of the time amazingly risky especially if there ought to be an event of life-essential (when emergency data is changed). Terrible condition may likewise prompt extreme information misfortunes.

- **Data novelty**: The enemy may from time to time get data in travel and replay them later using old key in progressively prepared to perplex the organizer. Data freshness surmises that data is new and no one can replay the old message.
- **Authentication**: It is a defender amid the peak basic necessities in any IoT based medicinal services structure using WIBSN, which can successfully deal with the mirroring ambushes. In WIBSN based human administrations structure, all the sensor centers send their data to a facilitator. By then the coordinator sends discontinuous updates of the patient to a server. In this particular circumstance, it is significantly fundamental to ensure both the character of the facilitator and the server [13]. Authentication primarily helps in keeping up the individuality of every particular client.
- **Privacy**: An increasingly attractive property of the anonymity is the unrecognized one, which guarantees that the enemy can neither perceive who the patient can recognize whether two discourses begin from same cloud calm [14]. Along these lines, mystery covers the wellspring of a bundle in the midst of remote correspondence. It is an administration that can engage mystery.
- **Harmless Localization**: Most WIBSN applications require precise estimation of the patient region. Nonattendance of systems which are keen empowers an adversary to send in right reports about the patient region by declaring false banner qualities. Presently, with a particular true objective to ensure a safe IoT-based human administrations structure using BSN [39], it is essential that the system should speak to all the previously mentioned security requirements. Further at last it can contradict diverse security threats and strikes like data modification, emulate, spying, replaying, etc. Table 11.1 explains the Security Requirements of IoT and WISBN.

Table 11.1 Security Requirements of IoT and WISBN

Security Requirements	Characteristics
Data confidentiality	– It is mandatory to safeguard the data from coverage. WIBSN should not to discharge patient's imperative information to external or neighbouring frameworks. I
Data consistency	– Retaining data arranged does not defend it from external changes
Data novelty	– Data freshness surmises that data is new and no one can replay the old message
Authentication	– It is a defender amid the peak basic necessities in any IoT based medicinal services structure using WIBSN, which can successfully deal with the mirroring ambushes. In WIBSN based human administrations structure, all the sensor centers send their data to a facilitator
Privacy	– An increasingly attractive property of the anonymity is the unrecognized one, which guarantees that the enemy can neither perceive who the patient can recognize whether two discourses begin from same cloud calm
Harmless Localization	– Applications require precise estimation of the patient region. – To ensure a safe IoT-based human administrations structure using BSN, it is essential that the system should speak to all the previously mentioned security requirements

11.12.2 Practical Challenges in IoT and WISBN

Some of the practical challenges are represented below in Fig. 11.6 and describes below.

- **Memory space**: A novel WIBSN ought to deliberate the limited memory space of biosensors very, which possibly impacts the cryptography intention with computational unpredictability and keys system.
- **Computational competence**: On account of the constrained memory and the necessity of low vitality utilization of biosensor with limited computational ability and lightweight calculation.
- **Energy ingestion**: It is an imperative issue for biosensor hubs, which should be negligible, since biosensor hubs are fueled by exceptionally little batteries with lower utilization to work for an extensive stretch of time. Accordingly, any security system for BSNs ought to be planned cautiously.
- **Minutest delay**: An important strategy standard in the WIBSN security contrivance is competent to minimize delays in order to observe with WIBSN requirements.
- **Communication overhead**: Through the cause of the restricted data transmission accessible in a WIBSN, low communication overhead is prerequisite. For illustration, secure WIBSN setup must be done in less than 1 s and the most extreme suitable time for ECG (electrocardiogram) transmission is 200 ms [40]. Crisis circumstances in a WIBSN that requires the ability for quick restorative response without debilitating security. Cryptographic calculations utilized by these hubs must be straightforward so as to bring down calculations intricacy. In

Fig. 11.6 Practical challenges in IoT and WISBN

addition, if the message confirmation or encryption (decoding) components are not rather quick, a foe may dispatch a DoS assault to debilitate the assets of lawful biosensor hubs and make them less fit for completing their planned capacities. Yet, most normally utilized cryptographic systems are in-feasible in BSNs, for instance open key cryptosystems.

Because of the elusive standard for the WISBN biosensors gather and the communicate highlight of the remote channel biosensors use to convey, WIBSNs possibly face a ton of security dangers. These dangers get from two sources: outside assaults and inner assaults. Outer foes can listen stealthily on all traffic inside a WIBSN, If outside enemies are fruitful, they not exclusively can attack a client's Sensitive micro data yet additionally can stifle real data or supplement a fake biosensor hub into the WIBSN.As pursues, the distinctive methods for dangers in a WIBSN have been illustrated below in Fig. 11.7 and explains in well manner.

- **Interception (Eavesdropping)**: The problematic issue in WIBSN is to abstain from being listened in wherever by mysterious stabbings or attacks. On the off chance that an aggressor can pick up the sensitive micro data transmitted in a WIBSN, it is probably going to be utilized malevolently.
- **Communication Interruption**: Communication interruption consequences are the crushing of a part of a remote terminal or a component of WIBSN. It affects the season of a battery sent in each WIBSN to live, which likewise decrease the communication rate. It can result in a Dos assault. Under the condition of a client's crisis, these dangers are probably going to execute one's life at the very least

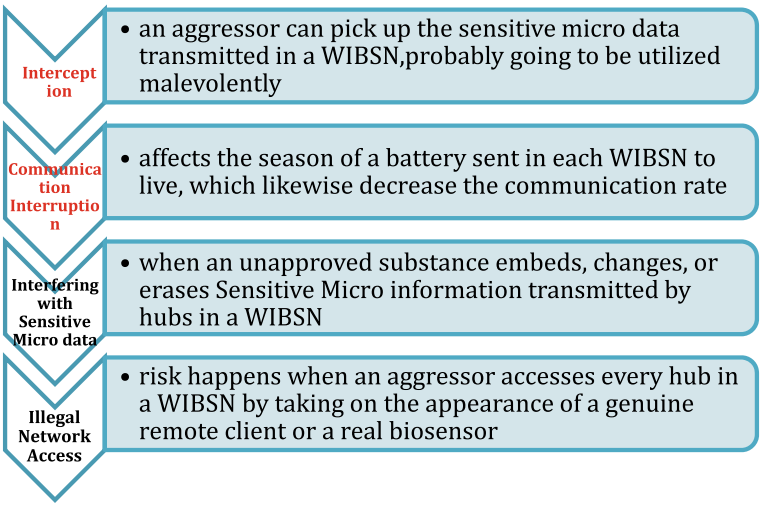


Fig. 11.7 The distinctive methods for dangers in a WIBSN

- **Interfering with Sensitive Micro data**: This happens when an unapproved substance embeds, changes, or erases Sensitive Micro information transmitted by hubs in a WIBSN. This is an assault on uprightness and can result in a Dos assault or man in the center assault. For instance if the human services information of a client is adjusted, doctor may influence a wrong finding and end to up with a mistake decision, which will breathe life into a genuine mischief of clients in a WIBSN and emergency clinic or clients will endure a gigantic misfortune.
- **Illegal Network Access**: This risk happens when an aggressor accesses every hub in a WIBSN by taking on the appearance of a genuine remote client or a real biosensor. This can result in port checking and being assaulted by a malware.
- **Refutation**: This danger happens when a sender or collector denies the way that it have transmitted or gotten sensitive micro data in a WIBSN individually. In electronic therapeutic, this danger must be expelled for a sheltered treatment in a WIBSN.

The summary and conclusion is explained in the following section.

11.13 Summary and Conclusion

This chapter presented some research perspective on applications of IoT in Body Area Sensor Network. The aim of this chapter has been fulfilled by means of attaining four objectives. At first, learning and evaluation of IoT supported parameters such as hardware and cloud platforms have been studied to find the suitability for e-health care services. Secondly, analysis of existing IoT based wearable's solutions for e-healthcare has been done. Thirdly, identification of encounters related has been analyzed with IoT aware e-health care domain. Finally integration of WIBST and IOT has been attained from this arduous study. In all, the proposed wearable sensor nodules or nodes could be attached to different positions of the humanoid body to measure physical signals like the temperature, pressure, pulse rate, ECG. Furthermore, it also detects fall condition using the accelerometer sensor node by providing an emergency notification. In the later portions of the chapter accommodates the IoT in cloud platform for e-healthcare, practical challenges and the security challenges cum thread of IoT and Body Area Sensor Network. From the analyses of all it is inferred that the goodness such as instantaneous recording and observing, end-to-end connectivity and affordability, data collection, tracking and alerts and remote medical assistance have been now well improved. Some challenges must be met out like Data security and privacy, integrating multiple devices and protocols and cost-effectiveness to meet about the applications IoT in healthcare, for example sinking emergency chamber interval time, Following patients, staff, and catalog, Augmenting drug controlling, and Guaranteeing obtainability of dangerous hardware.

References

1. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
2. Somatic data blood glucose collection transmission device for internet of Things, Google Patents, 2013. CN Patent 202,838,653. http://www.google.com/patents/CN202838653U?cl=en
3. Rathee, A., Poongodi, T., Yadav, M., Balusamy, B.: Internet of things in healthcare wearable and implantable body sensor network. In: Soft Computing in Wireless Sensor Networks, pp. 126–148. Taylor and Francis (2018)
4. Darwish, A., Hassanien, A.E.: Wearable and implantable wireless sensor network solutions for healthcare monitoring. Sensors (Basel). **12**(9), 12375–12376 (2011)
5. Hamdi, M., Boudriga, N.: Secure wearable and implantable body sensor networks in hazardous environments. In: Proceedings of the International Conference on Data Communication Networking and Optical Communication Systems, pp. 85–92 (2010)
6. Moosavi, S.R., Gia, T.N., Rahmani, A.M., Nigussie, E., Virtanen, S., Isoaho, J., Tenhunen, H.: SEA: a secure and efficient authentication and authorization architecture for IoT based healthcare using smart gateways. Procedia Comput. Sci. **52**, 452–459 (2015)
7. Hurtado, N.M.C., Zarifi, M.H., Daneshmand, M., Llobet, J.A.: Flexible micro displacement sensor for wearable/ implantable biomedical applications. IEEE Sens. J. **17**(12), 3873–3883 (2017)
8. Liao, Y., Leeson, M.S., Higgins, M.D., Bai, C.: Analysis of in-to-out wireless body area network systems: towards QoS -aware health internet of things applications. Electron. **5**(38) (2016). https://doi.org/10.3390/electronics5030038
9. Harshitha, S.R.P., Narramneni, P., Raghavee, N.S.: Body sensor using internet of things (IOT). ARPN J. Eng. Appl. Sci. **13**(8), 2916–2922 (2018)
10. Rishani, N.R., Elayan, H., Shubair, R.M., Kiourti, A.: Wearable, epidermal and implantable sensors for medical applications. arXiv:1810.00321v1 [eess.SP] (2018)
11. Samie, F., Bauer, L., Henkel, J.: An approximate compressor for wearable biomedical healthcare monitoring systems. In: Proceedings of the 10th International Conference on Hardware/Software Co-design and System Synthesis, pp. 133–142. IEEE Press (2015)
12. Chang, V., Kuo, Y.-H., Ramachandran, M.: Cloud computing adoption framework: a security framework for business clouds. Future Gener. Comput. Syst. **57**, 24–41 (2016)
13. Jansen, W., Grance, T., et al.: Guidelines on Security and Privacy in Public Cloud Computing, pp. 10–16. NIST Special Publication (2011)
14. Suo, H., Wan, J., Zou, C., Liu, J.: Security in the internet of things: a review. In: International Conference on Computer Science and Electronics Engineering (ICCSEE). IEEE, pp. 648–651 (2012)
15. Istepanian, R., Hu, S., Philip, N., Sungoor, A.: The potential of internet of mhealth things m-iot for non-invasive glucose level sensing. In: 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 5264–5266 (2011)
16. https://www.rxlist.com/ryzodeg-drug.html
17. Provenzano, V., Guastamacchia, E., Brancato, D.: Closing the loop with OpenAPS in people with type 1 diabetes—experience from Italy. Diabetes **67**(1) (2018). https://doi.org/10.2337/db18-993-P
18. https://www.asthma.org.uk/connectedasthma
19. Latuszynski, D.K., Schoch, P., Qadir, M.T., Cunha, B.A.: Roteus penneri urosepsis in a patient with diabetes mellitus. Heart Lung **27**(2), 146–148 (1998)
20. https://www.sensimed.ch/sensimed-triggerfish
21. Culpepper, Larry, Culpepper, Larry, Muskin, Philip R., Stahl, Stephen M.: Major depressive disorder: understanding the significance of residual symptoms and balancing efficacy with tolerability. Am. J. Med. **128**(9), S1–S15 (2015)

22. Lee, S.I., Park, E., Huang, A., Mortazavi, B., Garst, J.H., Jahanforouz, N., Espinal, M., Siero, T., Pollack, S., Afridi, M.: Objectively quantifying walking ability in degenerative spinal disorder patients using sensor equipped smart shoes. Med. Eng. Phys. **38**(5), 442–449 (2016)
23. Yao, J., Feng, B., Zhang, Z., Li, C., Zhang, W., Guo, Z., Zhao, H., Zhou, L.: Blood coagulation testing smartphone platform using quartz crystal microbalance dissipation method. Sensors (Basel) **18**(9), 1–12 (2018)
24. https://www.apple.com/healthcare/apple-watch
25. Fanucci, L., Saponara, S., Bacchillone, T., Donati, M., Barba, P., Sánchez-Tato, I., Carmona, C.: Sensing devices and sensor signal processing for remote monitoring of vital signs in chf patients. IEEE Trans. Instrum. Meas. **62**(3), p553–p569 (2013)
26. Constant, N., Douglas-Prawl, O., Johnson, S., Mankodiya, K.: Pulse-glasses: an unobtrusive, wearable hr monitor with internet-of-things functionality. In: 2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN). IEEE, pp. 1–5 (2015)
27. Pharow, P., Blobel, B.: Mobile health requires mobile security: challenges, solutions, and standardization, Stud. Health Technol. Inform. **136** (2008)
28. Li, Y., Chen, X., Tian, J., Zhang, X., Wang, K., Yang, J.: Automatic recognition of sign language sub-words based on portable accelerometer and EMG sensors. In: International Conference on Multimodal Interfaces and the Workshop on Machine Learning for Multimodal Interaction, pp. 17–21. ACM (2010)
29. Ng, W., Lau, H.-L.: Effective approaches for watermarking XML data. In: International Conference on Database Systems for Advanced Application, pp. 68–80. Springer, Berlin (2005)
30. Vilamovska, A.-M., Hatziandreu, E., Schindler, H.R., van Oranje-Nassau, C., de Vries, H, Krapels, J.: Study on the requirements and options for RFID application in healthcare (2009)
31. Kalantarian, H., Motamed, B., Alshurafa, N., Sarrafzadeh, M.: A wearable sensor system for medication adherence prediction. Artif. Intell. Med. **69**, 43–52 (2016)
32. Kumar, P., Verma, J., Prasad, S.: Hand data glove: a wearable real-time device for human-computer interaction. Int. J. Adv. Sci. Technol. 41–52 (2012)
33. Jara, A.J., Zamora-Izquierdo, M.A., Skarmeta, A.F.: Interconnection framework for mhealth and remote monitoring based on the internet of things. IEEE J. Sel. Areas Commun. **31**(9), 47–65 (2013)
34. Sokol, M.C., McGuigan, K.A., Verbrugge, R.R., Epstein, R.S.: Impact of medication adherence on hospitalization risk and healthcare cost. Med. Care **43**(6), 521–530 (2005)
35. Granados, J., Rahmani, A.-M., Nikander, P., Liljeberg, P., Tenhunen, H.: Web enabled intelligent gateways for ehealth internet-of-things. Internet of Things, User-Centric IoT, pp. 248–254. Springer, Berlin (2014)
36. Tamura, T., Kawarada, A., Nambu, M., Tsukada, A., Sasaki, K., Yamakoshi, K.-I.: E-healthcare at an experimental welfare techno house in Japan. The Open Med. Inform. J. **1** (1), 1–7 (2007)
37. Pirouzan Group. Available at http://pirouzansystem.com/
38. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. **57**(10), 2266–2279 (2013)
39. Hossain, M.S.: Cloud-supported cyber–physical localization framework for patients monitoring. IEEE Syst. J. **11**(1), 118–127 (2015)
40. Bortolotti, D., Mangia, M., Bartolini, A., Rovatti, R., Setti, G., Benini, L.: An ultra-low power dual-mode ecg monitor for healthcare and wellness. In: 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, pp. 1611–1616 (2015)
41. Dubey, H., Monteiro, A., Mahler, L., Akbar, U., Sun, Y., Yang, Q., Mankodiya, K.: FogCare: fog-assisted internet of things for smart telemedicine. Future Gener. Comput. Syst. arXiv:1701.08680v1 [cs.DC]

Chapter 12
Securing Internet of Medical Things (IoMT) Using Private Blockchain Network

K. Anitha Kumari, R. Padmashani, R. Varsha and Vasu Upadhayay

Abstract A key initiative taken by Government of India in response to Prime Minister Narendra Modi's "Digital India" move is the formation of Internet of Things (IoT) ecosystem for smart healthcare. Any security flaw occurring during authentication with a centralized environment affects the connectivity of devices in the network and the transaction of data in IoT. As a solution, Blockchain technology emerges to use in IoT network for the betterment. The Internet of Medical Things (IoMT) is the collection of medical devices and applications that connect to healthcare IT systems. In IoMT environment, a private Blockchain network is created containing all the participants of a hospital including doctors, lab technicians, patients and clinical laboratories etc., There exists no necessity to carry the report by the patients during every visit, as the data is already available in the network. The data is completely decentralized to avoid failure, data loss and to provide faster recovery. Whenever a change is attempted by a third person in the database, a notification is sent to all the members of the group. Since this is a private Blockchain, it requires an additional level of authentication. Whenever any new person requires being a part of the network a document for proof is provided. The data is transparent, so any modification done by any member of the group will get notified to everyone. An additional level security can be provided for data transfer based upon the mutually agreed security parameter and any modification in database is accepted upon approval of all members. In addition, when a hospital is not able to provide any sophisticated treatment to the patient due to lack of medical facilities, recommendation is sent to the patient; thereby new hospital added to the

K. Anitha Kumari (✉) · R. Padmashani · R. Varsha · V. Upadhayay
Department of IT, PSG College of Technology, Coimbatore, Tamil Nadu, India
e-mail: anitha.psgsoft@gmail.com

R. Padmashani
e-mail: padmashani@gmail.com

R. Varsha
e-mail: varsharavichandran97@gmail.com

V. Upadhayay
e-mail: vasuupadhayaytech@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_12

private network after successful authentication to access patient's record. To access record, quantum key may be generated and distributed across the network.

Keywords IoMT · Private blockchain · Secure network · IoT

12.1 Introduction

Connecting computing devices that lie embedded in everyday objects so as to enable them to send and receive data through internet is called the Internet of Things (IoT). In this perspective, a failure in an IoT ecosystem affects a large number of devices, exposing huge amounts of data, both personal and of the community.

Blockchain is a decentralized methodology with cryptographically enabled functions for security purpose and distributed system of block of data that has inbuilt strength thus enabling secure real-time records. Since it provides security with a strong form of encryption standard, the attackers find it very difficult to access of data from IoT devices. Also, this dramatically reduces the chances of any single point of failure even if that network is quite populated. The most important advantage of using Blockchain is the elimination of middlemen. The data transactions between multiple networks that are recorded by machines with absolutely no human oversight and their custodianship can be tracked as well. In order to modify a block in the Blockchain, one would need a write-access to it but this would only be held by machines thus completely making humans unable to do any sort of tampering of the data with inaccurate information. With an increasing number of devices connected through IoT and a humungous increase in the volume of data involved day by day, the present day cloud storage and processing service would become unsustainable and inefficient in the long run. The distributed nature of Blockchain allows massive redundancy of data since data storage would be duplicated across the devices that make up the network and make the data closely available whenever one needs it without having to transfer it, thus cutting down on the time it would take to transfer data and also assures no disruption of business activity should a server be down, hence solving the problem stated above.

12.1.1 The Blockchain Technology

According to [1], Blockchain technology was mainly developed for bitcoin crytocurrencies. It is a public ledger system which is used for ensuring the reliability of the data. Bitcoins are publicly available money payment systems which basically revolve around the distributed ledger called the blockchain.

Even though based on the inferences it looks as if blockchain are highly reliable concept [2] has identified few challenges in the blockchain technology. They are:

Throughput which is very less when compared to Twitter and VISA transactions, Latency—The time taken for processing inside a bloc is comparatively very high when other similar implementations are taken into considerations, Size and bandwidth—More and more blocks gets involved in transactions which are very difficult to manage and process, Security—51% attack which basically means one single entity is responsible for the overall operation, Wasted resources—A large amount of time and resources are wasted by sending on a concept called Proof of Work where each participant of the transaction will be given with hash codes which acts as a cryptographic puzzles. These puzzles should be put together in order to read the proper message, Sometimes this feature acts as an authentication mechanism, Usability—User friendliness is not guaranteed, Versioning—When the blocks are divided into multiple chins in order to make the overall management simpler, all the chunks should follow the same version. Else it will be difficult to manage due to compatibility issues.

Generally speaking, Blockchain is a technology that enables recording of a transaction and also its storage. It is not centrally controlled, remains unchanged over time and this recording of peer-to-peer transactions is distributed and stored in a digital ledger made up of linked blocks of transaction. Just like a database, blockchain too stores information but majorly differs in the aspect that no central controlling device is used in Blockchain. The absence of a controlling entity like a bank or a government means that a number of nodes, say personal computers, form a network where the data is located. Obviously this data is available publicly but the accessibility of the data is restricted and this ensures security.

This was originally called block chain, getting its name from blocks since it is a growing list of records. These blocks are linked using cryptography. Each block consists of:

- A cryptographic hash of the previous block.
- A timestamp.
- Transaction data.

Hash value is calculated in each block in order to make sure that much of the data is not getting modified during a transaction. Timestamp is created for each event and gets appended along with the remaining contents. Timestamp plays a vital role whenever any authentication operation needs to be performed at any particular point of time. The transaction data involves the actual input whereas the remaining two acts as the metadata. Figure 12.1 shows how the data flows in blockchain architecture.

The computer science technologies see an exponential growth and it is very difficult to analyse the performance of each and every upgrades. But a researcher always finds new solutions to everyday problems partly with innovative ideas and sometimes reusing the ideas of existing techniques. The accuracy and performance of the existing systems does not match with the complex requirements of the real world. So there is always a need for a better solution when compared with the available solution. Apart from the computational requirement security also gives

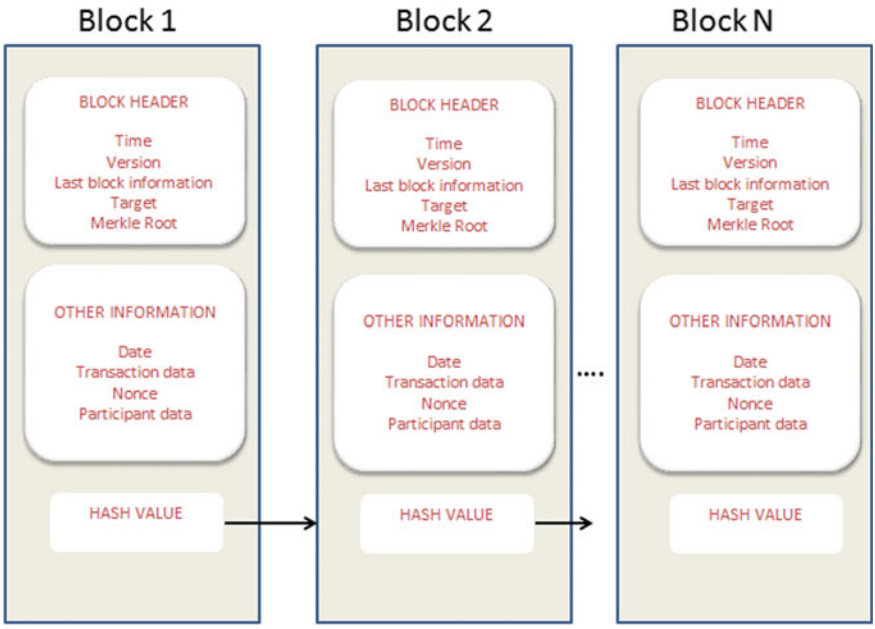


Fig. 12.1 Representation of blockchain

pressure from its side [3, 4]. Even though many high performance computing devices like GPUs are available, from the security point of view so many software and tools are available which easily trespasses the security premises of an organization. Security may not be an important concern for all applications. But for some applications security plays a vital role. One such area which requires high level of security is healthcare management. Multiple solutions are available in the market now. But they do not fully ensure that the data which the hospital servers maintain are completely safe. Because in the available solution in the market simply checks whether the data has been modified or not. But it does not say whether that modification was made by an authorized person or not. So the need of the hour is to have a system which notifies all the valid users of a system about the changes which takes place in an environment.

Blockchain is a recent trend which best suits the above requirement. It is a technology which takes care of both transaction states and the storage requirements. The highlights of this technology includes: no need for a centralized storage maintenance and is stored in a distributed environment in the form of digital ledgers. The data which is stored does not change frequently and is preceded by a series of transactions. This is similar to a traditional database management systems where in the data gets stored but differs in the way of storage. In a normal data management system, centralized database server stores all the information. But here, the data gets stored in a distributed fashion.

There is no specific entity like a government agency which maintains all the records. Blockchain technology makes sure that the data is accessible to everyone and it is very secure at the same time. This is always required for the general public as they do not prefer to stand in long queues in places like bank just to get the data alone. This feature of the blockchain makes sure that the data can be accessed even from their mobiles. Some of the features of blockchain which makes it unique from other existing systems include distributed data storage, immutable transactions and publicly available data.

12.1.2 Distributed Data Storage

In the database management systems currently available in the market, a centralized server will take care of the storage and retrieval of data. The data will be secured in this case but it cannot make sure that the data will be available to everyone who is in need of that. Another major drawback of this approach is that, when this centralized database server fails due to some technical issues, then the data cannot be retrieved back. These pitfalls in the system are overcome by blockchain technology.

The data is made available to everyone. The user can access the data using any devices like a personal computer, laptop, mobile phones etc. Also there is no single point of failure as the data is distributed and acts as a default backup mechanism. So even when the data fails or is getting deleted in one system, the remaining systems will take care of the failure and restores the backup copies. A simple distributed storage is shown in Fig. 12.2.

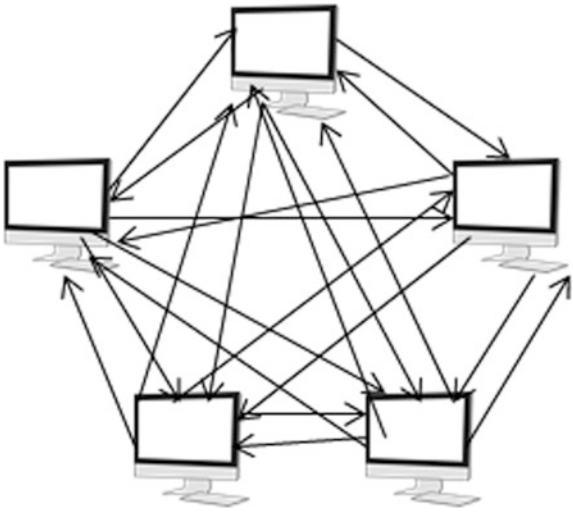


Fig. 12.2 Distributed blockchain

12.1.3 Immutable Transactions

The basic unit block in a block chain environment typically makes use of the cryptographic hash functions for securing the data. The user can make use of any hash function but for security purpose the user has to make sure that the hash value to be a little bit higher data so that it will be safe from Brute force attack. The logic used in the blocks is, whenever any data is transmitted in a blockchain the hash value is calculated using any strong cryptographic algorithm. Whenever an unauthorized person tries to tamper with the data available in the blockchain, the hash value changes drastically by the phenomenon known as "Avalanche effect", wherein a single bit changes in the input changes multiple bits in the output and thereby changing the hash value. This gets notified to other blocks and hence violating the chain. This gives notification to all the users who are alerted about the changes taking place.

12.1.4 Publicly Available Data

The main objective of a blockchain technology is to make the data available to everyone. This also poses a serious impact on the security aspect of the network premise. So in order to maintain the privacy of the data, instead of displaying the actual names of the user, some unique numeric codes are generated and are sued as an alternate for the users' actual name. In general, the blocks contain information about the past to execute the present data and predicting the future.

12.2 Types of Blockchain

Different types of block chain are available. But they can be broadly classified into:

1. Private Blockchain
2. Public Blockchain
3. Consortium Blockchain.

12.2.1 Private Blockchain

In this type, a central authority takes the sole responsibility to carry out overall management. He does not store all the information in a centralized location. Rather he maintains the transactions alone. But the data get stored in a distributed fashion only. The users of the system are not expected to possess high performance

computing devices. Rather the central authority eases the work of the user by performing the calculations in their side itself.

In a private Blockchain, write access is given to only one person or organization whereas the read access is either restricted or public. Example applications include database management, auditing, etc. which are internal to a single company, and so public readability may be undesirable. Private Blockchain takes the actual advantage of Blockchain technology by forming groups and participants who can verify transactions internally. A private Blockchain runs the risk of security breaches just like in a centralized system. They may scale better and comply better with governmental data security and privacy regulations. Examples of private Blockchain include MONAX and Multichain. A representation is shown in Fig. 12.3.

Nature and characteristics of private Blockchain:

- Reduction in transaction costs and data redundancies
- Simplified data-handling and more automated compliance mechanisms.

12.2.2 Public Blockchain

All the data are publicly available to anyone who is a part of the blockchain network as shown in Fig. 12.4. Anyone who is registered in the network can add new record, modify existing record, and even delete the record. Even though the data is publicly available, security is also guaranteed, by making sure that data dos not gets modified wrongly. But this kind of architecture is not suitable for all kind of application. This may be suitable for those areas where sharing of resources alone is required and verification of the content is not mandatory.

Whoever wishes to initiate or want to be a transaction can download the code and start running a public node on their local device, validating transactions in the network and participating in the agreement process. This gives anyone the right to

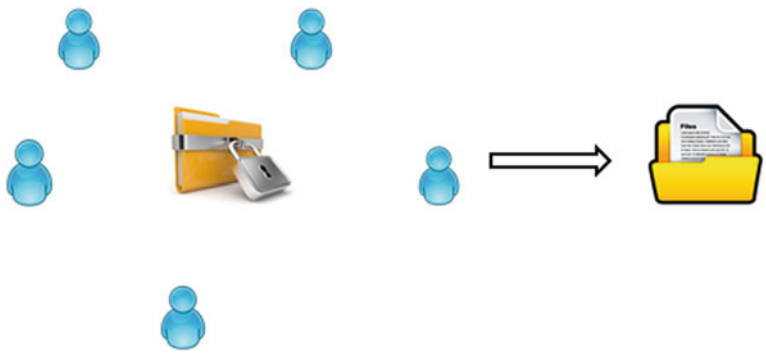


Fig. 12.3 Private blockchain

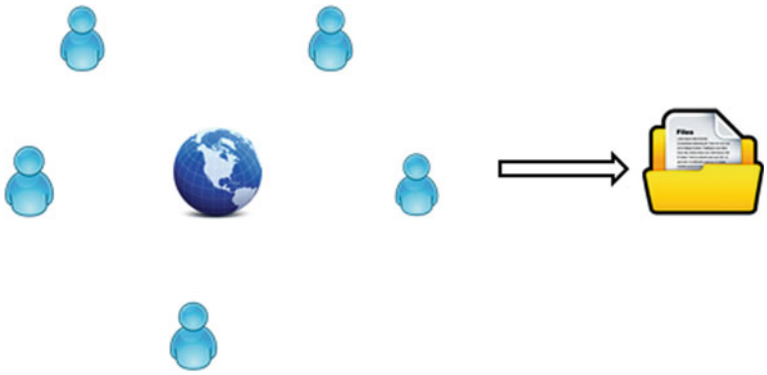


Fig. 12.4 Public blockchain

participate in the process that determines which blocks get added to the chain and what the current shape and size of the Blockchain is. Anyone can transact in the network. The transactions should go through as long as they are valid. Anyone can access and read transactions using a block explorer. Transactions are transparent but anonymous. Several state-of-the-art public Blockchain protocols based on Proof of Work consensus algorithms are open source and not permission. It simply implies that anyone can participate, without permission. Examples include Bitcoin, Ethereum, Monero, Dash, Litecoin, etc.

This nature of the public Blockchain has two major implications.

- Everyone bears the potential to disrupt current business models through disintermediation.
- Distributed infrastructure costs: no need to maintain servers or system admins radically reduces the costs of creating and running decentralized applications DApps).

12.2.3 Consortium Blockchain

It is also called semi private blockchain. It is a variation of public blockchain wherein not all the data available are made as public. Rather the availability of the data is decided by the rights they have. For example, doctors may have higher privilege to access all the records whereas the patient may not have access to all the data like they have limited access to some confidential information. Bitcoin is one important example for this type of blockchain.

- In a consortium network, the power does not reside with a single authority. It is operated under the leadership of a group. So, a consortium Blockchain is private for a group of companies or entities.

- Unlike Public Blockchain network, Consortium network does not allow any person with the Internet connection to participate in the process of verifying transactions.
- Consortium Blockchain are faster and provides higher scalability and transaction privacy. Consortium Blockchain are mostly used in the banking sector.

The consensus mechanism is maintained by a pre-selected set of nodes. Typically, these nodes would be from all the entities forming the consortium.

12.3 Working of Blockchain

Whenever a user wants to enter inside a block chain network, they will be provided with a private key and a public key pair. The user is identified using the public key. In order to see what the user has shared in the blockchain environment, the private key is mandatory.

Blockchain works on three main principles that are compiled and pave the way for security and safety in digital relationships. The three principles are:

- Shared ledgers or distributed ledgers—this is union of shared records. There is no 'one central authority' that has the responsibility of maintaining the ledger and all updates are done on the ledger on a real time basis. These updates are performed by the participants in the network and it takes a maximum of few seconds to see reflections of the changes in the ledger.
- Authentication—before even adding a transaction to the chain, the transactions are authenticated by means of validating and verifying them through algorithms and thus this technology is considered to be genuine. In addition to this, the authenticity of any particular transaction is sealed as soon as it has been encrypted, signed and stored digitally.
- The concept of private key cryptography—using a secret key as a variable in addition to encryption and decryption algorithms is called private key cryptography. The algorithm need not be a secret, and this public algorithm uses this key that is strictly kept secret. This is the concept used in Blockchain where the secret secure key is the reference of the digital identity and these transactions are on the open network.

Each page in a record exchange, or a ledger transaction, shapes a block. That block affects the following block or page through cryptographic hashing. As such, when a block is finished, it makes an exceptionally unique secure code, which tie into the following page or block, making a chain of blocks, or Blockchain. This form of working of blockchain ensures security on the users, making blockchain one of the most reliable forms of storage ever. This is illustrated in Figs. 12.5 and 12.6.

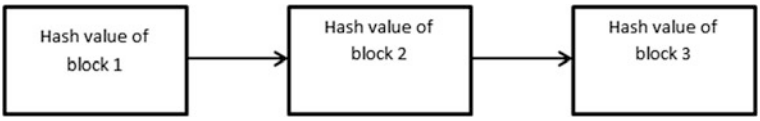


Fig. 12.5 Cryptographic hashing

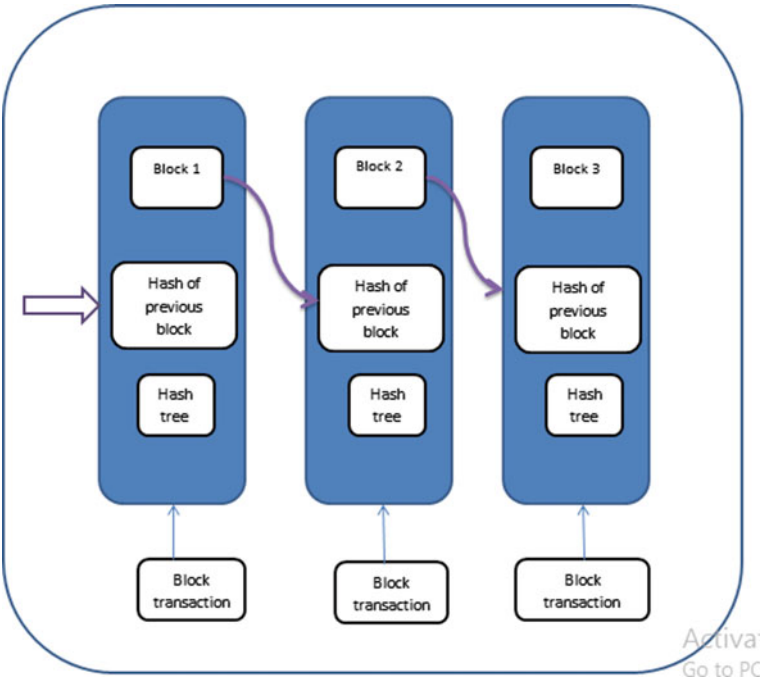


Fig. 12.6 A depiction of cryptographic linking of blocks in a blockchain

12.3.1 Steps Involved in Working of Blockchain

The following steps are followed when a blockchain is created and processed.

- A user, in need of a transaction, requests for one.
- In the network of blocks, one block is created for representing his transaction.
- Being a network of interlinked blocks, irrespective of whether it's centralised or decentralised, the newly created block is broadcasted to all the nodes of the network.
- Validation of the block then occurs. This, perhaps, is the most important factor in imparting security to a blockchain and prevents any form of infiltration. The validation is on the basis of majority decision. If majority of the nodes declare

the block valid, the next step is carried out. If not, the blocks not added to the chain. Thus, no outsider can be added/appended/included in the chain.
- Once the block is deemed to be valid, it is added to the chain. This means the previous block hash field of this node is updated to be the hash value of the last block currently in the chain. The block will be added after its hash is generated or computed.
- The transaction data in the block would then be executed after verification.

The steps in Fig. 12.7 give an overall view as to how blockchain works systematically. From the steps it can be deciphered that there can be safety and security assured. Also, hacking into blockchain would be virtually impossible. In order to hack a block, one must know the hash code of those blocks and it is extremely unlikely for the hash to be figured out. It is a lengthy code and the probability of finding it is very low. Even if done, the timestamp would give away the intrusion and hash would also regenerate, thus making any undesired activity to be excluded since the nodes that can access it would become aware of such an intrusion.

12.3.2 Attesting Data in Blockchain

The data that is stored A distributed ledger (a "blockchain") empowers everybody in the system to have a similar wellspring of truth about which accreditations or credentials are legitimate and who confirmed the legitimacy of the information inside the certification, without uncovering the real information or the actual data. Only references and the associated attestation of a user's legitimate credentials are entered on the ledger.

Steps: The following steps are carried out while attesting ay data in the blockchain.

- A third party service verifies the user credentials.
- These credentials, once verified, are placed on a blockchain (digital pointer).

Thus, this acts as the database holding all user details which help in authentication. The best analogy would be the usage of this database to check against the user details entered on a, say, login form.

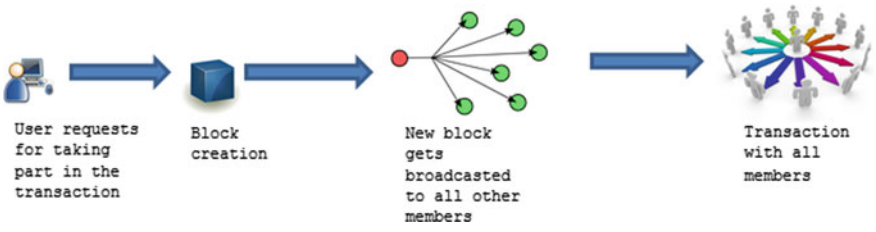


Fig. 12.7 Steps involved in working of blockchain

- An institution asks a user to provide identity credentials.
- Provided identity credentials are checked against the blockchain.
- If the records provided match the records on the blockchain, the user's identity is said to be verified, or attested.

12.4 Current Healthcare Systems

Healthcare system plays a vital role in our day to day life especially for old age people. In the recent days, a hospital visit by an old aged person has become a customary one. The hospital system requires the patient to do a lot of tests just to make sure that they are perfectly fit. The records needs to be maintained properly else the tests which were performed should be done repeatedly which ultimately results in wastage of money and the health of the patient.

The main objective of any healthcare management system is to provide high quality service to the patients. But this has become a very tedious one because of the ardent rules and laws imposed by the government and the hospital management. One cannot always ensure that the service provided by the provider is always satisfactory. Sometimes the patient and the hospital cannot have a direct contact rather they go through an intermediate person. That person cannot be relied upon all the time. Sometimes if money is going to be the motive of the person, then his main objective will be making money and not on providing a quality healthcare service.

The crucial part of any healthcare management system is patients' medical record. This data is distributes among many systems and hence makes the process of accessing the data very difficult. Proper exchanging of the information is also not done properly in the current system. This creates a big gap which needs to be filled out by making use of proper mechanisms.

The healthcare organizations store the reports of the tests and other procedures locally in the respective hospital servers. This might be easy from the hospital point of view. But they face a very serious flaw from the patients' view since they need to perform the tests again and again if they are not satisfied with the diagnosis and the treatment given by the hospital. This is really a time consuming procedure for the patient. The doctors also face issues if they are not able to diagnose the disease properly because of missing data in the reports. The maintenance of the records is also a very expensive procedure for a hospital management.

Any healthcare system ultimately keeps patient health management as a priority and focusses on providing quality health services. But providing these become extremely arduous and lengthy with several regulations and laws being imposed. There is a huge gap between the payers and providers which is a major setback in providing quality health service. To make matters worse, there exists a dependency on the intermediaries in the supply chain. Data about the patients is critical and these are scattered across systems and this makes the data inaccessible and not handily available. The absence of a smooth process management renders this

existing healthcare system incomplete. It can also not handle information exchange which makes it inadequate and in need of huge changes.

The healthcare organizations still make use of outdated systems which house patient data. They can cover the functionality of storing the patient data locally but makes life difficult for medical practitioners during the time of diagnosis. It would be time consuming and tedious from patient perspective as well. This considerably increases the cost of maintenance of these businesses. The healthcare system thus obviously needs a better system to deliver appropriate patient care and high quality health care. But these organizations are wary of the huge misuse of data that could cause lot of trouble because of any breach.

So there is always a need of the system which takes care of the flaws discussed above but at the same time should take care of two major issues: money and security. Small hospitals will not be having enough revenue to invest in servers to maintain the records. On the other hand multispecialty hospitals have enough money to buy servers but sometimes they are not able to provide quality service to the patients. This is because when any security breach in the security premise, the data are prone to leakage and there won't be any privacy to the patients 'data.

Some of the issues face by the current scenario is:

- Part of the data available in the servers is either missing or erroneous.
- Proper recording of the reports are not done properly. Sometimes the entry might be made by a newbie who does not have any prior experience.
- Apart from identifying a breach in the system, the recovery cost is costly and may increase in future.

In the current healthcare system faces many issues and they need a system which performs better. For example, a pharmaceutical company might have patented a new medicine. Initially the cost might be little bit higher. So some fraudulent companies which want to make money might produce similar medicine with similar name and appearance and release the same into the market at a very low cost. People tend to be get attracted by such product as they do not want to spend money on a similar costly product. This results in a very big loss to the company. Many do not find this as a very dangerous issue. Counterfeiting the drugs is an important issue to be taken care of. Unless and until there is no problem arising, the fraudulent company goes on with the production. If in case a massive death rate occurs in a particular, after consuming the fraudulent medicine, there the issue starts. The authorized manufacturer of the medicine might face some legal issues. If the supply is tracked properly, then these kinds of issues might be eradicated to a considerable extent.

As of December 2018, a survey revealed the following:

- These fraudulent activities take place mostly in China and India.
- According to Word Heath Organisation, either the drugs contain wrong components or it contains wrong composition of the components.
- A total of 200 billion dollars is involved in this per year

- Out of this, a major portion of income comes through the ales of the drugs through internet.
- This involves a coverage of 30% of the rugs sold worldwide.

It is not the fact that simply manufacturing fake medicine is illegal. This in turn might result in many other serious issues [5]. The patients may buy such fake medicines unknowingly. No proper guarantee can be given that the medicines might cure the diseases in all the cases. Sometimes taking a contaminated or wrong medicine for a prolonged period might result in many serious ailments. This is because the companies do not mix the ingredient in proper proportions. The way in which these medicines are administered to the patients might differ from one company to another.

Also this results in a huge loss to the nations' revenue. Millions of dollars are involved in this sector. Also there will be recession in this area as the companies do not need so many employees. Blockchain can be used here to solve this problem [6–11]. Another persistent difficulty in today's healthcare system is Health Information Exchange. Even though many fraudulent companies make money out of this business, the one who is directly affected is the patient. They actually do not have any idea about what is happening in the background. The details about the patient are leaked out and sometimes they are sold out for research purpose. They don't have any idea about what data is stored, where it gets stored, how it gets stored and who stores it. The mere presence of technologies and cutting edge gadgets in the healthcare facilities does not provide means of collection, analysis and seamless data exchange. Thus, today's healthcare system needs a system that is efficient in terms of both economy and usage, smooth in functioning and also transparent. All this paved way for the introduction of a technology in the healthcare system, the Blockchain.

Patient health data management is difficult because of two main issues in the healthcare industry.

- First, each patient is unique therefore there can be no such thing as a common disease or common treatment strategy. So what works on a patient might not work on the other and vice versa due to inter-individual variability. Hence, there is a need to access the complete medical records in order to adapt the treatment and provide personalised care. All in all, healthcare is becoming more and more patient-centred and thus more and more specific ad patient data oriented.
- Second, sharing information among the medical community is a major challenge.

Even today, doctors use social networks to communicate and share patient data. Medical data is sensitive and should always go through secured networks when revealed. The lack of any sort of secure structure to share data is an important obstacle for scientific advancements. Though medical records are kept in very different locations without having a common database sounds secure, this derails scientific advances since only on allowing the researchers to access the data there

can be a heavy contribution to scientific advances worldwide especially when it comes to rare diseases or minorities.

12.4.1 Requirement of Current Healthcare System

Through Blockchain, it is possible to have a single common database of health information that enables sharing after creation. The stakeholders who get benefited from this are the doctors, patients and pharmacists. They data are easily available and easily accessible. Even though it looks very simple, no compensation is done from the security point of view. Patients are the one who gets benefited more using this as the doctors will be able to diagnose the diseases properly. Also the doctors will be able to study the root cause of a disease properly. They may be able to identify the pattern of the disease and may predict what new disease may merge in the future. Many researches can be carried out based on the data which is easily available and many productive results and invention can be expected based on the analysis.

In the current healthcare system, lot of issues prevail. With passing of time, they only seem to grow and hence there is an unprecedented need for an advanced technical system. To denote a practical example, counterfeiting of drugs is a major problem in the supply chain. This is a growing pharma fraud wherein a drug is produced and sold deceptively, i.e. an aim to represent another drug in its authenticity or effectiveness. This emerging problem is serious and needs to be counter controlled since a lot of misdiagnosis and side effects can occur. This problem has caused companies millions of dollars in losses. If only there was a system in place that could accurately track features in the supply chain, this problem could be easily solved.

To have a better diagnosis, the data should be made available easily and also accessing the data should be at an ease. Also, if the data which belongs to one hospital is shared with other hospital in a blockchain based network, then all the above mentioned issues can be addressed. The patient data acts as a huge repository of information. It solely depends upon how the data is interpreted.

Through Blockchain, it is possible to have a single common database of health information that enables sharing after creation. This is the healthcare system that gives easy access to doctors, pharmacists and even patients at anytime and anywhere. Irrespective of the electronic medical system they use, this system would remain accessible across entities and in addition offers transparency and high security. This allows doctors to spend more time on actual patient care and treatment. Statistics would also improve, thus facilitating clinical trials and therapies for treatment of any diseases that are rare or unheard of. Doctors may find it difficult or even fail to catch those rare diseases but not the system.

To have treatments that are effective, diagnosis that are accurate and an ecosystem that is cost-effective, there has to be, between providers of healthcare solutions, a smooth sharing of data in the healthcare system. A lot of insights can be

discovered through patient data and the resources have to be properly utilized to make the most out of these insights from the patient data that is growing day by day.

12.5 Blockchain in Healthcare

A number of areas in the healthcare system can be benefitted through the application of blockchain. One of the important uses of blockchain in the healthcare industry is drug traceability to rule out drug counterfeiting. To better understand it with stats and facts, the below metrics revealed by the Health Research Funding organization helps. As of December 2018, a survey revealed the following:

- Counterfeit drugs make up of 10–30% of the total drugs sold in the developing countries.
- This market is worth 200 billion US Dollars annually.
- Out of this, 75 billion comes from internet sales of these counterfeit drugs.
- Most of these drugs are manufactured in either India or China.
- As of 2014, 60 different Pfizer medicines and products had been counterfeited.

According to World Health Organization, about 16% of the counterfeit drugs are composed of the wrong ingredients and 17% are composed of the wrong levels of necessary ingredients. The main issue with fake drugs or counterfeit drugs is not that they are fake. Rather, the main issue is that they can be very different from the original product in a quantitative and qualitative way. Even though many of them don't have the active ingredients they claim they do, this can be particularly dangerous for the patients that take these fake drugs since it won't treat the disease it was supposed to treat. In addition, the product can cause unexpected secondary effects if the ingredients and the dosages are different.

From an economic perspective, the drug counterfeiting industry brings about loss of billions of euros for the European pharmaceutical sector and tens of thousands of jobs are lost because manufacturers employ less people than they would if fake drugs didn't exist. Blockchain can be used here to solve this problem. Another pressing problem in today's healthcare system is Health Information Exchange. Identity thefts and mishaps are common in everyday life. But these happening on patient data are all the more worrying since it would pave the way for desperate patients to become victims to spamming and financial crimes. Patients have little to no control over their data and are completely blinded by the obliviousness of where their data is shared, what data is stored and who has access to it.

The mere presence of technologies and cutting edge gadgets in the healthcare facilities does not provide means of collection, analysis and seamless data exchange. Thus, today's healthcare system needs a system that is efficient in terms of both economy and usage, smooth in functioning and also transparent. All this paved way for the introduction of a technology in the healthcare system, the Blockchain.

Patient data management is difficult because of two main issues in the healthcare industry.

- First, each patient is unique therefore there can be no such thing as a common disease or common treatment strategy. So what works on a patient might not work on the other and vice versa due to inter-individual variability. Hence, there is a need to access the complete medical records in order to adapt the treatment and provide personalised care. All in all, healthcare is becoming more and more patient-centred and thus more and more specific ad patient data oriented.
- Second, sharing information among the medical community is a major challenge.

Even today, doctors use social networks to communicate and share patient data. Medical data is sensitive and should always go through secured networks when revealed. The lack of any sort of secure structure to share data is an important obstacle for scientific advancements. Though medical records are kept in very different locations without having a common database sounds secure, this derails scientific advances since only on allowing the researchers to access the data there can be a heavy contribution to scientific advances worldwide especially when it comes to rare diseases or minorities.

12.5.1 Population Health Data

Population health data refers to the statistical information collected among the population. The data collected should not be biased. Hence it is collected from diverse amount of people in order to maintain randomness. Forms will be circulated among the people and they do not want to reveal their names in the forms in order to hide their identity. For example, if a survey needs to be conducted which summarizes the possibility of giving birth to a chid for a married couple who are having age above 40 years, it is enough if the survey is conducted to couples who are above 40 years and need not cover those couples who are below 40 years. At the same time, it is not necessary to conduct the survey at the same state or country. It can even be conducted among different countries but restricted to that age group alone.

Security of the data is an important concern. If security alone is the man objective, then usually people who are maintaining the data will be storing the data in sophisticated servers. If this is the case then accessibility of the data becomes very a tedious task. Blockchain technology when employed in such an environment will be producing promising performance. Real-time implementation of such architecture is feasible and is easy to implement at a lower cost saving time.

Blockchain allows the participants to share their data freely and hence distributed among different participants. More number of patients is directly proportional to the increase in the number of records in the data sets. Emerging

technologies like Machine Learning, Deep Learning and Artificial Intelligence finds these datasets very useful as more number of researches can be performed on top of it. Many promising results and inventions can be expected from this. The pharmacy company also gets benefited from this in one way. Because whenever a new epidemic or a disease is about to breaks down in a particular area, then they have to come with new medicines to cure the disease. Precautionary measures can be taken by the government if in case the doctors are able to predict new diseases.

12.5.2 Secure Healthcare Setups

Existing hospital management systems currently stores the information in a centralized server making it very much prone to single point of failure. Whenever some unauthorized person gains access to this server, then there is no privacy to the data being stored. When this server is compromised by the outsider, chances are there for the attacker to change the data. Sometime he may release the data to some other companies for the sake of money.

This can be overcome with the help of Blockchain. It can help prevent this kind of internal threats. The idea would be to impose a number of independent actors in the organization. They would each have, not the same, but a different level of access on the Blockchain ledger. The access of these ledgers will come with encryption embedded within the blocks of the Blockchain. Thus the organizations are saved from external attacks and threats. The sort of problems ranging from ransom attacks to corruption of data to failure in the hardware would all be prevented with correct implementation of Blockchain in the healthcare organizations.

12.5.3 Clinical Trials

Health organizations conduct clinical trials so that any medicine that has been developed or proposed for a specific disease can be checked and analysed for its effectiveness. An initial hypothesis is formulated and the drug is tested based on the hypothesis. Based on the success level of the trial, large scale implementation of the drugs is done. This obviously means that huge data sets would be required to conduct these clinical trials. The researchers generate reports, ratio of the effectiveness of the drug, the statistics and so on by conducting regular tests, focussing on these data sets. These reports are used to analyse the data which then become major deciding factors.

The results produced by the pharmaceutical companies are not satisfactory. They project the results in such a way that the companies get benefited from them. No one is going to demand the company to show the list of experiments performed and the corresponding results. Even if someone moves to the court legally to demand the company to produce proper justification, they will not project proper results.

Authentication of the document is not done in most of the companies. Blockchain technology can be deployed in such a situation in order to have transparency of the data and more secure transactions. The overall transactions which take place right from the manufacture to dispatch of the documents to the patients should be made unbiased.

In order to achieve this, the procedure of manufacturing the medicine, the components used, the regulatory measures, related documents, and other details should be made available along with the timestamp. This will ensure that all the transactions are transparent and are easy for verification. This acts as the proof.

How blockchain can help: Blockchain provides verification of the document anywhere and anytime by anyone to make sure that the authenticity of the records is maintained properly. In order to insert new record inside a blockchain network some of the important nodes should provide approval. This procedure is applicable for modification of the record. If someone tries to modify the record without proper consent, then the results gets reflected in many nodes. So majority of the nodes gets notification even before the modified data reaches the clients and thereby saving from any major issues.

To store some record inside a block chain network, cryptographic hash function is applied to the data to be stored. Usually Secure Hash Algorithm (SHA256) is used for this purpose. This calculates unique hash code for each and every document. If any changes are made to the existing document, then it ultimately results in a different hash value. Key pairs are used to verify the document. Private key is used to check the content and public key is used to make sure that the user is already registered to the network and they are already verified by the network. So one can ensure that if any changes happen in the network, it is because of the insider and not from the outsider. Public and private keys are provided using a bitcoin wallet.

How verification is done: To verify whether the information the person has is similar to the original information stored on the blockchain, the person would go through the following procedure:

- Apply SHA256 algorithm over the data which they have it in their hand
- Compare the key pairs generated
- If the keys are the same as that of the existing ones, then it means that the data has been the same and is not modified.

Such a secure and transparent procedure makes sure that the research community can use this to a greater extent to produce good results, and they can even develop some standard protocols. This procedure will reduce the paper work, maintenance of the records for audit, document forgery and acts as a digitally verified document.

This can be achieved by having a simple catalogue of the above said documents. In addition, the supply chain management and accountability of drugs can be kept on track through the use of Blockchain technology.

12.5.4 Protection Against Counterfeited Drugs

One of the main objectives of using a blockchain is in the field of drug traceability. Since time stamping the product details has been mandatory in the aforementioned statements the drug details are easily traceable and easy to verify.

Out of the different type of blockchain architectures available, the private blockchain is a preferred choice. Here a central authority maintains all the records. A single point of failure is not there as the data is distributed but only a person monitors the flow of the transaction. Any company who wish to be a part of the network should register themselves in the network. They will be verified by this central authority in order to make sure that fake drugs are not registered. The manufacturers, distributors or the retailers act as the miners as decided by the pharmaceutical companies. Different rights are given to each person depending upon the position on the supply chain. Everyone in the blockchain network should work together to achieve the above mentioned purposes. In the current scenario, the transactions are not clear. So if any issue arises, then one will be blaming the other to claim responsibility for the issue. If everything is made transparent then the supply chain flow can be identified easily and the root cause of the problems can be identified easily. At the same it has to be made sure that the data are stored in a secure location. The complete list of transactions can be seen clearly as and when they get added to the network.

If in case any flaw in the product is identified by the company themselves then they can easily identify the block where the flaw has occurred and they can either modify or remove the bloc completely thereby avoiding any further damage to the system as well as to the stakeholders.

Thus, blockchain allows preventing two main issues surrounding drug traceability and thus counterfeited drugs. They are:

- Allowing companies track their products down the supply chain thus creating an airtight circuit impermeable to counterfeit drugs.
- Allowing stakeholders and labs to take actions on the event of occurrence of any problems by identifying the exact location of their drugs.

How this is achieved: A hash is generated when a drug is produced and this contains all the relevant information about the product. Upon each transaction, in this case, each time when the drugs move from one entity to another like manufacturer to the distributor, this information is store in the blockchain. This facilitates for easy tracking of the drug.

12.5.5 Patient Data Management

Blockchain also addresses the notion of data ownership. Currently patients are not given proper authentication as the data is not transparent. Lots of wearable's like smart watches are manufactured daily in the market which collects a lots of personal

information about the person. This is one of the major drawbacks as it does not allow the user to control their own data.

Privacy of the data of the patient needs to be maintained at the same time. Because when they store any information in a blockchain it means that they make the information public to all the participants of the blockchain network. One cannot deny saying that they cannot make their information public because only of all the information are made available then proper diagnosis can be done. This also helps in the medical insurance side. When someone claims for the insurance amount falsely, the company can in turn check the patients history and verify whether they have produced forged document or not. Data management becomes a major issue when such a huge amount of data has to be stored. The existing system is not capable enough to store the information at a faster phase. Blockchain comes into picture to solve this problem too.

How blockchain would help: Blockchain can provide a structure for data sharing as well as security.

In this particular use case, this is achieved as briefed below:

- Healthcare providers collect information from the patients such as their names, their date of births, procedures that have been performed on them and their prescriptions.
- The data is stored in the organisation's existing databases. In case of availability, they can also be stored on cloud computing systems or their systems or both.
- A hash is created from each source of data. This is redirected to the blockchain along with the patient's public ID.
- To manage patient data access, smart contracts are used.

There is an API through which healthcare stakeholders can query the blockchain which provides the location as to where the data can be found without revealing patient's identity. If needed, the patient can share his full medical record to these stakeholders with or without any identifiable data. The patient can decide to whom he gives access to and under what conditions. Once accessed, this data can be analysed and shared by the medical community and researchers alike. To elaborate, one of the main advantages of this technology applied in this particular use case is that it allows the patient to control the access he gives to his medical records.

The patient defines through a smart contract the conditions under which his or her data can be accessed on the blockchain. Moreover, all this will be done through an API and the patient will set the conditions on his or her profile.

- When the patient is conscious, the combination of the patient's private key and the provider's private key unlocks the access to the data.
- If the patient isn't conscious, one or more third parties, picked by the patient, give their permission before the healthcare provider accesses the data.

In addition, medical records are not the only source of data related to a patient. As IoT develops, wearable become an important source of information. This type of data could be used in the patient's interest to track his or her activities, set goals and even adapt treatments. Using smart contracts, all this can be done.

12.6 Conclusion

Blockchain technology has proven to be a revolutionary innovation in healthcare world. It provides a secure platform to encrypt and store patient's records digitally in the ledger that can be accessed only by the authorized person thus protecting the patient's identity from outside sources. This enables secure storage, automates administrative process, secure transfer of information, and improves care for patients. Smart contracts can also be employed between patient and doctor to ensure credibility. Thus this chapter provides an eye opening for use of Blockchain in healthcare sector as, the prime need of a smart healthcare begins with security and security begins with Blockchain.

References

1. Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K.: Where is current research on blockchain technology? A systematic review. PLoS ONE **11**(10), e0163477 (2016)
2. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media Inc., Sebastopol (2015)
3. Anitha Kumari, K., Sudha Sadasivam, G., Rohini, L.: An efficient 3D elliptic curve Diffie-Hellman (ECDH) based two-server password-only authenticated key exchange protocol with provable security. IETE J. Res. T & F **62**(6), 762–773 (2016)
4. Anitha Kumari, K., Sudha Sadasivam, G.: A Comparative Analysis of Classical Cryptography vs. Quantum Safe Cryptography, Medical Big Data and Internet of Medical Things: Advances, Challenges and Applications. CRC Press, Boca Raton (2018)
5. Thomson, L.L.: Health care data breaches and information security addressing threats and risks to patient data. In: Data Breach and Encryption Handbook, pp. 57–85 (2012)
6. Cichosz, S.L., Stausholm,M.N., Kronborg, T., Vestergaard, P., Hejlesen, O.: How to use blockchain for diabetes health care data and access management: an operational concept. J. Sci. Technol. **13**, 248–253 (2018)
7. Nugent, T., Upton, D., Cimpoesu, M.: Improving data transparency in clinical trials using blockchain smart contracts. F1000 Res. (2016)
8. Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. **42**, 130 (2018)
9. Boulos, M.N.K., Wilson, J.T., Clauson, K.A.: Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. Int. J. Health Geogr. (2018)
10. Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T.: FHIRChain: applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J. **16**, 267–278 (2018)
11. Zhao, H., Bai, P., Peng, Y., Xu, R(2018), Efficient key management scheme for health blockchain. CAAI Trans Intell. Technol. **3**, 114–118

Chapter 13
Application of Internet Assistance Computation for Disease Prediction and Bio-modeling: Modern Trends in Medical Science

Manojit Bhattacharya, Avijit Kar, Ramesh Chandra Malick, Chiranjib Chakraborty, Basanta Kumar Das and Bidhan Chandra Patra

Abstract The newer trends have been shown in modern biomedical science, where bio-computational based approaches apply Internet of Things (IoT); which has provided smart facility of health condition monitoring, disease diagnosis and modeling. Therefore, computational application regarding biomedical system comprises with core level like genomics to boarder area as proteomics. Through big data growth as well as ascending of specialist bioinformatics tools into clinical and medical care societies helps correct detection and interpretation of biomedical data facilitated to untimely findings of the disease, caring of patient and promising health system supports. Conversely, the correctness of clinical diagnosis is reducing while the excellence of stored data showing incompleteness or imperfections with relation to in vivo environment. Such internet assistance bioinformatics tools now greater looks genotype to phenotype analysis focus bimolecular structure remodeling with multiple advances, their interaction to environment and ultimately future evolution in global scale. This can better achieved for the vast storage of biological data with supporting bibliographic and accurate biological annotation over internet database like GENBANK, NORD, OMIM etc. lead to the eHealth care in advance time and space. Current chapter deals with the contemporary available innovations which associate the data mining from different internet oriented bioinformatics tools and techniques, server lead to genotype remodeling, Insilco therapeutic approaches,

M. Bhattacharya · R. C. Malick · B. K. Das
ICAR-Central Inland Fisheries Research Institute, Barrackpore, Kolkata, West Bengal 700120, India

A. Kar · B. C. Patra (✉)
Department of Aquaculture Management & Technology, Centre for Aquaculture Research, Extension & Livelihood, Vidyasagar University, Midnapore, West Bengal 721102, India
e-mail: patrabidhan1962@gmail.com

C. Chakraborty
Adamas University, 24 Parganas North, Kolkata, West Bengal 700126, India

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_13

drugs discovery along with the evolutionary trends for mass community services and better future implication. A significant drive also taken to highlight the possibility for upcoming research on IoT-based healthcare centred laid on numbers of well-known topics and challenges linked with intelligent cyber-physical smart universal contexts.

Keywords Internet of things · Bioinformatics · Healthcare · Disease · Therapeutic

13.1 Introduction

Internet assistance disease prediction is an advanced perception that reflects the linked set of anybody, all, every time, anywhere, every support, and at a complete web-based system. Such electronic device based software applications are the largish movement into next-generation know-how practices. It showing large impression towards the entire medical industry interlink of exclusively certain elegant components and policy inside the current electronic web foundation through extensive settlement. Such well-being normally comprises superior linkage of services, devices and systems ahead of machine program set-up [1]. For that reason, in-depth application of computational technology is quite feasible practically each sector of medical science [2].

Internet assisting system put forward correct way out to the wider choices for better health security, clinical emergency, medical monitoring, surgery and many more. Presently, it's enjoying the most promising and cost-effective, time-saving option globally in unique ways [3, 4]. Consequently, multiple bio-imaging and diagnostics components, clinical sensors and devices recognized as elegant substance like as the central part of internet assistance tools and technique. Practically, specific approaches and proficient forecast of inadequate health monitoring and service system can make certain applying internet-based network determined technologies. Rapid mining and crisis management of disease diagnosis, patient urgency, medical case history and databases may provide in whenever need basis for medical practitioner [5].

From the last decade this topic paying extensive attention by researchers focus to the impeding approaches about clinical disease diagnosis concerned with numbers of convenient challenges. Therefore, internet-linked computer-based healthcare services and applications support to the better policies formation within various countries and organizations worldwide.

Conversely, internet assistant bio-modeling system still presents preliminary phases within its healthcare management fields. Aims to the future research present practical knowledge practices into the disease prediction, treatment section expected to be useful for various stakeholders interested in planned medical science.

Crucially analyzing the real facts and data these chapters definitely guide to inspect the advanced trends of internet allied computational assistant in clinical

research and figure out diverse medical issues. Correspondingly it's reflecting on such phenomenon that also contributes among followings objectives:

- Showing the wider assessment of internet-based services and management associated with the clinical therapeutic aspects and its real-time applications.
- Exploring numerous authentic scientific performances to enhance the computer companionable healthcare linked prototypes and products.
- Delivering of protection and individuals subject matter in a boarder sense contiguous to healthcare elucidation and recommend the best-fitted safety model.
- Exploring the present internet supported healthcare system classification in aspects of different-trend wise as summary form.
- Several strategically approach integration that sustains the novelty of e-healthcare system by application of bio-computation technologies.

Such informative research and development actions lead to the best healthcare services using the wireless sensor network (WSN), that also consider as primary internet supported attempt to the healthcare research [6, 7]. Moreover, the continuing tendencies make absent from customary standard and vicinity of IP-based web sensor network using the promising low-power wireless private area network. If the wireless sensor network develops into a center part of the Internet system, afterward a cautious analysis is needed [8–10].

Therefore a crucial attempt is necessary for establishing the innovative guidelines, algorithms, systems support and working architectures for electronic healthcare management. In focal point for the refinement of internet-based computational approaches guide to the disease prediction, prevention, treatment and assessment of physical or mental injury within accurate or superior ways.

13.2 Internet Supported Healthcare Networks

The internet linked-network for healthcare system in the most prime managing component of modern clinical sectors. Helps to access and assist the medical facts (data) reception and transmission within the numbers of communicating methodologies.

Subsequently, Fig. 13.1 represents the working platforms, structural design and topology of the healthcare system that may be consider as a good starting point for developing insights into internet support network [11, 12].

13.2.1 Network Topology

The network topology introduces the collection of numerous components within a computer-based healthcare network and point to the purposeful situation of a faultless thematic part.

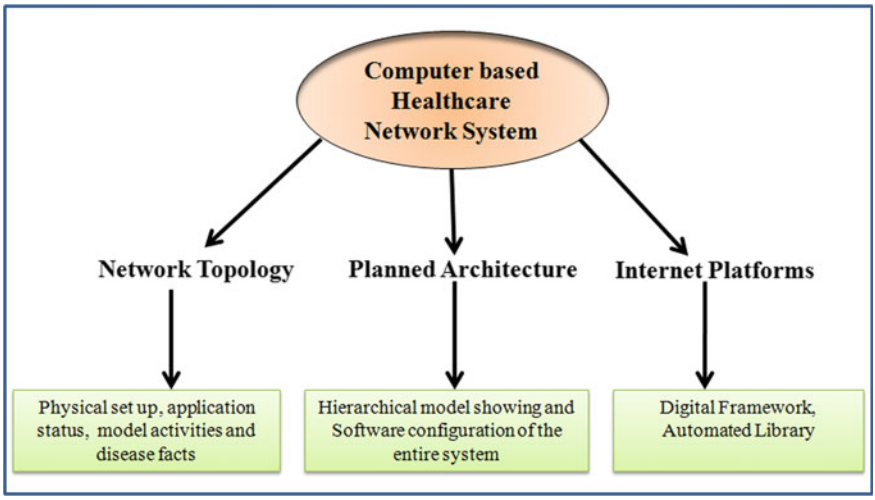


Fig. 13.1 Modern healthcare trends

Significant grid collection of assorted computing system contribute to the important cryptograms and sensor based data like; body temperature, blood pressure, oxygen saturation level and electrocardiograms shaped in a topology. That may alter storage performances and varied computing status of modern electronic devices (smartphones, laptops, notebook etc.) within the performing computing frameworks in hybrid mode [13].

To captures and measured the patients health related problems, multiple convenient sensors and medical devices are affixed to the body parts (Fig. 13.2). Afterwards collected data are then furthered evaluate and store for useful findings of clinical treatment aspects. Depending on these methods, medical practitioner can able to supervise in remote mode (away position) and also take action in proper need. Parallelly, such topology also consist of an obligatory network arrangement intended the live stream and projection of linked medical data, case and videos. The model concept configuration composed with the interrelated network with web access, network of internet protocol (IP), and the network of Global systems for Mobile Communications (GSM) having gateway permit condition [14–16].

For managing the difficulties of disease prediction and wrong medicinal treatment advanced technology-based internet sustained devices also implied. Purpose of clinical diagnosis and healing outcomes diverse sensor supported wearable devices are attached to patients in an internet-health technology-based cloud network for ultra frame analysis. Such electronic access is able to collect data/score, exhibit and stored for future assessment in remote condition [17]. Integration of computational venture with clinical framework and strategies the identical web-based topology also established [18]

Distinguishing related exercises and jobs in medicinal administrations is a major factor in structuring the bio-computational topology system. Multiple treatment

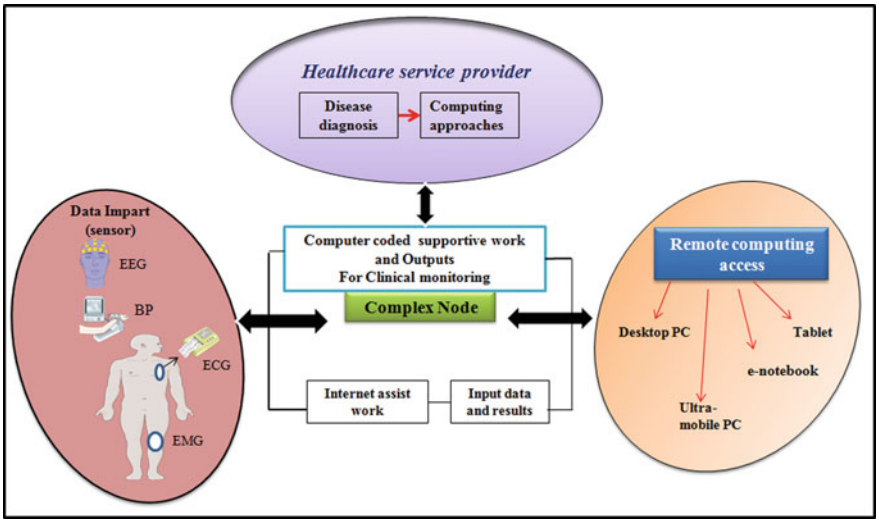


Fig. 13.2 A conceptual diagram of IoT based ubiquitous healthcare solution

phases handling to include medicinal services benefits for the most part from the viewpoint of human services within specialist organizations [19]. Appropriate medicinal services exercises have been shown with regards to therapeutic crisis administrations and web-based network (Genbank, NCBI, OMIM) together with distributed computing for unavoidable disease diagnosis and medical care has been implied [20]. Such phenomenon also observed like be the traditional full-work organizing framework with the ubiquity of web network. At that point, the topologies have to incorporate a standarad medicinal framework on account of a semantic medical checking infrastructural periphery [21].

13.3 Internet Supported Healthcare System and Relevance

Internet holds healthcare services design also functional to the varied ranges together with concern about all aged patients, the practical managing of chronic disease connected to the organization of public wellbeing and physical robustness. Highlighting to design in a superior appreciative of such widespread subject, this chapter generally classify the following section in two main features: system services and its appliance.

Significant relevance is made to add splitting up as different groups: distinct- and assemblage-state the of application.

The solitary state of application pass to an exceptional disease or ill health, while a bunched circumstance application manages various infections type collectively in

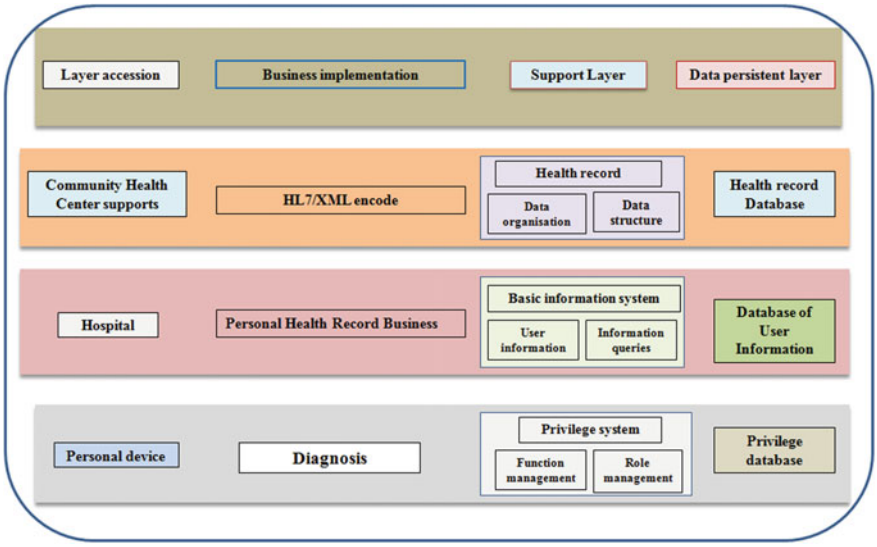


Fig. 13.3 Healthcare and applications of the internet system

general. Remarkably, such classification composition is surrounded to dependent on the present accessible human services arrangements utilizing the internet based tools and techniques. This rundown is characteristically unique in present status and can be effectively upgraded by including extra administrations with particular highlights and various applications covering both single- and bunched condition arrangements. This area presents every one of the healthcare and applications appeared in Fig. 13.3.

13.3.1 Internet System Services

The internet system services are foreseen to empower an assortment of human services benefits in which every administration gives a lot of clinically sustain arrangements. With regards to biomedical assurance, there is no typical sharpness of internet of things system services. In any case, there might be a few cases where an administration can't be impartially separated from a specific arrangement or application. Present write up suggests that the system service approaches likely by certain methods conventional in nature and can possibly be a structure obstruct for a lot of arrangements or applications. Moreover, it ought to be noticed that general administrations and conventions required for computer-based internet structures may require slight prescriptions for their appropriate working in human services situations. These incorporate notice administrations, asset sharing administrations, internet providers, cross-network conventions for heterogeneous gadgets, and

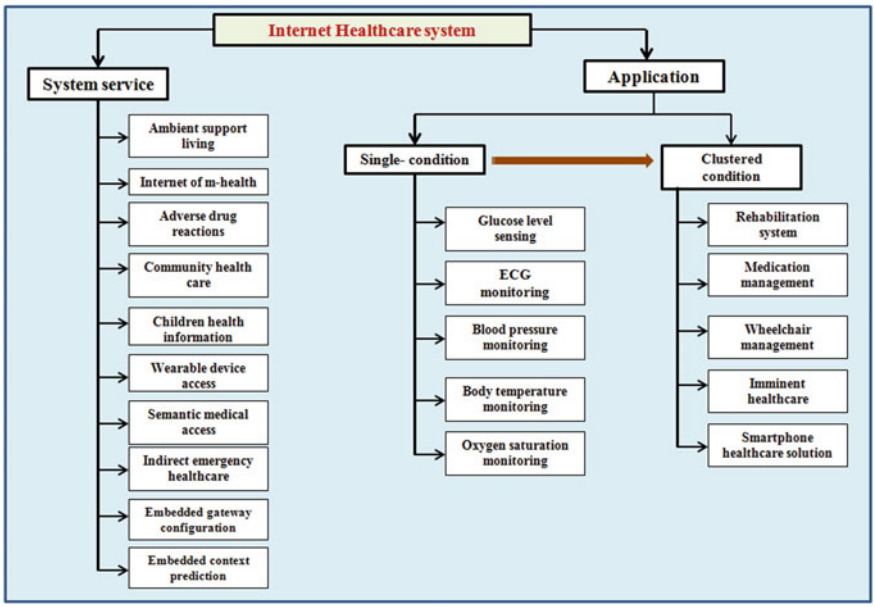


Fig. 13.4 System services and applications of Internet Healthcare

connection conventions for real availability. The simple, quick, secure, and low-control disclosure of electronic gadgets and effective organization can be added to this recent rundown.

Nonetheless, a description of such summed up internet services for healthcare management system is past the extent of this overview. The intrigued individual is allowed to the writing for an increasingly far-reaching comprehension of this success point. The accompanying subsections incorporate different sorts of disease prediction and clinical diagnostic support in advance healthcare system (Fig. 13.4).

13.3.2 Background Supported System

Generally, not even a specialized support system on such summed up the internet assisted system are past the extent of this overview. The service support allied system to the lettering for an increasingly far-reaching comprehension of this stated point. The accompanying subsections incorporate different types of clinical and disease prediction network bio-model. Main rational of background supported system is to pull out the self-governing condition of aged peoples habitats in a proper suitable and secure approach [22]. Perfect explanation supplied by internet services could build patients approval by ensuring the vice versa backing in a greater way out of any problem. This engineering essentially fills in as a system for giving human services related to healthcare to older and weakens people. As the

fundamental innovation for executing this engineering, wide zone LAN framework is utilized for dynamic interchanges, and radio recurrence recognizable proof and close field correspondences are utilized for latent correspondences. Absolute incorporation of algorithms based medical facts for detection of medical problems of aged individuals such closed loop smart objects are facilitated to the healthcare services [23].

At that point, this consequential foundation also utilizes the internet support to empowering correspondence between partners, for example, older patients, care personnel, doctors, and family relatives. These endeavors have propelled scientists to create conventions for smart electronic objects and shut down the medical system services work through computer applications. The untie, protected, and multistep stage dependent on the internet technology and distributed computing system already proposed [24]. Such phase tends to unusual constraint related with the effectiveness, protection, the gushing nature of services and information stockpiling, that practicality has been varied by introducing for wellbeing door with respect to a personal computer as reference execution. Past investigations have featured the requirement for medical care and relating innovative help and introduced a provisional guide for condition-of-the-art healthcare technologies [16, 25].

13.3.3 Mobile Health (m-health) of Internet Things

Application of mobile computing services, communication technologies and specific medical sensors for superior healthcare services is known as mobile (m-health) [26]. Theoretically, such approaches showing model connectivity of healthcare system involving tele-networks for upcoming potential m-health practices, that also showing unique characteristics participate better entities. Likewise, the sensing of glucose level, heart rate pattern, movements of drugs or pharmaceuticals product etc., their execution issue and challenges [27]. A functional framework for message-exchange based versatility is presented in this section, yet its confined with the low system control utilization that may be present in changed condition (Fig. 13.5) [22].

13.3.4 Destructive Reaction of Drugs

The damage caused by the taking of medicine (drug component) is considerate as destructive drug reaction [28]. Its occur following to a solitary portion of a medication or drug drawn out organization or as a result of a blend of at least two medications. Since such adverse is intrinsically conventional, that is, not specific to the drug for a specific infection, there is a need to structure certain regular specialized issues independently and their answers [29]. With the assistance of a pharmaceutical sense data framework, this data is seem too planned to detect

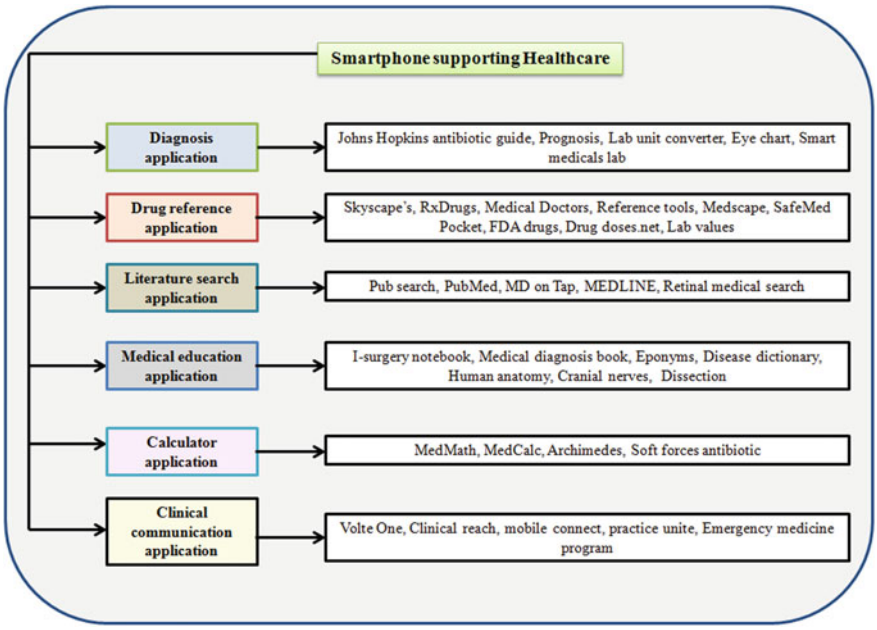


Fig. 13.5 Mobile healthcare system service architecture

whether the medication is perfect with its hypersensitivity issue and electronic wellbeing record. Lastly, to controlled and address the adverse effects by impotent of internet-based computer support technology solution [17].

13.3.5 Community Medical Care System

Concept of community medical care system linked with the idea to form a network covered in a surrounding part of a regional areas. Like be an internet oriented-network-based civil emergency clinic, a local location, or a provincial network. The connection of a few such systems can be acknowledged as a helpful system structure. In such manner, a specific system sustains called network human services is inescapable for gathering aggregate specialized necessities as a bundle or package. The energy efficient medical care monitoring also proposed within rural scale like be cooperative manner [30]. Here a clear, rightful confirmation and approval component have to be joined in light of the facts that it is an agreeable system condition state. Which may be considered as "virtual hospital", being a part of community medical network. An occupant wellbeing data administration stage dependent on a practical system of a four-layer organization has been considered, and a technique for sharing information between restorative offices and the administration stage for getting wellbeing records and getting to remote therapeutic guidance [31].

13.3.6 Health Information of Children

Bringing issues to focused around younger peoples wellbeing and developing the overall population just as kids themselves on necessities of a child with enthusiastic, social, or emotional well-being issues and their family relatives are also essential [32]. Looks for the energetic scientists to build up the particular computer linked services called children wellbeing data to address this need in a powerful way. In such manner, an intuitive object set in a child specialist ward offering children healthcare information went for teaching, diverting, and engaging hospitalized children is planned formed for mobile healthcare services based of internet technology and mobile medical wellbeing system that can recommend patient to secure and greatly healthful propensities with the assistance of their educators and guardians also [33, 34].

13.3.7 Wearable Technology Appliance

Different non-distinctive sensor components have been produced for an assorted scope of restorative medicinal applications, specifically to internet assisted systems [35]. Those elements potential to convey equal services throughout computer application. Conversely, the wearable components consisting of a group of advantageous quality intended to computational machine configuration. So that, the coordination of previously mentioned sensors into wearable items is evident. As the heterogeneous idea of wearable items and therapeutic sensors reveals various difficulties for specialists and engineers moving in the direction of the assumed incorporation. Therefore, an enthusiastic service factor is known as Wearable technology access also important to require. This strategy presents a model framework that can be utilized in a wide assortment of medicinal services applications through different portable, mobile registering computing methods [36].

13.4 Computer Applications in Healthcare

Auxiliary to internet assisted program, software applications need a closer look. It's quite fine to perceive that medical are utilized to create applications, while applications are straightforwardly utilized by clients and patients. In this way, administrations are engineer driven, while applications, client driven. Although the applications canvassed in this segment, different devices, and other human medical services tool at present accessible in the market are talked about. These items can be seen as internet of things developments that can prompt to the different medicinal services arrangements. These following subsections address different internet based technology based medicinal services applications, including both single- and grouped condition applications.

13.4.1 Determination of Glucose Level

Grouping of metabolic diseases, diabetics define as the high level of blood sugar (glucose) in a long period. Monitoring of blood sugar showing person based prototype of changing glucose intensity within the scheduling of feeding actions and time also [37]. Sensors supported device for patient allied with internet connectivity reflects proper sensing and monitoring of glucose status. Background processor with computer or smart phone and generic computer hold devices demand a remarkable innovation [38, 39].

13.4.2 Monitoring of Electrocardiogram

The electrical movement of the heart documented by electrocardiography incorporates the estimation of the basic pulse and the assurance of the essential cadence just as the analysis of belated QT interims, multifaceted arrhythmias and myocardial ischemia [40]. Practical exercise of the internet assisted computation tools and technique to Electrocardiogram checking can possibly give the greatest data and can be utilized to its highest degree [41]. Numerous studies showed such facts specialized to the versatile remote securing transmitter and the remote getting processor [42, 43]. The framework incorporates an inquiry mechanization technique to identify unusual information with the end goal that cardiovascular capacity can be detected consistently [44, 45]. In an integration condition, the existence of a thorough recognition software-based language calculation of Electrocardiogram signals at the relevance layer of the internet network tool arrange for Electrocardiogram graph data observing and assessment [46, 47].

13.4.3 Monitoring of Blood Pressure (BP)

Mixing of a blood pressure meter and a wireless technology empowered smart cell phone turns out to be a piece of BP observing dependent on web computer system tended to health supervision [23]. The propelling situation wherein BP also consistently controlled remote mode is introduced by demonstrating the interchanges structure between a wellbeing condition and the wellbeing focus [48]. The subject of BP detection gadget works relies upon the association with versatile processing electronic device is tend to proper functioning [49]. The gadget for BP information accumulation and broadcast more on an internet linked electronic digital system [50]. This gadget is made out of a BP mechanical assembly body with a correspondence unit. An area wise operational terminal for carry-on BP checking dependent on preprogram computing system and services [51].

13.4.4 Monitoring of Body Temperature

Body temperature observing is a fundamental piece of medicinal care services since body temperature is an unequivocal imperative indication in support of homeostasis [52].

Idea of mobile internet computing program is fluctuated utilizing a body temperature sensor that is installed in the bit version, that a common example of achieved body temperature varieties appearing fruitful activity of the created same framework is displayed. The temperature estimation framework was dependent on an entry part over the proposed system approaches [53]. The home passage transmits the client's body temperature with the assistance of infrared discovery. The primary framework parts in charge of temperature recording and transmission looked in a computer connected program for checking body temperature [54].

13.4.5 Monitoring of Oxygen Saturation

Heartbeat measurement by oximetry is an appropriate device about non-invasive, relentless observing of blood oxygen immersion. The incorporation of the e-web system with heartbeat oximetry is helpful for innovation-driven restorative medicinal services applications [55]. The capacity of the wearable heartbeat oximeter is represented its purposeful, valid application [56]. This battery operated gadget accompanies availability dependent on a Bluetooth connected part and the sensor associates straightforwardly to the singular phase. A software upgraded low-control/ease beat oximeter for distant patient checking also proposed [57]. This gadget can be utilized to consistently screen the patient's wellbeing over computational arranges. The incorporated heartbeat oximeter framework for telemedicine relevance also depicted [58]. Wearable heartbeat oximeters for wellbeing checking utilizing the oxygen saturation can be adjusted to the computing network [59].

13.4.6 Rehabilitation System

Since physical medication and recovery can improve and re-establish the useful capacity and personal satisfaction of those with some physical weakness or handicap, they speak to an essential part of the prescription. The internet network support can possibly improve restoration frameworks regarding relieving issues connected to maturing populaces and the lack of medical care specialists. Effective computer based support can be a compelling stage for associating every single vital asset to offer real-time data connections. Such advancements can frame a beneficial framework to help powerful remote conference in far-reaching recovery [60]. There are numerous internet dependent recovery frameworks, for example, an incorporated

application framework for penitentiaries [61], the restoration preparing of hemiplegic patients, updated city therapeutic recovery framework, and the language-preparing framework for childhood chemical imbalance [62–64].

Numerous other compact restorative appliances are accessible however there is no express exhibit of the incorporation of those gadgets into inter of things systems. Therefore, it is just a short time before these gadgets become installed with those topological network capacities. Expanding quantities of therapeutic applications, gadgets, and medical cases put with the developing interest for internet based management and care services over the whole world.

Few medically supported territories whose incorporation with the network model seems fast approaching incorporate hemoglobin identification, unregulated cell expansion, anomalous cell development, malignancy treatment, eye infection, skin disease, and associated remote medical surgical operation procedure [65, 66].

13.5 Trends and Status of Internet-based Healthcare Diligence

Internet assisted medicinal services encountered a blasted of movement and imagination, energizing business people and investment status. The break shows up as a functioning gathering of new companies and huge opportunities that are eager to be a piece of what might be a giant advertises just as empowering items and advances. This area gives a broad rundown of these items and advancements for a superior comprehension of the stated position. Supposing of a model of the wearable element (sensor) for continuous following, fall discovery, and cautions. It essentially consolidates the GPS, portable information, short informing services and a stimulator to recognize irregular developments, for example, a fall and after that reports them to an outsider [67]. Wider scale of information technology answers for China's restorative industry and individual human services system and it additionally offers their administrations for medical clinics, general medical care offices, and wellbeing the executives [67].

13.6 Internet Security System in Healthcare

Internet of things is developing quickly. In the following quite a while, the medicinal area is relied upon to observe the far-reaching reception of that system and expanding through new electronic health supported gadgets and applications. Medical care allied gadgets and applications are relied upon to manage crucial private data, for example, individual medicinal services information. What's more, such keen gadgets might be associated with worldwide data systems for their entrance whenever, anyplace. Along these lines, the internet linked medical care space might be an objective of aggressors. To encourage the full reception of the

such object in the human services area, it is basic to recognize and break down particular highlights of security and protection, including security prerequisites, vulnerabilities, risk models, and countermeasures, from that specified point of view.

Security necessities to internet-based healthcare services are analogous for the typical infrastructure state. For that reason, to pull off the protected service system, it's urgent to concentrate on the subsequent security rations.

13.6.1 Privacy

Privacy guarantees the unavailability of restorative data for unapproved clients. Furthermore, secret messages oppose uncovering their substance to busybodies.

13.6.2 Reliability

Reliability guarantees that got therapeutic information are not modified in travel by a foe. Furthermore, the uprightness of put away information and substance ought not to be undermined.

13.6.3 Confirmation

Confirmation empowers an IoT wellbeing gadget to guarantee the personality of the friend with which it is imparting.

13.6.4 Accessibility

Accessibility guarantees the survivability of IoT based medical care system (either nearby or worldwide/cloud administrations) to approved gatherings when required even under refusal of-administration assaults.

13.6.5 Authentic Data

Authentic data incorporates information novelty and prime originality. Since every internet-computing human services system gives some time differing estimations, there is a must requirement to guarantee that each and every case data is new. Information originality essentially suggests that every datum set is later and guarantees that no enemy replays old messages.

13.6.6 Non-repetition

Non-repetition shows that a hub can't deny communicating something specific sent before.

13.7 Security Limitations

Internet supported computer application security rations not to make certain applying conventional security tools and techniques, narrative counteract dealings also required to face the original challenge. Internet oriented gadgets are implanted with low-speed processors. The focal handling unit (CPU) in such gadgets isn't amazing regarding its speed. Also, these gadgets are not intended to perform computationally in case of costly tasks. That is, they just go about as a sensor or actuator. In this manner, ending a security arrangement that limits asset utilization and along these lines, amplifies security execution is a difficult job. The quantities of such gadgets have expanded progressively, and along these lines more gadgets are getting associated with the worldwide data organize. Hence, planning exceptionally adaptable security conspire without trading off security necessities turns into a complex errand. The medical caring gadget may join a well service system anyplace, whenever. Moreover, it can leave a system either effortlessly (with appropriate leave notice) or shamefully (suddenly). Worldly and spatial confirmation attributes of therapeutic gadgets make the system topology dynamic. Subsequently, formulating a security model for this sort of unique system topology is a troublesome test. To relieve potential vulnerabilities, there is a need to stay up with the latest. Subsequently, refreshed security patches are required for IoT wellbeing gadgets. In any case, planning a system for the dynamic establishment of security patches is a difficult errand. Security in physical status is a significant piece of IoT wellbeing gadgets. An assailant may alter gadgets and after that may later concentrate cryptographic privileged insights, change programs, or supplant those with malignant hubs. Alter safe bundling is an approach to guard against such assaults; however, it is trying to actualize by and by.

13.8 Conclusions

Scientific communities of every part of the world tried to explore numerous attempts for technological way out to upgrade the disease prediction and therapies from present computer assistance tools and techniques. This chapter marked to figure out and concluded the several features of Internet oriented computational network configurations and suitable strategies that hold up the clinical case or medicinal data broadcasting and further impactful functions. Consequently, the wider research and developmental approaches also furnished connected to the best healthcare practices and bio-modeling relevance in recent scenario (Fig. 13.6).

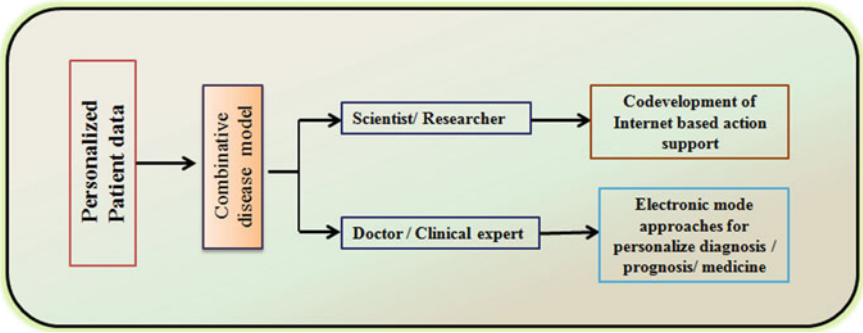


Fig. 13.6 Disease modeling in e-healthcare

Additionally, the chapter reflects comprehensive progress and updated depiction related to the internet supported computational technologies that handled purposeful medical care of infants and adults, persistent disease management, personal health supervision, and chronic stress managing features.

Focus to the impeding part of facilitating technology and industrial inclination in a wider outlook about the updated and running progression of internet applications, impart devices, functional sensors employed to reasonable health associated electronic components and linked services lead to the unlimited expansion of computer supported diseases diagnosis, clinical applications for future up gradation. Superior realization also has been done about the human health security requirements and challenges of diverse problems within this specified subject to suggest a mock-up to neutralize the undesired hazards.

The exchange occurrence on a few significant issues, for example, institutionalization, arrange type, plans of action, the nature of administration, and wellbeing information security is required to encourage a promising premise for further research on computer-based medicinal services administration. This chapter represents eHealth services, internet-linked strategies and guidelines centered on the wellbeing of different partners keen on evaluating computational bio-modeling associated medicinal services advances. Finely, the consequences of this overview are relied upon to be helpful for scientists, engineers, medical care experts, and health services policymakers working in the territory of the advanced internet technologies and best bio-medical service practices.

References

1. Höller, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S., Boyle, D.: From Machine to the Internet of Things: Introduction to a New Age of Intelligence, pp. 9–14. Elsevier (2014)
2. Guinard, D., Trifa, V., Wilde, E.: A resource oriented architecture for the Web of Things. In: IoT, pp 1–8 (2010)

3. Tan, L., Wang, N.: Future internet: the internet of things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), V5-376-V375-380. IEEE (2010)
4. Pang, Z.: Technologies and architectures of the internet-of-things (IoT) for health and well-being. Doctoral Dissertation, KTH Royal Institute of Technology (2013). https://pdfs.semanticscholar.org/222d/206e8fc758c19ac06680db61a555fd6b71ed.pdf
5. Vasanth, K., Sbert, J.: Creating Solutions for Health Through Technology Innovation. Texas Instruments (2014). Available at: http://www.ti.com/lit/wp/sszy006/sszy006.pdf. Accessed 15 Apr 2019
6. Ko, J., Lu, C., Srivastava, M.B., Stankovic, J.A., Terzis, A., Welsh, M.: Wireless sensor networks for healthcare. Proc. IEEE **98**(11), 1947–1960 (2010)
7. Alemdar, H., Ersoy, C.: Wireless sensor networks for healthcare: a survey. Comput. Netw. **54** (15), 2688–2710 (2010)
8. Mainetti, L., Patrono, L., Vilei, A.: Evolution of wireless sensor networks towards the internet of things: a survey. In: SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks, pp. 1–6. IEEE (2011)
9. Christin, D., Reinhardt, A., Mogre, P.S., Steinmetz, R.: Wireless sensor networks and the internet of things: selected challenges. In: Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose sensornetze, pp. 31–34 (2009)
10. Alcaraz, C., Najera, P., Lopez, J., Roman, R.: Wireless sensor networks and the internet of things: do we need a complete integration? In: 1st International Workshop on the Security of the Internet of Things (SecIoT'10) (2010)
11. Zhu, Q., Wang, R., Chen, Q., Liu, Y., Qin, W.: IoT gateway: bridgingwireless sensor networks into internet of things. In: 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp. 347–352. IEEE (2010)
12. Grønbæk, I.: Architecture for the Internet of Things (IoT): API and interconnect. In: 2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008), pp. 802–807. IEEE (2008)
13. Viswanathan, H., Lee, E.K., Pompili, D.: Mobile grid computing for data- and patient-centric ubiquitous healthcare. In: 2012 The First IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things (ETSIoT), pp. 36–41. IEEE (2012)
14. Zhao, W., Wang, C., Nakahira, Y.: (2011) Medical application on internet of things. In: IET International Conference on Communication Technology and Application (ICCTA 2011), pp. 660–665 (2011)
15. Yang, N., Zhao, X., Zhang, H.: A non-contact health monitoring model based on the internet of things. In: 2012 8th International Conference on Natural Computation, pp. 506–510. IEEE (2012)
16. Istepanian, R.S.: The potential of Internet of Things (IoT) for assisted living applications. In: IET Seminar on Assisted Living 2011, pp. 1–40. IET (2011)
17. Yang, G., Xie, L., Mäntysalo, M., Zhou, X., Pang, Z., Da Xu, L., Kao-Walter, S., Chen, Q., Zheng, L.-R.: A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. IEEE Trans. Ind. Inform. **10**(4), 2180–2191 (2014)
18. Jara, A.J., Zamora, M.A., Skarmeta, A.F.: Knowledge acquisition and management architecture for mobile and personal health environments based on the internet of things. In: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1811–1818. IEEE (2012)
19. Xu, B., Da Xu, L., Cai, H., Xie, C., Hu, J., Bu, F.: Ubiquitous data accessing method in IoT-based information system for emergency medical services. IEEE Trans. Ind. Inform. **10** (2), 1578–1586 (2014)
20. Doukas, C., Maglogiannis, I.: Bringing IoT and cloud computing towards pervasive healthcare. In: 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 922–926. IEEE (2012)

21. Zhang, G., Li, C., Zhang, Y., Xing, C., Yang, J.: SemanMedical: a kind of semantic medical monitoring system model based on the IoT sensors. In: 2012 IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom), pp 238–243. IEEE (2012)
22. Shahamabadi, M.S., Ali, B.B.M., Varahram, P., Jara, A.J.: A network mobility solution based on 6LoWPAN hospital wireless sensor network (NEMO-HWSN). In: 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 433–438. IEEE (2013)
23. Dohr, A., Modre-Opsrian, R., Drobics, M., Hayn, D., Schreier, G.: The internet of things for ambient assisted living. In: 2010 Seventh International Conference on Information Technology: New Generations, pp. 804–809. IEEE (2010)
24. Zhang, X.M., Zhang, N.: An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and telemedicine. In: 2011 International Conference on Computer and Management (CAMAN), pp. 1–4. IEEE (2011)
25. Gonçalves, F., Macedo, J., Nicolau, M.J., Santos, A.: Security architecture for mobile e-health applications in medication control. In: 2013 21st International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2013), pp. 1–8. IEEE (2013)
26. Istepanian, R.S., Jovanov, E., Zhang, Y.: Guest editorial introduction to the special section on m-health: beyond seamless mobility and global wireless health-care connectivity. IEEE Trans. Inf. Technol. Biomed. **8**(4), 405–414 (2004)
27. Istepanian, R.S., Hu, S., Philip, N.Y., Sungoor, A.: The potential of Internet of m-health Things "m-IoT" for non-invasive glucose level sensing. In: 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 5264–5266. IEEE (2011)
28. Arango, J., Chuck, T., Ellenberg, S.S., Foltz, B., Gorman, C., Hinrichs, H., McHale, S., Merchant, K., Seltzer, J., Shapley, S.: Good clinical practice training: identifying key elements and strategies for increasing training efficiency. Ther. Innov. Regul. Sci. **50**(4), 480–486 (2016)
29. Jara, A.J., Belchi, F.J., Alcolea, A.F., Santa, J., Zamora-Izquierdo, M.A., Gómez-Skarmeta, A.F.: A pharmaceutical intelligent information system to detect allergies and adverse drugs reactions based on internet of things. In: 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 809–812. IEEE (2010)
30. Rohokale, V.M., Prasad, N.R., Prasad, R.: A cooperative Internet of Things (IoT) for rural healthcare monitoring and control. In: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), pp. 1–6. IEEE (2011)
31. Wang, W., Li, J., Wang, L., Zhao, W.: The internet of things for resident health information service platform research. In: Proceedings of the IET International Conference on Communication Technology and Application, pp. 631–635 (2011)
32. Day, A.: Activities by program type (2014). http://www.samhsa.gov/sites/default/files/children-awareness-dayactivities-by-program-2014.pdf. Accessed 7 Mar 2019
33. Vicini, S., Bellini, S., Rosi, A., Sanna, A.: An internet of things enabled interactive totem for children in a living lab setting. In: 2012 18th International ICE Conference on Engineering, Technology and Innovation, pp. 1–10. IEEE (2012)
34. Vazquez-Briseno, M., Navarro-Cota, C., Nieto-Hipolito, J.I., Jimenez-Garcia, E., Sanchez-Lopez, J.: A proposal for using the internet of things concept to increase children's health awareness. In: CONIELECOMP 2012, 22nd International Conference on Electrical Communications and Computers, pp. 168–172. IEEE (2012)
35. Chung, W.-Y., Lee, Y.-D., Jung, S.-J.: A wireless sensor network compatible wearable u-healthcare monitoring system using integrated ECG, accelerometer and SpO2. In: 2008 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 1529–1532. IEEE (2008)

36. Castillejo, P., Martinez, J.-F., Rodriguez-Molina, J., Cuerva, A.: Integration of wearable devices in a wireless sensor network for an E-health application. IEEE Wirel. Commun. **20**(4), 38–49 (2013)
37. Guan, Z.J.: Somatic data blood glucose collection transmission device for Internet of Things. Chin. Patent **202**(838), 653 (2013)
38. Wei, L., Heng, Y., Lin, W.Y.: Things based wireless data transmission of blood glucose measuring instruments. Chin. Patent **202**(154), 684 (2012)
39. Lijun, Z.: Multi-parameter medical acquisition detector based on Internet of Things. Chin. Patent **202**(960), 774 (2013)
40. Drew, B.J., Califf, R.M., Funk, M., Kaufman, E.S., Krucoff, M.W., Laks, M.M., Macfarlane, P.W., Sommargren, C., Swiryn, S., Van Hare, G.F.: Practice standards for electrocardiographic monitoring in hospital settings: an American Heart Association scientific statement from the Councils on Cardiovascular Nursing, Clinical Cardiology, and Cardiovascular Disease in the Young: endorsed by the International Society of Computerized Electrocardiology and the American Association of Critical-Care Nurses. Circulation **110** (17), 2721–2746 (2004)
41. Dash, P.: Electrocardiogram monitoring. Indian J. Anaesth. **46**(4), 251–260 (2002)
42. Rasid, M.F.A., Musa, W., Kadir, N., Noor, A.M., Touati, F., Mehmood, W., Khriji, L., Al-Busaidi, A., Mnaouer, A.B.: Embedded gateway services for Internet of Things applications in ubiquitous healthcare. In: 2014 2nd International Conference on Information and Communication Technology (ICoICT), pp. 145–148. IEEE (2014)
43. You, L., Liu, C., Tong, S.: Community medical network (CMN): architecture and implementation. In: 2011 Global Mobile Congress, pp. 1–6. IEEE (2011)
44. Yang, L., Ge, Y., Li, W., Rao, W., Shen, W.: A home mobile healthcare system for wheelchair users. In: Proceedings of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 609–614. IEEE (2014)
45. Agu, E., Pedersen, P., Strong, D., Tulu, B., He, Q., Wang, L., Li, Y.: The smartphone as a medical device: assessing enablers, benefits and challenges. In: 2013 IEEE International Workshop of Internet-of-Things Networking and Control (IoT-NC), pp. 48–52. IEEE (2013)
46. Liu, M.-L., Tao, L., Yan, Z.: Internet of Things-based electrocardiogram monitoring system. Chin. Patent **102**(764), 118 (2012)
47. Mukhopadhyay, S.C.: Wearable sensors for human activity monitoring: a review. IEEE Sens. J. **15**(3), 1321–1330 (2014)
48. Puustjärvi, J., Puustjärvi, L.: Automating remote monitoring and information therapy: an opportunity to practice telemedicine in developing countries. In: 2011 IST-Africa Conference Proceedings, pp. 1–9. IEEE (2011)
49. Tarouco, L.M.R., Bertholdo, L.M., Granville, L.Z., Arbiza, L.M.R., Carbone, F., Marotta, M., De Santanna, J.J.C.: Internet of Things in healthcare: interoperability and security issues. In: 2012 IEEE International Conference on Communications (ICC), pp. 6121–6125. IEEE (2012)
50. Guan, Z.J.: Internet-of-Things human body data blood pressure collecting and transmitting device. Chin. Patent **202**(821), 362 (2013)
51. Xin, T., Min, B., Jie, J.: Carry-on blood pressure/pulse rate/blood oxygen monitoring location intelligent terminal based on Internet of Things. Chin. Patent **202**(875), 315 (2013)
52. Ruiz, M., García, J., Fernández, B.: Body temperature and its importance as a vital constant. Rev. Enferm. (Barcelona, Spain) **32**(9), 44–52 (2009)
53. Jian, Z., Zhanli, W., Zhuang, M.: Temperature measurement system and method based on home gateway. Chin. Patent **102**(811), 185 (2012)
54. Natarajan, K., Prasath, B., Kokila, P.: Smart health care system using internet of things. J. Netw. Commun. Emerg. Technol. **6**(3) (2016). www.jncet.org
55. Khattak, H.A., Ruta, M., Di Sciascio, E.: CoAP-based healthcare sensor networks: a survey. In: Proceedings of 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST). pp. 499–503 (2014)

56. Jara, A.J., Zamora-Izquierdo, M.A., Skarmeta, A.F.: Interconnection framework for mHealth and remote monitoring based on the internet of things. IEEE J. Sel. Areas Commun. **31**(9), 47–65 (2013)
57. Larson, E.C., Goel, M., Boriello, G., Heltshe, S., Rosenfeld, M., Patel, S.N.: SpiroSmart: using a microphone to measure lung function on a mobile phone. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing, pp. 280–289. ACM (2012)
58. Larson, E.C., Goel, M., Redfield, M., Boriello, G., Rosenfeld, M., Patel, S.N.: Tracking lung function on any phone. In: Proceedings of the 3rd ACM Symposium on Computing for Development, p. 29. ACM (2013)
59. Larson, E.C., Lee, T., Liu, S., Rosenfeld, M., Patel, S.N.: Accurate and privacy preserving cough sensing using a low-cost microphone. In: Proceedings of the 13th International Conference on Ubiquitous Computing, pp. 375–384. ACM (2011)
60. Tan, B., Tian, O.: Short paper: using BSN for tele-health application in upper limb rehabilitation. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 169–170. IEEE (2014)
61. Bhat, M.I., Ahmad, S., Amin, A., Ashraf, S.: e-Health with internet of things. Int. J. Comput. Sci. Mob. Comput. **6**(6), 357–362 (2017)
62. Guangnan, Z., Penghui, L.: IoT (Internet of Things) control system facing rehabilitation training of hemiplegic patients. Chin. Patent **202**(587), 045 (2012)
63. Yue-Hong, Y., Wu, F., Jie, F.Y., Jian, L., Chao, X., Yi, Z.: Remote medical rehabilitation system in smart city. Chin. Patent **103**(488), 880 (2014)
64. Liang, S., Zilong, Y., Hai, S., Trinidad, M.: Childhood autism language training system and Internet-of-Things-based centralized training center. Chin. Patent **102**(184), 661 (2011)
65. Gayat, E., Bodin, A., Sportiello, C., Boisson, M., Dreyfus, J.-F., Mathieu, E., Fischler, M.: Performance evaluation of a noninvasive hemoglobin monitoring device. Ann. Emerg. Med. **57**(4), 330–333 (2011)
66. Pesta, M., Fichtl, J., Kulda, V., Topolcan, O., Treska, V.: Monitoring of circulating tumor cells in patients undergoing surgery for hepatic metastases from colorectal cancer. Anticancer Res. **33**(5), 2239–2243 (2013)
67. Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.-S.: The internet of things for health care: a comprehensive survey. IEEE Access **3**, 678–708 (2015)

Part IV
IoT Implementation in Education

Chapter 14
QFD Approach for Integrated Information and Data Management Ecosystem: Umbrella Modelling Through Internet of Things

Arindam Chakrabarty and Tenzing Norbu

Abstract The journey of human civilization has been phenomenal and indeed multi-dimensional. It started with the struggle for existence, survival, growth, transformation and enrichment for gratifying physical as well as intellectual aspirations. Experiential knowledge system and scientific acumen had been the propeller of the engine of development which essentially began with the ignition of fire followed by the inventions of wheels and so on. With the growing complexities of life and multifaceted ambitions, the problems are becoming compounded which need to be solved by the interface of cognitive skills and technology. Triumph of human societies has crossed many milestones at different ages i.e., Stone Age, Bronze Age and Iron Age through evolutionary historical episodes like Paleolithic, Mesolithic and Neolithic era. The dynamics of contemporary human civilization solely depends on knowledge economy at the behest of the present information age. The impetus of information has been widely accepted and practiced across the horizontally and vertically integrated economic orientations worldwide. The degree of intensity and commitment might differ among various societies throughout the globe. The concept of Internet of Things (IoTs) has become popular among practitioners, academia and researchers as it acts as the idea of umbrella value proposition with the synergy of related multipliers. The growth trajectory for the advancement and welfare of human races primarily depends on the availability, accessibility and usability of data on multi-dimensional variables. In fact, efficient data management system has become the backbone of all the developmental models. The government agencies even the corporate sectors are also reciprocating to this call of the hour and collect data in accordance with their sectoral limitation. This is

A. Chakrabarty (✉)
Department of Management, Rajiv Gandhi University (Central University), Itanagar, Arunachal Pradesh 791112, India
e-mail: arindam.management@gmail.com

T. Norbu
Centre for Management Studies (CMS), North Eastern Regional Institute of Science & Technology (NERIST), Itanagar, Arunachal Pradesh 791110, India
e-mail: tenzing.management@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_14

welcoming but not exhaustive since it suffers from inconsistencies manifolds. Now, the priority and thrust have been convoluted on the real time data rather being confined into mere collection and use of unintegrated raw data. This chapter would attempt to develop a model based on 'Quality Function Deployment (QFD)' approach using IoT platform to augment the real-life data management system which would interact and share between all the stakeholders conforming the spirit of selective data privacy and confidentiality. This would also strive to bring reforms in the existing process of planning, strategy formulation and project implementations.

Keywords QFD approach · Integrated information · Data Management Ecosystem · Umbrella Modelling · Internet of Things (IoTs) · Real-life data management system

14.1 Introduction

14.1.1 Genesis and Practice of IoT

The term Internet of Things dates back to the year 1999. Most of the sources believe that Kevin Ashton (Co-founder of MIT's Auto-ID Centre) is the one who coined the phrase "Internet of Things". However, the acronym IoT is deemed to be the later innovation. IoT is one of the burning topics in the IT world now. It is a network of physicals things embedded with software, microchip, sensor etc. which enables immediate access to information about the physical world thereby leads to improvement in efficiency and productivity. In a span of two decades, it has got widespread acceptance across the world.

14.1.2 Opportunities for IoT

The opportunities of IoT are enormous and ever increasing. The Business Insider projects around 24 billion IoT devices shall be installed by the end of 2020 [1]. However, the forecast of other researchers exceeds far ahead. Gartner projected around 25 billion devices by the same timeframe [2].

The IoT led ecosystem has been widely practiced in today economy and it is emerging with higher volumes in various sectors like Aerospace and Aviation, Automotive, Telecommunications, Medical and Healthcare Pharmaceutical, Retail, Logistics and Supply Chain Management, Manufacturing, Process, Transportation, Agriculture and Breeding, Media, Entertainment, Insurance, Mining etc. The Return on Investment (ROI) in IoT segment is projected to touch 13 trillion USD by 2025 [3].

It is predicted that more than half of spending on IoT sector may primarily focus on dedicated and customized manufacturing, transportation, logistics and utility services by 2020 which essentially portray that the future industry would be dominated by high-end transformative technologies [4].

14.1.3 Application of IoT

Over a period of time, IoT has emerged as an indispensable component for the development of every nation worldwide. It is being applied in diverse areas such as Smart Home, Wearable, Connected Cars, Industrial Internet, Smart Cities, Agriculture, Smart Retail, Energy Engagement, Healthcare, Poultry and Farming etc. Many industries like Healthcare, Transportation, Agriculture and Breeding, Media and Entertainment, Insurance, Recycling, to name a few, are increasingly using IoT [5]. Therefore, IoT intervention is inevitable in today's era to foster the growth of economy.

14.1.4 Information and Data Management Ecosystems: Experiences from India

The development of economy essentially relates to its resources, knowledge system, rate of creation of new knowledge and optimal sharing of knowledge and resources for making its dynamic and meaningful application. So, the focal point of supremacy in economic model depends on the sharing of information and knowledge system across the stakeholders to a large extent. In India, the state sponsored institutions including academia and research organizations have been creating high quality knowledge and various forms of information and databases regularly. But it suffers from comprehensive integration of all the knowledge and databases in a harmonious manner. As a result of that the India loses its quality and meaningful application. According to Global Entrepreneurship Index (GEI), 2018, India ranked 68th position out of 137 countries across the globe where India scored least in Technology Absorption (5%) followed by Networking (14%) and Cultural Support (14%) in order to understand the propensity of entrepreneurship in India from global standards [6]. This signifies that in general, India lacks in sharing knowledge and information that essentially has created least performance in absorbing technology from lab to market followed by its culture of creating integrated network or platform for sharing information.

Of late, the State Agencies are concentrating to create nationwide database network for example Shodh Ganga in India for Higher Education, INFLIBNET, various reports of Sample survey or Rounds of NSSO Working Groups etc. However, these attempts are miniscule in comparison to its overall demand.

The availability of integrated knowledge set, the ease of access and its effective use are the pre-requisites for scientific and economic development of the state. The transparency and disclosure of Private Sectors in India are not encouraging in general barring a few large firms. There are instances of dubious information and over-estimations of information revealed by the organizations. The concept of creating integrates and shareable Corporate Database is almost absent in India except miniscule attempts by a few agencies purely for commercial purposes.

14.1.5 Exploring Problems in Information and Data Management Ecosystems

The economy of developing nations is quite different from the developed ones. The firms in India are, in fact, sandwiched by various compelling forces and inhibiting factors. The dynamics of rapid technological advancement, bottlenecks like resource crunch, global competitions and turbulence in policy directions are the indicative examples of such antecedents. All the firms in India do not function on excelling their core competency for fetching higher growth. Many of them suffer from threat perception for their existence, survival and perpetuity. Under these circumstances; it may be suicidal for the firms to share all its information in the name of transparency or disclosure. So, India has become the victim of its inherent inconsistencies and challenges for creating integrated and shareable database system as compared to western world.

14.1.6 Concept of 'Quality Function Deployment' (QFD)

QFD can be referred as a system that attempts to translate the quality parameters of Product, Process and Services as a part of TQM initiative for achieving desired customer satisfaction.

14.1.7 Development of QFD Approach

The works of Akao describes that the QFD approach originated in Japan during late 60s of 20th Century [7]. The QFD initiative was first observed when the Oil Tanker was designed at the Kobe Shipyards of Japan in 1972. Mizuno also used this model to design customer satisfaction framework into a service offering encounter. In the mid of 80s of 20th Century, Don Clausing of MIT introduced this QFD as a design tool to the United States [8]. In fact, QFD is a strategic intervention to unify all the key areas so that the outcome of the process could be excelled and optimized.

14.1.8 QFD's Areas of Application

QFD is applied in diversified fields of application like Production, Product Design, Manufacturing, Information Technology (IT), Engineering, Research and Development (R&D) etc. [9] and other facets of life. It is well sought instrument that may be deployed in the organizational functions that are necessary to assure customer satisfaction which may include business, data management enabler/ ecosystem etc. It is also deployed to achieve quality improvement, its management and to foster 4IR (Fourth Industrial Revolution).

14.2 Review of Literature

14.2.1 QFD

Since 1966, QFD has been extensively practiced by the leading companies across the world [10]. In fact, it is expected that QFD will be considered as effective tool for quality assurance in the information age [10, 11]. In QFD process, it is important to know weights for the customer requirements so as to initiate actions accordingly [12]. For this, a fuzzy Analytic Hierarchy Process (AHP) using extent analysis was proposed to determine the same. Besides, Wasserman also introduced a Decision Model for the prioritization of design requirement during the QFD planning process [13].

14.2.2 Integrated Information and Data Management Ecosystem

Integrated Information System (IIS) can play a crucial role for effective management of agriculture and ecosystem [14]. It is a tool for trouble-shooting, decision making and knowledge management [15]. Also for issues like Climate Change and Environmental Monitoring and Management, IIS is highly essential [16]. Integrated approach can serve as a model for Resource and Environment Management in the coming days.

Lari proposed a model which he believes that the model can serve as a framework for Quality Information Management within organizations [17].

Hua and Herstein iterated that IIS is necessary for successful policy making for the development of education system as it ensures open communication, information sharing and information use [18].

Carlson et al. proposed a system called Integrated Business Environmental Information Management (IBEIM) which efficiently supports and integrates environmental information management for Environmental Management Systems

(EMS) tools, LCA and other environmental process modelling tools, and Design for Environment tools. Through this system, Information and reports can be handled efficiently by organizations regardless of size [19].

14.2.3 Internet of Things (IoT) and Its Application

IoT can be considered as a global network infrastructure composed of numerous connected devices that rely on sensory, communication, networking, and information processing technologies [20]. A foundational technology for IoT is the RFID technology, which allows microchips to transmit the identification information to a reader through wireless communication. By using RFID readers, people can identify, track, and monitor any objects attached with RFID tags automatically [21]. RFID has been widely used in logistics, pharmaceutical production, retailing, and supply chain management, since 1980s [22, 23]. Another foundational technology for IoT is the Wireless Sensor Networks (WSNs), which mainly use interconnected intelligent sensors to sense and monitoring. Its applications include environmental monitoring, healthcare monitoring, industrial monitoring, traffic monitoring, and so on [24, 25].

14.3 Objectives of the Study

(i) To study the importance of Integrated Information and Data Management Ecosystems.
(ii) To propose QFD enabled Umbrella Modelling for Integrated Information and Data Management process through IoT intervention.
(iii) To explore opportunities and challenges for implementing the model in Indian context.

14.4 Research Methodology

This paper is exploratory. The study is based on secondary information. It has been developed reviewing various research papers, reports and using relevant information.

14.5 Analysis and Interpretation

14.5.1 Analysis—I

The importance of Integrated Information and Data Management Ecosystems is enormous. Glimpses of indicative importance are noted below:

- There is lack cross-sectional data on various indicators catering to diversified domains. Even the data are not reliable and regularly published. This leads to inconsistencies in generating panel data.
- In India, there is need of real-time observations in most of the dimensions of economy. Another dimension is the available data set are not generated or published on same reference period. Now-a-days, high precision of real-life data is available that helps to make strategies projections/forecasting of weather conditions which can be shared for agriculture, fishermen working in the river and seas, agriculture practices etc. This minimises both loss of resources and loss of human and domesticated animals through strategic displacement or precautionary measures.
- Academicians, researchers and policy makers can formulate appropriate strategies for the emerging issues in terms of priorities of economy.
- Both the cross-sectional and panel data are helpful for designing both short-term and long-term policy planning in the form of e-governance, investment or implementation strategies. Cross-sectional data is for evaluating certain policy implementation activities.

From various studies, it is found that in spite of having positive relationship between the rate of corporate disclosure and transparency with the firms' net worth and profitability [26, 27] miniscule of firms and mostly the large firms have evidenced their efforts and commitments for corporate disclosure and transparency. The MSMEs are least interested in this area that results lesser confidence among all the stakeholders. On the contrary, the firms practicing higher order of Corporate Disclosure are sometimes questioned in terms of credibility and reliability of such information. The instance of Satyam, Enron, Lehman Brothers etc. are the testimony of such arguments where the firms desperately elevated and over projected the firm's net worth by creating fictitious assets. So, the quality, reliability and credibility of information disclosed by the firms are of paramount importance if the society is committed to have ethical practice and good governance (Fig. 14.1).

It is also important how fast the information has been collected by the firm. If the firm has to devise policies or strategies based on past data, it would be merely the 'System Approach' to management which can solve the problem on 'Reactive Mode'. In contrast to that if the firm is enabled with real-time data management system, the business entities may be strengthened with the ability to have 'Contingency Approach' to management that can 'stop the bleeding' instantly by divulging prospective and proactive mechanism. If the experiences and knowledge system (excepting the critical business secrecy) are shared and exchanged, the society would traverse with greater accomplishment and exposure to progress in the journey of excellence collectively with differentiated individual success story.

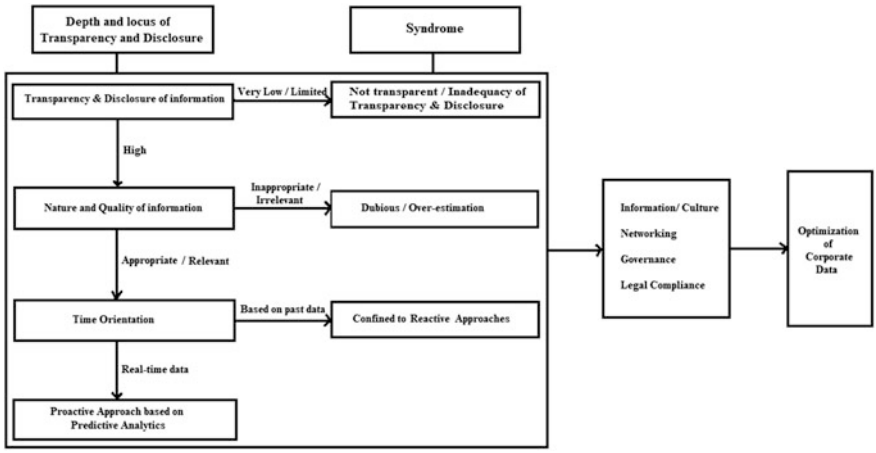
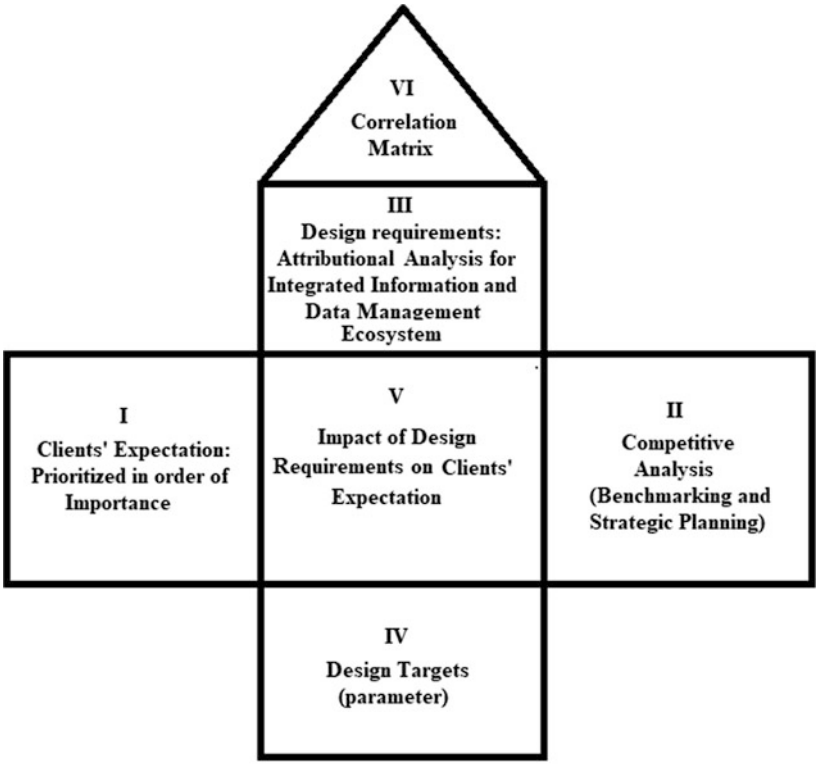


Fig. 14.1 Schematic diagram for rationalizing Integrated Information and Data Management Ecosystem. Developed by the Authors

The holistic development in the process of collectivism without diluting individual identity would have been the ultimate goal of effective and efficient Data Management Ecosystem. The degree of optimization of such process would determine the growth rate of Human Development Indicators. The 'Schematic Decision Box' has been depicted above to understand the depth and locus of Transparency and Disclosure that essentially prescribes for effective and efficient Integrated Information and Data Management Ecosystem.

14.5.2 Analysis—II

Abundance reserve of information and its on-time accessibility may be deemed as the most precious resource in the knowledge economy. The 4IR has empowered the society with the application of IoT that can be guided by developing Non-Human Intelligence through continuous Machine Learning (ML) protocol. The 4IR era enables the system that can interact with each other and analyse big quantum of data which may be collected on real-time basis. It is the high time to integrate and incorporate all the functional KRAs (Key Result Areas) that need to be blended to form a comprehensive ecosystem with the intervention of IoT infrastructure. The functional KRAs are to be embodied in the spirit of Quality Function Deployment (QFD).



House of Quality

The basic structure of QFD as explained in above figure essentially depicts how the QFD system operates in consonance with the voice of customer and the voice of organization divulging the spirit of Competitive Analysis. The relationship matrix helps to identify the designed targets.

The proposed model indicatively may comprise of the following functional KRAs (Fig. 14.2):

- **Real-time Information Recording System**: The devised framework would be able to collect record and retrieve all sort of valued information including research outcomes in the form of formula, copyright or patent etc., on real-time basis with the exposure of IoT led ecosystem.
- **Information Security Protocol and Client-Server Architecture:** The proposed model would instil appropriate Information Security Protocol so that the database would not corrupt or lose due to any malware attack. The system should have high precision 'Client-Server Architecture' so that it ensures free flow of data without any redundancy unless strategically entangled with limited access.
- **Interactive Protocol to develop Artificial Intelligence (AI) and Machine Learning (ML)**: The designed framework would conceptually be reinforced in

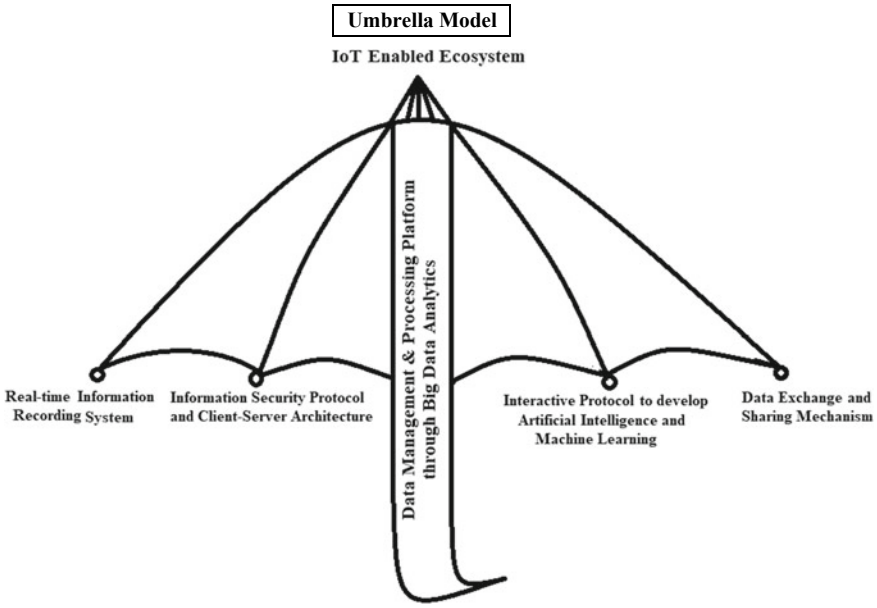


Fig. 14.2 QFD approach for Integrated Information and Data Management Ecosystem: Umbrella Model. Developed by the Authors

such a fashion that the various entities interact with each other at the fullest synergy of permutations and combinations to retrieve meaningful indications/ predictions. The system may be allowed to expose with AI augmented with continuous ML exercises.

- **Data Exchange and Sharing Mechanism**: The purpose of this model is to ensure that all the clients should be able to access, share and exchange the information at the fullest of capacity. This functional KRA would enable to optimise the essence of coordination, consolidation and collaboration among all the stakeholders with the optimum utilization of effective and efficient Data Management System.
- **Data Management and Processing Platform through Big-Data Analytics**: All these KRAs would converge to experience real-time and meaningful interpretation so that the broader dimension of Big-Data Analytics i.e., Descriptive, Predictive and Prescriptive could be achieved holistically for the dynamic problems emerged into the real-life situation. All these competing priorities could be manifested as a fusion of Umbrella Modelling as presented below.

In fact, the QFD approach is of paramount importance in designing an Integrated Information and Data Management Ecosystem. The Quality Functions or the KRAs are to be identified, strengthened and the dynamic form of interactions among the KRAs would create Non-human Intelligence.

14.5.3 Analysis—III

14.5.3.1 Opportunities

The Integrated Information and Data Management Ecosystem has enormous demand for transforming India in terms of economic development, R& D and all other Value Chain functions. The state has concentrated to excel its data infrastructure particularly at the pretext of 4IR. The Union Ministry of Company Affairs, India recently announced to incorporate AI into MCA21 e-Governance service which will make compliance and registration procedures easier. Moreover, it can play a vital role in resolving conflicts as well [28]. The indicative Opportunity Matrix for this Data Revolution System may be identified as follows:

i. Mobile penetration and internet access have been increasing in an incremental rate in India and Mobile Internet has become the pioneer in the access of internet service across the nation. The popularity of Direct Benefit Transfer (DBT) through Aadhar-based Biometric Smart Card has proved successful in Andhra Pradesh [29]. The Integrated Information and Data Management Ecosystem may lead to a massive transformation in the lives and economy of the regions which are remote and away from the central developmental trajectory.
ii. There is a growing trend for emphasizing on Corporate Disclosure in the country which may create gigantic opportunities for comprehensive Data Management System.
iii. In government system, RTI Act 2005 has opened and introduced the process of compulsory information flow on demand of every citizen of the nation. Thus, the Act enforces the government departments to collect, preserve and disseminates the information. However, there is no such Act for Corporate Bodies. The Integrated Information and Data Management Ecosystem would enable to synthesize all sorts of data that necessarily include the basic information of the corporate without intervening the key issues like Patent, Copyright, Business/Trade Secrets etc.
iv. The growing popularity, adaptability and application of IoT have mesmerized the academician researchers and even the users of young generations which essentially creates a platform for sharing multiple and high magnitude of dataset in the public domain or open access forum. If the valuable information is integrated, this could lead the society with fascinating experience and illuminating features.
v. Cutting-edge research depends on the voracity, quality and reliability of dataset and its continuum of data flow. This Pull Strategy would promote the culture and capacity for creating such high-end data infrastructure in the India and across the globe.

14.5.3.2 Challenges

In any study or research, the Opportunity Matrix determines the ease and expectancy mode of any model. But the future expectancy constructs must be complemented and supported by continuous form of tangible and intangible resources. One of the most vibrant factors may be the role of users and the commoners to make it successful. In Indian context, there are few indicative challenges or rather constraints that need to overcome. A subset of challenges are highlighted below:

i. The country suffers from the lack of infrastructure facilities. As 68% of Indians rest in villages [30], it is difficult to bring them in the ambit of the sophisticated and high-end Data Management Ecosystem unless equitable infrastructural development takes place. However, it requires huge investment of financial resources. It is up to the nation to decide on the competitive priorities, that is, what extent the government is committed to value the essence and aspirations of developing Integrated Information and Data Management Ecosystem. Even if all the state and non-actors are unanimous to achieve such landmark, it is practically impossible to develop equitable infrastructure across Pan India within a smaller time frame. The government has been taking initiative consistently. The hallmark of 'Bharat Nirman (2005–09)' initiatives were witnessed to develop the rural infrastructure primarily in irrigation, roads, housing, water supply, electrification and rural telephony [29]. The trend has been fuelled and continued by subsequent governments through their various policy interventions.
ii. India still suffers from adequate competency on a single language platform as it is difficult for the multi-lingual society to learn and practice on English language. The proposed Data Management System may be useful if majority of Indians can read and understand in English language.
iii. The initial investment of such prototype or framework is associated with high cost implementation and that needs to be absorbed by the state and non-state multi-stakeholders.

14.6 Recommendations

The paper has demonstrated how the historical data as well as real-life information and knowledge system can be recorded, preserved, accessed and optimized so that every stakeholder of economy may excel in a mutually benefitting and collaborative manner. The development of 4IR has created enormous opportunity and genuine demand for creating dynamic database infrastructure which would be expected to interact arbitrarily as a form of AI. The implication of this paper may be conceived with the notion how the various forms and facets of data platform can be conjugated, integrated and inter-linked to create an Umbrella-shaped morphology.

14.7 Limitation of the Study

The study intends to formulate a dedicated model for integrating Information and Data Management Infrastructure based on available research inputs and existing frameworks. The model needs to be implemented in a test region i.e., a small district or sub-division where the robustness of the model may be verified. The emerging attributes or concerns during this experimentation process may be explored, identified and incorporated with the existing model framework. Thus, the information ecosystem can be strengthened through continuous development process. However, the model has not been trialled as its present form.

14.8 Conclusion

The world has been progressing through information age where big data analytics has become prolific leader of the millennium. The synergy and synthesis of Artificial Intelligence (AI) based on both panel data and real-life information is the future of our society. The transition and transformation of new generation technology and scientific application essentially depends on the momentum, magnitude and the quality of data storing, preservation, analysis and interaction process through experiential learning and QFD of all the attributes and entities. The fusion of such heterogeneous modalities in a most coherent framework for achieving Integrated Information and Data Management Ecosystem has become the call of the day which needs to be augmented both for developing and developed nations.

References

1. Retrieved from: https://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5. Assessed 27 May 2019
2. Retrieved from: https://www.gartner.com/en/newsroom/press-releases/2015-01-26-gartner-says-by-2020-a-quarter-billion-connected-vehicles-will-enable-new-in-vehicle-services-and-automated-driving-capabilities. Assessed 27 May 2019
3. Internet of Things (IoT). Market Statistics: Use, Cases and Trends (Calsoft) (2018). Retrieved from: https://www.telecomcircle.com/wp-content/uploads/2018/04/. Assessed 27 May 2019
4. Retrieved from: https://www.bcg.com/en-in/industries/technology-industries/making-jump-to-internet-of-things.aspx. Assessed 27 May 2019
5. Bandyopadhyay, D., Sen, J.: Internet of things: applications and challenges in technology and standardization. Wireless Pers. Commun. **58**(1), 49–69 (2011)
6. Retrieved from: https://thegedi.org/2018-global-entrepreneurship-index/. Assessed 27 May 2019
7. Akao, Y.: An introduction to quality function deployment. Quality Function Deployment (QFD): Integrating Customer Requirements into Product Design, pp. 1–24 (1990)
8. Retrieved from: https://strategicdesignthinking.files.wordpress.com/2012/11/hbr-qfd.pdf. Assessed 27 May 2019
9. Retrieved from: https://quality-one.com/qfd/. Assessed 27 May 2019

10. Akao, Y., Mazur, G.H.: The leading edge in QFD: past, present and future. Int. J. Qual. Reliab. Manag. **20**(1), 20–35 (2003)
11. Akao, Y.: QFD: past, present, and future. In: International Symposium on QFD, vol. 97, no. 2 (1997)
12. Kwong, C.-K., Bai, H.: Determining the importance weights for the customer requirements in QFD using a fuzzy AHP with an extent analysis approach. IIE Trans. **35**(7), 619–626 (2003)
13. Wasserman, G.S.: On how to prioritize design requirements during the QFD planning process. IIE Trans. **25**(3), 59–65 (1993)
14. Xu, L., Liang, N., Gao, Q.: An integrated approach for agricultural ecosystem management. IEEE Trans. Syst. Man Cybern. Part C: Appl. Rev. **38**(4), 590–599 (2008)
15. Bravener, L.: AS9000 aerospace basic quality system standard—its origin, and how it compares to ISO 9000. Meas. Control **190**, 163–165 (1998)
16. Fang, S., et al.: An integrated information system for snowmelt flood early-warning based on internet of things. Inf. Syst. Front. **17**(2), 321–335 (2015)
17. Lari, A.: An integrated information system for quality management. Bus. Process Manag. J. **8** (2), 169–182 (2002)
18. Hua, H., Herstein, J.: Education management information system (EMIS): integrated data and information systems and their implications in educational management. In: Annual Conference of Comparative and International Education Society (2003)
19. Carlson, R., Erixon, M., Forsberg, P., Pålsson, A.-C.: System for integrated business environmental information management. Adv. Environ. Res. **5**(4), 369–375 (2001). https://doi.org/10.1016/s1093-0191(01)00088-0
20. Tan, L., Wang, N.: Future internet: the internet of things. In: Proceedings of 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China, 20–22 Aug 2010, pp. V5-376–V5-380
21. Jia, X., Feng, O., Fan, T., Lei, Q.: RFID technology and its applications in internet of things (IoT). In: Proceedings of 2nd IEEE International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, China, 21–23 Apr 2012, pp. 1282–1285
22. Sun, C.: Application of RFID technology for logistics on internet of things. AASRI Proc. **1**, 106–111 (2012)
23. Ngai, E.W.T., Moon, K.K., Riggins, F.J., Yi, C.Y.: RFID research: an academic literature review (1995–2005) and future research directions. Int. J. Prod. Econ. **112**(2), 510–520 (2008)
24. Li, S., Xu, L., Wang, X.: Compressed sensing signal and data acquisition in wireless sensor networks and internet of things. IEEE Trans. Ind. Inform. **9**(4), 2177–2186 (2013)
25. He, W., Xu, L.: Integration of distributed enterprise applications: a survey. IEEE Trans. Ind. Inform. **10**(1), 35–42 (2014)
26. Nandi, S., Ghosh, S.: Corporate governance attributes, firm characteristics and the level of corporate disclosure: evidence from the Indian listed firms. Decis. Sci. Lett. **2**(1), 45–58 (2013)
27. Norbu, T., Chakrabarty, A., Mall, M.: Developing corporate image through increased transparency and trust: financial disclosure in Indian SMEs. In: Manju, Singh, O. (eds.) Business Management Practices New Trends and Challenges, pp. 60–68. Bharti Publications, New Delhi, India (2018). ISBN 978-93-86608-60-4
28. Retrieved from: http://www.mca.gov.in/LLP/dca/help/efiling/bulletin_banks.pdf. Assessed 27 May 2019
29. Chakrabarty, A.: Is India poised for M-commerce in the cashless milieu? In: Duhan, P., Singh, A. (eds.) M-Commerce: Experiencing the Phygital Retail, pp. 205–216. Apple Academic Press (2019). ISBN: 9780429487736. https://doi.org/10.1201/9780429487736
30. Retrieved from: http://rurban.gov.in/about.html. Accessed 24 May 2019

Chapter 15
An Analytical Approach from Cloud Computing Data Intensive Environment to Internet of Things in Academic Potentialities

Prantosh Kumar Paul, Vijender Kumar Solanki and Raghvendra Kumar

Abstract Development and progress both are truly depends on knowledge dissemination and cultivation. Emerging technologies are the key pillar for complete industrial solutions; and ultimately for the building of solid industrial society. Moreover, it is an important step in reaching knowledge society development. Educational programs and courses play a greater role in such development. Social development is purely related economic progress and that is related to the educational delivery. In developing and underdeveloped countries, a true knowledge delivery system helps in the promotion of all respects and shorts. Information Technology is responsible for solid business solutions and improved business, product thus depends on education. Several computing and information technology products were developed in our recent past. Cloud Computing, Green Computing, Data Science, Internet of Things (IoT), Business Analytics, etc. are the important name in this regard and countries like China, India, South Africa etc. are doing well for solid infrastructure development. India is one of the largest educational hubs in the world with about 40,000+ HEIs (Higher Educational Institutes), but still there are lots of programs are missing in Indian academics. However, it is important to note that, India has huge potential to offer Bachelor's, Master's and Doctoral Degrees in these areas with the use of proper and emerging educational policies and strategies. It is some extend true that India fails to offer such dynamic and up-to-date programs in some context. This paper is painted the running programs in India and also depicted possible nomenclature and program with industrial envi-

P. K. Paul
Raiganj University, Raiganj, West Bengal, India
e-mail: prantoshkpaul@gmail.com

V. K. Solanki (✉)
CMR Institute of Technology, Hyderabad, TS, India
e-mail: spesinfo@yahoo.com

R. Kumar
LNCT Group of College, Jabalpur, MP, India
e-mail: raghvendraagrawal7@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_15

ronment and context as per the international trends. The future potential of such program has been depicted with SWOT for making a true Digital India with smartest and effective way.

Keywords Cloud Computing · Big Data Management · Green computing · Virtualization · Analytics and data science · Higher education · India · Knowledge society · Digital India · Corporate universities · Industrial universities

15.1 Introduction

Actual manpower creation and development are depends on universities and educational institutes in different way. Most of the international universities these days are moving towards offering emerging subjects by the use of latest and sophisticated educational methodologies which are sought after in industries and society. Information Science and Technology domain is broad and most interdisciplinary in nature and there are many emerging areas rising, which include Cloud Computing, Big Data Management, Green Computing, Analytics and Data Science, Usability Engineering, etc. Today, apart from the organizations, institutions, the government units are also (around the world) moving towards a huge Information Technology product uses [1]. In India, there are many Government initiatives being undertaken in 1990s to the recent past. Recently in 2015, Government of India has also launched the Digital India Project to make a truly IT enriched and IT enables society. It is a real fact that the shortage of proper manpower in the respective fields in Indian universities and also higher educational institutes in the developing countries is a great factor of underdevelopment of information technology utilization in development (ICT4D). In countries like India, China, Brazil, South Africa, Russia proper steps must required to undertake as remedies for handling shortage manpower in these fields [7, 17]. The educational models and modes etc. need to revamp as per requirement of society and institutions and to build a true society and digital India. In India few programs on emerging computing and information technologies have been started recently in a few universities and institutions in private nature and few governments are also moving [3, 5, 17] in this direction. Internet of Things (IoT) is a system that connects physical objects like sensors node which collects real time data and is accessible through the Internet. Objects are assigned an IP address and this gives them the ability to collect data and transfer them to the server through a network. IoT has capacity to consolidate straightforwardly and consistently, countless heterogeneous frameworks, while giving open access to choose subsets of information for advancement of a whole array of computerized administrations. Building a general engineering structure for an IoT system is thus an exceptionally complex assignment, primarily in view of the substantially large assortment of gadgets, interface layer innovations, and administrations that need to be included in such a framework. In this unique circumstance,

the IoT is assuming an essential part as an empowering agent of a wide scope of utilizations, both for businesses and the all-inclusive communities.

The present study is dealing with conceptual research framework and it is also in theoretical in nature. The study is dealing with the following objectives (but limited to):

- To learn about the rising areas of Information Science and Technology with its brief overview and features etc.
- To dig out the features and educational opportunities of Cloud Computing & Internet of Things, Data Science and Big Data Analytics etc. in International universities.
- To learn about the promising and possible educational models, modes and its availability in the developed countries.
- To learn the current educational models in developing countries; mainly in India with proposed models and education delivery models.
- To learn about the Information Science and Technology integrated Science, Technology, Engineering, Management, Humanities programs.
- To find out core challenges, issues, etc. in the implementation of these emerging subjects and courses in Indian similar territories.
- To learn about the Digital India project recently started in India and the role of these emerging courses to make a true and prosperous Digital India.

15.2 Methodologies

Like any other conceptual and empirical research work in this present study several methods as well as methodologies have been used. The conceptual work and theoretical work deals with review of literature and thus several review materials have been consulted. To study about the current trends in cloud computing, big data, human computer interaction and other emerging domains the general Google Search strategy has been used, here the tag MS/BS Cloud Computing or Data Science etc. respectively have been used. In the search strategy up to 15 pages were considered to learn later about program offering internationally. Moreover to learn latest of the running programs in Indian universities, the websites of UGC, AICTE, MHRD have also been accessed. In this regard UGC considered as the main link to study about approved universities and to move the respective universities. Such links have used to go such universities and become used as Primary source for this research work. Importantly for this study related journals and communications of education, information technology, computing, MIS etc. also utilized.

15.3 Big Data Management

Sciences about the Data may be called as Data Science which is responsible for the collection, selection, processing, management and dissemination of data and similar facets. Recently from different circles large number of data and similar contents have been generated and become an important issue and challenge. Data Science an emerging domain, now and has been arrived to analysis of data and related affairs, including data-creation, sharing, storage and also transfer. Business Intelligence is one of the closest branch of Data Science, however, Big Data Management is also very much close with the domain [2, 4, 6, 18]. Various descriptive statistics including sophisticated information breadth to calculate things are the important criteria for Big Data Management. Today, most of the Industries, organizations are using Data Analytics and all these are driving with the use of compelling Business-Commercial Solutions, and distinguish themselves to the clientele, investors along with regulators. The Analytics market is growing rapidly with Growth Rate of India is about 8%. Various international companies such as Wal-Mart, Target, Citibank, Microsoft, ICICI Bank, etc. (also telecommunication companies like Airtel, Vodafone, and Reliance etc.) are using analytics and data science tools which facilitates and processes and systems. It is a fact that Big Data become an important professional and emerging carrier. Many Universities along with other educational institutes are internationally moving towards offering Data Science programs [8, 10, 17].

15.4 Big Data Management: Current Knowledge Programs and Possible Programs

The data Science practice may deal huge financial support and may reach about EUR250bn per year (according to the McKinsey Global Institute) in all the sectors. In the UK, *Department of Culture, Media and Sports* explained that "The digital economy in the UK is accounts for about £1 in each £10 that the UK market produces every year". There are several bodies and councils have created such as cross-research council 'Digital Economy' or 'Technology Strategy Board' including the 'Connected Digital Economy Catapult', have started their functioning in making digital economy and true sustainability [11, 13, 29, 30]. Apart from Sustainability, now skills become an important part and all these are used for the modeling, multi-disciplinary, data management and numeracy and so on. Most of the international associations, foundations, etc. have mention that the fields of science, technology, engineering and mathematics (STEM) will play more proper role in building of intelligent data systems for mapping healthy information systems [27, 28, 32]. A sophisticated Digital India needs proper Digital Economy and that needs conceptual and skills of knowledge for managing, manipulating large datasets and interprets including representing them as information and knowledge [12, 15, 19].

According to McKinsey Global Institute data 'Data Science is suffering with big data tools and technology'. It has become an important part of the industries, organizations, scientific foundations, etc. Thus, Data Science and Big Data Management become emerging name in the program/course catalogues in the international universities. Some of the nomenclatures of this subject are used:

- Analytics
- Data Science
- Big Data Management
- Data Science and Technology
- Data Analytics
- Data Management and Analytics etc. [14, 16, 19].

United Kingdom is the pioneer in offering Data Science programs as far as this study is concerned. Here are a few programs depicted with universities, duration, eligibility, etc. (Refer Table 15.1).

Table 15.1 The popular Data Science related programs offered by UK based universities

Programs	University	Duration	Incoming branches
MSc-Data Science	Sheffield University	1 year to 2 years	Any bachelor degree
MSc-Data Science	City University, London	1 year to 28 months	Bachelor with Computing/Pure Science/Health/Psychology/ Engineering/Economics/Business etc.
MSc-Data Science	Goldsmith University of London	1 year to 2 years	Bachelor with Computing/Pure Science/Finance/Engineering/ Economics/Business etc.
MSc-Data Science	Lancaster University, UK	1 year to 2 years	Bachelor with Computing/Statistics/ Mathematics/Environment
MSc-Data Science	University of Glasgow	1 year to 2 years	Bachelor with Computing or related subjects
MSc-Data Science	Kings College, London	1 year to 2 years	Bachelor with Computing/Pure Science/Mathematical Science/GIS/ Engineering/Economics/Business etc.
MSc-Data Science	University of Southampton	1 years	Bachelor with Computing/Pure Science/Mathematical Science/ Engineering
MSc-Business Analytics	Imperial College, London	1 year to 2 years	Bachelor with Computing/Pure Science/Mathematical Science/ Engineering/Economics/Business etc.
MSc-Data Science	University College, London	1 year to 2 years	Bachelor with Computing/Pure Science/Mathematical Science/ Engineering/Statistics/Quantitative Science etc.

(continued)

Table 15.1 (continued)

Programs	University	Duration	Incoming branches
MSc-Data Science & Analytics	Brunel University, London	1 year to 2 year or 1.5 years with internship	Bachelor with Computing/Pure Science/Mathematical Science/ Engineering/Statistics/Quantitative Science etc.
MSc-Data Science	University of Essex, UK	1 year	Bachelor with Computing/Pure Science/Mathematical Science/ Engineering/Statistics/Quantitative Science etc.
MSc-Data Science	University of Dundee, UK	1 year to 2 years	Bachelor with Computing
MSc-Data Science	Edinburg Napier University, UK	1 year to 3 years	Bachelor with Informatics, artificial intelligence, cognitive science, computer science, electrical engineering, linguistics, mathematics, philosophy, physics or psychology
MSc-Data Science	Queen Marry University of London, UK	1 year to 2 years	Bachelor with Electronic Engineering, Computer Science, Mathematics or a related discipline
MSc-Data Science	Royal Holloway, University of London, UK	1 year to 2 years	Bachelor with Computer Science, Economics, Mathematics, Physics, or other subjects that include a strong element of both mathematics and computing
MSc-Data Science	University of Warwick, UK	1 year to 2 years	Bachelor with Mathematical Sciences
MSc-Data Science	University of Brikbeck	2 years	Bachelor with Computer or Strong Foundation/Experience in the Field
MSc-Data Science	University of Sussex	1 year to 2 years	Bachelor with Computer Science, Mathematics, Physics, Bio Sciences or other subjects that include a strong element of both mathematics and computing
MSc-Data Science	Heriot Watt University	1 year to 2 years	Bachelor with Computer related Subjects with Database and Programming Subject
MSc-Health Data Science	Swansea University, UK	1 year to 3 years	Bachelor degree but preferences will be for the relevant subjects
MSc-Big Data	University of Stirling, Scotland	1 years	Bachelor degree in relevant subjects
MSc-Data Engineering	University of Dundee, UK	1 year to 2 years	Bachelor with computer related subjects
MSc-Big Data Science & Technology	University of Bradford, UK	1 years	Bachelor degree in computer science, computer engineering, informatics or other computer-related subjects

15.5 Cloud Computing

Cloud computing is a mechanism for virtualized software and hardware availability. Cloud computing depends on the architecture that needs less use of computer, hardware including IT Infrastructure delivery; moreover, it also helps in use of minimum software with utilization of applications [17, 20, 22]. Here hardware, software, services, etc. is coming as Service Oriented Architecture (SOA). Here several types of IT service are coming under one roof, thus organizations and institutions are adopting service of several kinds which are lying on a cloud. Physical hardware, software, applications, etc. are playing a greater role. Green computing strategies are also important for creation of a healthy cloud based systems due to its less involvement in devices and similar systems. It is a popular name after the internet and several tools are released in different sectors. Cloud Computing utilization is possible in remote environment; and it is integrated with several Information and Communication Technology services performed by similar technologies. It is accommodating for the creation of an environment of Grid Computing. Internationally universities are offering several programs on cloud and here with the adopted strategies, we find that UK is a pioneer in offering MSc-Cloud Computing program [18, 21, 23]. The Table 15.3 is depicted its nomenclature, universities and offered modules at a glance. It is a fact that universities are offering programs keeping in mind nature of Cloud Computing with Private Cloud, Public Cloud and Hybrid Cloud Computing models. Cloud Computing related jobs are included (in Table 15.2) but not limited to the following.

Table 15.2 Cloud Computing based job opportunities

Cloud Computing related jobs	
Cloud Administrator	Network Administrator
Cloud Architect	Information Systems Designer
Cloud Data Manager	Cloud Information Analyst
Cloud Web Manager	CIO and CTO
Cloud Network Architect	Director, Cloud Services
Cloud Systems Expert	Network Manager (Cloud)
Cloud Designer	Green Cloud Expert
Cloud IT Infrastructure Manager	Information Administrator

Table 15.3 Cloud Computing programs in international universities (UK)

Programs	University	Core structures
MSc-Cloud Computing	University of Newcastle	**Core**–Big Data Analytics, Distributed Algorithms, Enterprise Middleware, Group Project in Cloud Computing, Cloud Computing, Machine Learning Research Skills, Advanced Programming in Java, **Optional**—Systems Designing/ Information Systems and Trust, **Thesis** etc.
MSc-Cloud Computing	Cork Institute of Technology	**Core**—Cloud Strategy Planning and Management, Computing Research & Practice, Managing Virtual Environments, Data Centre Networking, Cloud Storage Infrastructure, Cloud Security, Software Development with several **Electives**, **Projects**
MSc-Cloud Computing	University of Essex	**Core**—Cloud Technologies & Systems, Computer Security, Converged Networks & Systems, High Performance Computing, Professional Practice & Research Methodologies, **Optional**—E Commerce, Programming, IP Networking and Applications, Mobile and Social Applications Programming, Network Security, Advance Web Technologies, Entrepreneurship, Information Retrieval, **Thesis** etc.
MSc-Cloud Computing	University of Leicester	**Core**—Advance Web Technologies, Internet and Cloud Computing, Service Oriented Architecture, Advance System Designing, Semantic Web, Software Reliability, Software Re-Engineering etc.
MSc-Cloud Computing	National University of Ireland	**To Focus**: Software as a Service (SaaS), Infrastructure of Service (IaaS)
MSc-Cloud Computing	Anglia Ruskin University	**Core**—Computer Networks, OS & Virtualization, Secure Systems, Cloud Infrastructure & Services, Data Science & Big Data Analytics, Research Methods, Major Project
MSc-Computing (Cloud Computing)	Dublin City University	**Core**—Cloud Architecture, System Software, Secure Programming, Cloud Technologies, Network Security, Formal Methods, Research Skills
MSc-Cloud & Enterprise Computing	Nottingham Trent University	**Core**—Advance Software Engineering, Entrepreneurial Leadership & Project Management, Service Oriented Cloud Technologies, Enterprise & Cloud Systems Management, Network & Cloud Security, Research Methods *with Project*

(continued)

Table 15.3 (continued)

Programs	University	Core structures
MSc-Advance Computer Science (Cloud Computing)	University of Leeds	**Core**—(Any Four) Parallel and Concurrent Programming, Cloud Computing, Big Data Systems, Data Science, Bio Inspired Science, Knowledge Representation & Reasoning, Algorithms, Semantic Technologies and Applications, Image Analysis, Scientific Computing, Scheduling, Graph Theory, **Optional**—(Any Three)
MSc-Network Management & Cloud Computing	Middlesex University, Dubai	**Core**—Computer Networks & Internetworking, OS & Application Environment, Network Management, Network Security & Services, Virtualization & Computing, Enterprise Network Trouble Shooting

15.6 Cloud Computing Programs in World Versus India

Cloud Computing programs are with emphasis on Security-as-a-Services, Web-as-a-Services, Software-as-a-Services, Infrastructure-as-a-Services etc. are in high demand. Most of the universities are offering programs on MSc-Cloud Computing though few have started BSc-Cloud Computing. Though, it is difficult to find the program PhD-Cloud Computing. However, PhD thesis on Cloud Computing is offered in most IT/Computing departments [18, 24, 25] in India and other developing nations.

Cloud Computing programs are also available from other corporate players and companies of international level and that may possible to grab by the interested candidates of different countries [26, 31]. Among the programs, few important are included:

- MCSA and MCSE (Private Cloud)
- RHCVA
- CCNA and other Cisco Certification with Cloud Computing and Virtualization Flavor.
- Novel and Oracle Certification in Cloud Computing platform.

Thus, these programs are easily possible to grab by the Indian professionals and seekers. Though full-fledged programs in the Cloud Computing with BSc/BSc/BTech/BE/MTech/ME/MPhil/BBA/BCA/MCA its more or less absent in Indian Educational Institutes. It is important to note that, India is the largest educational system in the world and having 800+ Universities and around 40,000 institutes of higher education offers Beyond School (10 + 2) education. Even around 5000 institutes are engineering/technical colleges. It is also worthy to mention in this context that around 7000 institutes are also under AICTE has management specialization. Hence, as a whole India is a potential country, but programs in Cloud

Computing compare to its possibilities and benefits are limited [24–27]. Only a few institutes are offering programs on Cloud Computing in India, among them few important are listed in Table 15.4.

15.6.1 Possible Programs and Cloud Computing: Indian Context

It is a fact that Cloud Computing and similar programs are available in a few technology institutes (about 10 out of 10,000 institutes). Though, it may offer in several technology domains as a specialization. Engineering degrees may offered with a BS/BSc (Research) focused too. Few proposed programs in Engineering concentration are listed and proposed in Table 15.5.

Cloud Computing is applicable in other areas and places, including the branches of Science, Commerce, Social Science, Management Science case to case basis. Such programs may start easily in the existing department. Few programs have been listed in Table 15.6. It is a fact that most of the universities and colleges in India deals with different subjects and branches, thus related branches are proposed in Table 15.6 herewith.

Table 15.4 Few Cloud Computing programs in Indian universities

Universities	States	Type of university	Programs
VIT University	Tamilnadu	Private-Deemed	MTech-CSE (Cloud Computing)
Amity University	Uttarpradesh	Private-State	MTech-Cloud Computing
Vel Tech University	Tamilnadu	Private-Deemed	MTech (IT Infrastructure and Cloud Computing)
Graphic Era University	Uttarakhand	Private-Deemed	BTech-CSE (Cloud Computing)
University of Petroleum and Energy Studies	Uttarakhand	Private-State	BTech-CSE (Cloud Computing)
Hindustan University	Tamilnadu	Private-Deemed	MCA (Cloud Computing) BTech IT (Cloud Computing) BTech CSE (Cloud Computing)
University of Technology and Management	Meghalaya	Private-State	BTech-CSE (Cloud Computing)
SRM University	Tamilnadu	Private-Deemed	MTech-Cloud Computing
KL University	Andhrapradesh	Private-Deemed	MTech-Cloud Computing

Table 15.5 Proposed Cloud Computing programs of technology concentration in Indian context

Engineering/Technology: Cloud Computing	
BTech/BE/BSc (Research/Tech)-Cloud Computing (CC)	MTech/ME/MSc (Research/Tech)-Cloud Computing
BTech/BE BSc (Research/Tech)-Cloud Computing & Virtualization	MTech/ME/MSc (Research/Tech)-Cloud Computing & Virtualization
BTech/BE BSc (Research/Tech)-Cloud & Green Computing	MTech/ME/MSc (Research/Tech)-Cloud & Green Computing
BTech/BE BSc (Research/Tech)-Cloud & Enterprise Computing	MTech/ME/MSc (Research/Tech)-Cloud & Enterprise Computing
BTech/BE BSc (Research/Tech)-Cloud Computing & Informatics	MTech/ME/MSc (Research/Tech)-Cloud Computing & Informatics

Table 15.6 Proposed cloud computing programs in different concentration in Indian context

Science	Commerce	Social Science	Management
BSc/MSc/BSc (Research)-Cloud Computing BSc/MSc-BSc/ MSc (Research) IT (CC) BSc/MSc/BSc/ MSc CS (CC) BSc/MSc/BSc/ MSc-IS (CC) BSc/MSc/BSc/ MSc-SE (SaaS) BSc/MSc/BSc/ MSc Networking (IaaS)	B. Com/M. Com. (Cloud Computing and Management) B. Com/M. Com (E-Commerce with Cloud) B. Com/M. Com (Cloud Business) B. Com/M. Com (Cloud & Green Accounting)	BA (Digital Humanities with Cloud Apps) BA (Social Informatics with Cloud Apps) BA-Economics (Digital Internet Economy)	BBA (Cloud Systems Management) MBA (Cloud Business Management) PGBDA (Cloud with Big Data Management) PGDM (Cloud & Digital SEO)

15.6.2 In Science and Computer Applications

The nomenclature of Information Technology is available with BSc, MSc degree and Computer Science are also available with BSc, MSc, MPhil degree. Another subject Computer Applications is also available with BSc, MSc. The nomenclature of Software Engineering, Information and Communication Technology are also offered in wide numbers of colleges. Thus the Human Computer Interaction and UE programs may possible to offer as a specialization in the exiting branches or specialization [9]. Though based on availability of physical infrastructure, intellectual infrastructure, availability of future students (keeping in view placement related affairs), the HCI or UE program may offer as a complete and full-fledged degree.

In the Computer Application nomenclature, apart from BSc, MSc another degree is most popular i.e. Master of Computer Applications (MCA). Presently 1459

number of institutes are offering the MCA with total intake of 110,585. Though still, specialization is not at all offered and proposed in AICTE. And thus most universities not offered specialization at this level, but the degree of **MCA** may offer as Human Computer Interaction/UE/UXD etc. [24–27]. And similarly **BCA** (Human Computer Interaction/UE/UXD/Human Centered Computing etc.) may also offer. Hence, starting of the programs are not at all big deal or tough.

15.7 Digital India and Social Development

Government of India launched several IT and Computing projects apart from recent (2015) 'Digital India' program. The main aim of the 'Digital India' includes building an IT enable information society. Center of 'Digital India' program has depended on following official agendas:

- Broadband Highways.
- Universal Access to Mobility.
- Public Internet Access Program.
- E-Governance—reforming Government by the technology.
- E-Kranti—the electronic delivery services.
- Information for All.
- Electronics Manufacturing.
- IT for Jobs.
- Early Harvesting Program.

There are 44 missions/agenda under the E-Kranti. The following figure will be helpful to learn about the common services offered by the E-Kranti. This is most flagship program of the 'Digital India' project. Figure 15.1 is depicted the Cloud, applications in modernizing and building Digital India as much as possible.

Communication infrastructure building is also an important agenda of 'Digital India' and here broadband backbone at Pan India basis is proposed and considered vital. *BharatNet*; has come up with new agendas, it is world largest rural broadband system with more than 2.5 lakhs of Gram Panchayats connectivity. For the Aadhaar based services, NREGA, Common Service Centers (CICs), Rural Banking, Information delivery etc. *BharatNet* is important and valuable.

Another important and valuable implementation in Communication segment is—*BSNL NGN* (Next Generation Networks). This is a packet based network and helps in several types of objects such as Voice, Data and Multimedia in one landline.

E-Sign is another cloud enriched application that facilitates an Aadhar holder to digitally sign a document. The current method is in-personal physical presence; but the e-sign will give the freedom physical presence.

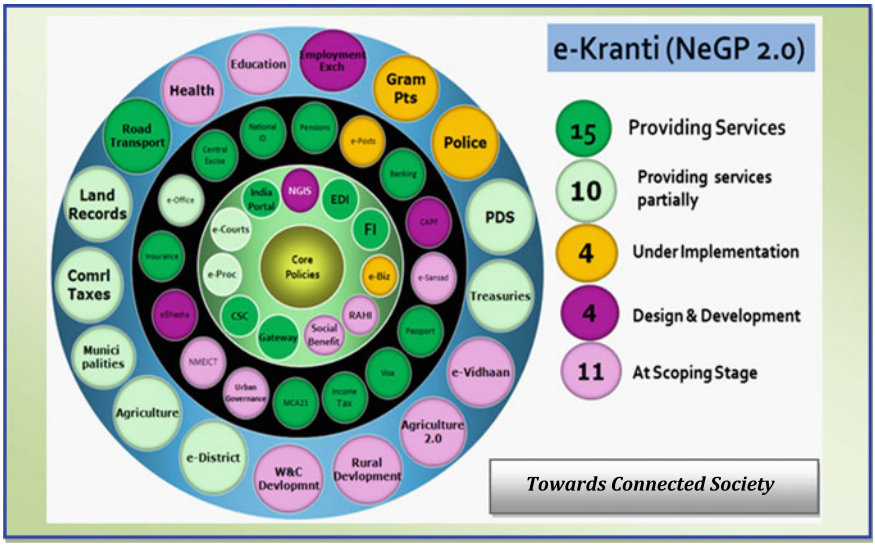


Fig. 15.1 e-Kranti Cloud platform of Digital India program

Digital India Platform (DIP) is a cloud enable platform that designed to keep digitalization of manual document and all the information and content are stored. It is registration and payment based.

Digital India Mobile Apps is provides easy access to information by the advance phone or smart phone. In cloud environment it is provides a virtual link and more make ready for almost all the OS version like Android, iOS, and windows.

The **My Gov Mobile App** is another which provides a variety of Crowds sources initiatives such as job creation, skill India development etc.

Swach Bharat Mission App is also Cloud enable for the promotion of 'Cleaning and greening'. And the aim and agenda will get both board based and localized and reach the people across India.

India's rank in IC application in Public Administration in 2012 was 125; down from 119 in 2010 (In respect to United Nations E-Government Development index). Hence newly launched cloud-based government services, has huge opportunities for promoting e-Governance and similar services. National Knowledge Network, National Informatics Center Network (NICNET) and other services are important steps for ICT4D the latest Storage Area Network data centers and State Wide Area Networks (SWANs) are being established in all most all the territories which includes; 35 states/UTs for promoting digital infrastructure.

The important fact is, 'Cloud Computing' is also associated with latest agenda of the Government of India, IT for Jobs and thus proving solid environment is urgently needed for building cloud enable ICT4D. Here the development of manpower is

highly required. All the services have mentioned above needs proper and sophisticated internet and network connectivity and here Cloud Computing' enable services are required.

Open Data platform, Social Media Engagement and Online Messaging is based on additional resources for information and content sharing; these are also directly and indirectly related to the Cloud Computing and similar activities.

15.8 Building a True Digital India vis-à-vis Need of Big Data Management, Cloud Computing

Thus, for building a true Digital India, we need to start educational programs on a variety of educational programs and degrees. Each of the proposed technologies such as Big Data Management, Cloud Computing and Human Computer Interaction/Usability Engineering to be utilized in large manner [24]. Though among the burden of solid implantation of these technologies few important are included:

- Less awareness among the common people to use these technological products and services.
- Fewer initiatives by the public administration and Government.
- Less awareness and unwillingness towards implementation of technologies in the common services and public governance.
- Minimum research and innovation of integration of the Technologies in the Service Science products and services.
- Availability of very minimum educational programs at higher levels, such as Bachelor Degree, Masters Degree, Doctoral Degrees etc.
- Less and minimum skill manpower in the areas of Cloud Computing, Big Data Management, HCI-Usability Engineering etc.

This way the Government of India and State Governments (28), Union Territories, NCR and other governing regions need to implement Cloud-Big Data-HCI Technologies in the practice areas and also in the need to take the proper steps for launching Cloud-Big Data-HCI Technologies training, educational programs for solid development of the society.

If we see some of the initiatives and steps, then, we may note that The Tamil Nadu government will select 100 entrepreneurs and train them in Cloud Computing and Mobility technology. The government will also train college students. Moreover, it is estimated that 10 lakh teachers and 60 lakh students across 1500 institutes over the next 18 months will be benefited from the local Microsoft Cloud in India as far as Tamilnadu is concerned.

Multinational and reputed organizations have also started a project for social development and among these Facebook started Free-Basics were important. In October, 2015 Google had announced to build a Wi-Fi system (Green and Eco

supported) in the selected places for the promotion of digital humanities and information systems. Cloud-Big Data-HCI Technologies have a huge market in India and there is an urgent need of offering such educational programs in a large number of engineering colleges, universities or with tie-ups with foreign universities or industrial sectors for real and fast implementation. Hence, this will also help to the focused users to take advantage of the several types of benefits of advanced capabilities.

15.9 Suggestion and Further Possible R&D

Cloud-Big Data and allied technologies are possible starting in several capacities and settings. All the technologies are better to start in collaboration and following steps may be followed:

- Apart from Full Time and fixed timing and schedule, such programs may be started in the other flexible mode of learning, timing flexibilities (with the same amount of timings/credits etc.).
- Cloud-Big and allied technologies related programs may be started in collaboration with the industrial units on the concerned subject and a particular term or subject/s may be offered by joint venture.
- Programs may also offer in Online mode for the collaborative manpower development and especially for the corporate seekers.
- Cloud-Big Data and allied technologies may be offered in a multi-institutions in nature where program taught in interdisciplinary culture.
- Proper organizational, institutional and academic collaboration is highly appreciated to prepare industry ready and social informatics practitioners for building a true Digital India.
- Cloud-Big Data and allied technology programs need to offer in consultation with the industry players to prepare relevant manpower.
- Issues and challenges need to resolve by taking the proper steps and measures for starting program on an international level, international nomenclature, interdisciplinary culture, collaboration etc.
- Program of Cloud-Big Data and allied technologies are purely skill based and may start in collaboration with other departments and centers in numerous available higher education units as depicted in Table 15.7.

Table 15.7 Possible institutions where Cloud-Bigdata-HCI related technologies may be offered; individually in related departments or with collaboration with other departments, if needed [24–27]

Universities and others Higher Educational Institutions (HEIs)	The numbers	Remarks with Cloud Computing and Big Data	Remarks with HCI and UE
Institute of National Importance			
Indian Institute of Technology [IITs]	23	Possible in CSE/ CA/IT Departments	Psychology/ Management (with Psycho experts) collaboration preferred
Indian Institute of Information Technology [IIITs] *established as INI*	04	Possible in CSE/ CA/IT Departments	Psychology/ Management (with Psycho experts) collaboration preferred
Indian Institute of Information Technology [IIITs] *established by other means with care from GoI*	17	Possible in CSE/ CA/IT Departments	Psychology/ Management (with Psycho experts) collaboration preferred
National Institute of Technology [notes]	31	Possible in CSE/ CA/IT Departments	Psychology/ Management (with Psycho experts) collaboration preferred
School of Planning and Architecture [SPAs]	03	Program with Cloud Architecture is possible	Psychology/ Management (with Psycho experts) collaboration preferred
Indian Institute of Management [IIMs]	19	Program with Cloud System Management	Psychology/ Management (with Psycho experts) collaboration preferred
Indian Institute of Science Education and Research [IISERs]	07	Program may on Research Focus	Psychology/ Management (with Psycho experts) collaboration preferred
Academy of Sciences and Innovative Research	01	The program may on Research Focus	Psychology/ Management (with Psycho experts) collaboration preferred
Indian Institute of Engineering Science and Technology [IIEST], Shibpur	01	Possible in CSE/ CA/IT Departments	Psychology/ Management (with Psycho experts) collaboration preferred
Other Higher Educational Institutes			
Central Universities	46	Possible in CSE/ CA/IT Departments	Psychology/ Management (with Psycho experts) collaboration preferred

(continued)

Table 15.7 (continued)

Universities and others Higher Educational Institutions (HEIs)	The numbers	Remarks with Cloud Computing and Big Data	Remarks with HCI and UE
State Universities (Funded)	342	Possible in CSE/ CA/IT Departments	Psychology/ Management (with Psycho experts) collaboration preferred
State Universities (Privately Funded)	239	Possible in CSE/ CA/IT Departments	Psychology/ Management (with Psycho experts) collaboration preferred
Deemed Universities	125	Possible in CSE/ CA/IT Departments	Psychology/ Management (with Psycho experts) collaboration preferred
Affiliated Colleges	30,000+	Possible in CSE/ CA/IT Departments	Psychology/ Management (with Psycho experts) collaboration preferred
Management Colleges	3217	Possible with management/IT expert or division collaboration	Psychology/ Management (with Psycho experts) collaboration preferred
Computer Applications Colleges	6375	Possible in CA and if needed other related departments	Psychology/ Management (with Psycho experts) collaboration preferred

15.10 Conclusion

Emerging technologies such as Cloud Computing, Big Data technologies, Human Computer Interaction, Usability etc. are most valuable for the creation of intelligent Information infrastructure. The development of the organizations and institutions with cloud integration within the existing systems is positively possible with the Cloud Systems. In information and knowledge society, computing and information technologies played a lead role for different sectors viz. Healthcare, education, tourism, business and commerce, governance, etc. Initially, only the private companies and institutions were engaged in the cloud computing in, today, many Government agencies are offering cloud services as well as cloud enriched product supported by different platforms and models viz. Public cloud, private cloud, hybrid cloud empowered with IaaS, PaaS, SaaS, etc. It is a fact that proper policy and regulation, including the framework with adequate man are must for a sustainable development but countries like India has limited space and initiative of this space. Though better initiatives from both Government and private sectors are highly solicited, and this is continuing. Preparation of Human resources and skill

manpower are the need of the hour. Universities, educational institutes and other organizations are moving towards the creation of new age programs for solid development of society and organization. India is a home to a large number of Higher Educational Institutions (HEIs) and this is increasing rapidly. Apart from the traditional subjects and streams, HEIs are also started in the new age program slowly. Private players have done a good job in this context for the development of new age and industry focused, specialized programs. Central Universities, and Institutes of National Importance (INIs) needs to change their perception of these emerging programs and here in this paper proposed courses, programs may help in the development of digital societies and humanities; moreover creation of the skilled manpower may help in building a true Digital India.

References

1. Altbach, P.G.: Research and training in higher education: the state of the art. HEE **27**(1–2), 153–168 (2002)
2. Annand, D.: The problem of computer conferencing for distance-based universities. Open Learn. **14**(3), 47–52 (1999)
3. Bhattacharya, I., Sharma, K.: India in the knowledge economy—an electronic paradigm. IJEM **21**(6), 543–568 (2007)
4. Buyya, R., Ranjan, R., Calheiros, R.N.: Modeling and simulation of scalable cloud computing environments and the CloudSim toolkit: challenges and opportunities. In: International Conference on High Performance Computing & Simulation, 2009. HPCS'09, pp. 1–11. IEEE (2009)
5. Calheiros, R.N., Ranjan, R., Beloglazov, A., De Rose, C.A., Buyya, R.: CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Softw.: Pract. Exp. **41**(1), 23–50 (2011)
6. Clemons, E.K.: Information systems for sustainable competitive advantage. Inf. Manag. **11** (3), 131–136 (1986)
7. Davenport, T.H., Prusak, L.: Information Ecology: Mastering the Information and Knowledge Environment. Oxford University Press (1997)
8. Dikaiakos, M.D., Katsaros, D., Mehra, P., Pallis, G., Vakali, A.: Cloud computing: distributed internet computing for IT and scientific research. Internet Comput. IEEE **13**(5), 10–13 (2009)
9. Foronda, V.R.: Integrating information and communication technology into education: a study of the schools project in Camarines Sur, Philippines. J. Dev. Sustain. Agric. **6**(1), 101–113 (2011)
10. Gurbaxani, V., Whang, S.: The impact of information systems on organizations and markets. Commun. ACM **34**(1), 59–73 (1991)
11. Harmon, R.R., Auseklis, N.: Sustainable IT services: assessing the impact of green computing practices. In: Portland International Conference on Management of Engineering & Technology, 2009. PICMET 2009, pp. 1707–1717. IEEE (2009)
12. Hooper, A.: Green computing. Commun. ACM **51**(10), 11–13 (2008)
13. Karthikeyan, N., Sukanesh, R.: Cloud based emergency health care information service in India. J. Med. Syst. **36**(6), 4031–4036 (2012)
14. Kettinger, W.J., Lee, C.C., Lee, S.: Global measures of information service quality: a cross-national study. Decis. Sci. **26**(5), 569–588 (1995)
15. Kumar, K., Lu, Y.H.: Cloud computing to mobile users: can offloading computation save energy? Computer **4**, 51–56 (2010)

16. Melville, N., Kraemer, K., Gurbaxani, V.: Review: Information technology and organizational performance: an integrative model of IT business value. MIS Q. **28**(2), 283–322 (2004)
17. Paul, P.K.: Green information science: information science and its interaction with green computing and technology for eco friendly information infrastructure. Int. J. Inf. Dissem. Technol. **3**(4), 292 (2013)
18. Pau, P.K., Dangwal, K.L.: Cloud Computing Based Educational Systems and its challenges and opportunities and issues. Turk. Online J. Distance Educ. TOJDE **15**(1), 89–98 (2014)
19. Paul, P.K., Chatterjee, D., Rajesh, R., Shivraj, K.S.: Cloud computing: overview, requirement and problem in the perspective of undeveloped and developing countries with special reference to its probable role in knowledge network of academic field. Int. J. Appl. Eng. Res. **9**(26), 8970–8974 (2014)
20. Schmidt, N.H., Erek, K., Kolbe, L.M., Zarnekow, R.: Towards a procedural model for sustainable information systems management. In: 42nd Hawaii International Conference on System Sciences, 2009. HICSS'09, pp. 1–10. IEEE (2009)
21. Subashini, S., Kavitha, V.: A survey of security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**(1), 1–11 (2011)
22. Wang, D.: Meeting green computing challenges. In: Electronics Packaging Technology Conference, 2008. EPTC 2008. 10th, pp. 121–126. IEEE (2008)
23. Watson, R.T., Boudreau, M.C., Chen, A.J.: Information systems and environmentally sustainable development: energy informatics and new directions for the IS community. MIS Q. 23–38 (2010)
24. http://www.digitalindia.gov.in. Accessed 10 Oct 2016
25. https://www.ugc.ac.in. Accessed 10 Oct 2016
26. http://www.aicte-india.org. Accessed 10 Oct 2016
27. http://www.mhrd.gov.in. Accessed 10 Oct 2016
28. http://www.siliconindia.com/magazine-articles-in/25_Most_Promising_Cloud_Computing_Companies-LUBO681173186.html. Accessed 10 Oct 2016
29. https://en.wikipedia.org/wiki/data_science. Accessed 10 Oct 2016
30. https://en.wikipedia.org/wiki/Big_data. Accessed 10 Oct 2016
31. https://en.wikipedia.org/wiki/Cloud_Computing. Accessed 10 Oct 2016
32. https://en.wikipedia.org/wiki/Human_Computer_Interaction. Accessed 10 Oct 2016

Part V
IoT in Data Analytics

Chapter 16
IoT Data Management, Data Aggregation and Dissemination

T. Joshva Devadas, S. Thayammal and A. Ramprakash

Abstract The Internet of Things (IoT) paves the way to interact with the smart objects namely sensors, hardware, circuits and software. Research in IoT ensures that collecting, processing and distributing the data needs to be improved to carryout data aggregation, processing and dissemination tasks of IoT data management. Data Processing focuses on the characteristics Velocity, Volume, Variety, Variability, and Veracity. IoT Data Management may further be categorized as Communication, Storage and Processing. Data communication involves data processing among objects, sensor data and hardware. To store the data, Cloud or distributed storage is used and processing involves filtering and analytics. Data dissemination distributes the processed data to end users. Message-delay in multi-hop massive IoT network is significantly optimized. This chapter enumerates the IoT data management frameworks, challenges and issues. Also, deployment of IoT Data management for smart home and smart city is described.

Keywords IOT data management · Data aggregation · Dissemination · Data processing · Data communication · Data storage

16.1 IoT Introduction

In the real-world application everything is automated and digitized. Hence everywhere competition raises that causes reducing time over time. Significant contribution gained by Social Media to transmit data around the world. Big Data and Mobility renders its role by computing, analyzing, classifying instance of the data and transfer it to the destination with mobile services. Thus rise in digital technology need to imagine the

T. Joshva Devadas (✉)
Department of CSE, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India
e-mail: joshvadevadas@gmail.com

S. Thayammal · A. Ramprakash
Department of ECE, Kalasalingam Institute of Technology, Krishnankoil, Tamil Nadu, India

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_16

future of everything. To Bridge the gap between Today and Tomorrow Use of Objects, Software defined storages, leverage Infrastructure, Data driven security, Academic Alliance and Agent Technology are the constructs by which the existing system should be upgraded to withstand with the technological development. Each of these constructs should be addressed, analyzed and are configured to the existing technologies. Change in technology has major challenges to carry out the structural imbalances, manage to cut the operational cost, execute the system with balanced risk, high data availability, pre-processing/processing of unstructured data, must facilitate interdisciplinary data processing, scalability and affordability.

To meet out the challenges with growing technology in handling or managing or aggregating data all through the digital transformation, one way is to connect the functional elements of a system that have distinct identities through internet. Such connection of identical devices is referred as Internet of Things (IoT). Moreover, in this new era of IoT, the 'things' connecting the devices that are not associated with internet are configured, controlled and networked with varying communication protocols the devices communicated using IP networks. Many Applications use IoT to connect people with IoT or Things with Things. Also, the IoT has ability to transfer information over the network without human intervention. IoT works based on Anything, Any Time and Anywhere principle. Anything may refers to application data (app) or an interface (API) or a thing or data can be accessed through IoT. At anytime means that data can be processed either in batches or real-time or streams. Anywhere refers to the data that can be accessed from anywhere either at on premises or cloud or hybrid. The basic functional elements and operations involved in IoT are as depicted in Fig. 16.1.

From Fig. 16.1, it is observed that the IoT systems has five important phases and are listed as follows:

i. Sensors and/or Actuators
ii. Data acquisition system and Internet Gateway
iii. Edge IT (Edge Computing)
iv. Cloud and Data center
v. End User.

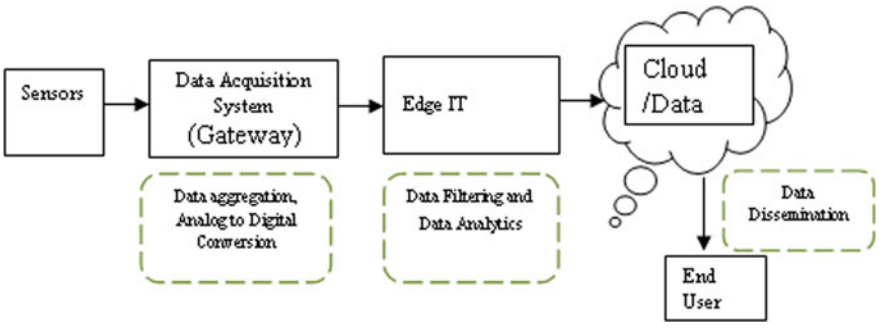


Fig. 16.1 Basic elements and processing steps in IoT system

16.1.1 Sensors and/or Actuators

Sensors and actuators have played significant role as sources in IoT applications. They generate IoT data by recognizing, identifying, measuring, quantifying and qualifying the target objects. IoT data sources are categorized into three types namely active, passive and dynamic sources. In the active source, sensors stream the data constantly. Optimum IoT sparse data aggregation and Dedicated IoT data communication is needed to reduce the data loss. In the passive source, sensor needs to be activated for sending the IoT data. So it transmits the data only when the request arises. It is low power sensor and preferable to use in remote area. In the dynamic source, sensors have the capability to transmit and receive the data. Also it has the capability to change the produced data, data format and frequency. Hence all the dynamic sensors are auto configurable. Also depending upon the produced data, sensors are classified as analog and digital sensors. However, sensors are chosen based on applications. Machine vision or Optical ambient light, Identification of Leakage Level, classify the water flow level, categorize the position/presence/proximity of the finger print, recording of Temperature are some of the applications of sensors. These application may use any of the following sensors available in the market based on the chosen application. The sensors are 7colorflash, IR emission, Photo resistors, IR receiver, Heart Beat, Digital Temp, Temp and Humidity, Laser emit, RGB LED, Light Blocking, Tilt Switch and Touch Tracking.

16.1.2 Data Acquisition System and Internet Gateway

The sensors generated data are aggregated and converted into digital form by Data acquisition system. The data acquisition system plays vital role to manage the data in IoT environment. The converted digital data is transferred to next phase through the internet gateway for edge computing. Internet gateway is connected to edge by means of Internet, Wi-Fi, Bluetooth and LAN.

16.1.3 Edge Computing

After data aggregation and digital conversion, the data is streaming into edge computing. However, it is necessary to further process the data before it reaches the cloud. Here, the edge IT performs the necessary data processing and analysis. The edge computing system is located nearer to sensors. Without, edge IT system, the cloud/data center need abundant resources (network bandwidth, capacity, security issues and storage in cloud) and also causes delay in data process. Hence, Edge IT pre-processes the data into meaningful information. For example, instead of sending

the water quality data directly to data center, can aggregate and convert the data and analyze it, finally send to cloud about any impurity present or pH level of the water.

16.1.4 Cloud and Data Centre

Cloud and Data centre is the core IT of the IoT environment. The demand of network resources for core IT is reduced by decentralized model of deployment called Edge Computing. Cloud is used to store the data more securely. Data centre performs the depth processing of the data and analyze it from various sensors. Also the data center is used to manage the data for further transmission to end user or securely stored in cloud for later retrieval.

16.1.5 End User

The end user is last phase in the IoT data cycle. Depending upon the applications the useful information is passed to end user or stored in cloud for later utilization. So the end user phase is an optional one in the IoT environment.

Research works have been developed in each of the elements in IoT system in the thrust areas of IoT on Software Technology, Cost of Hardware and Communication Technology and Low Power Consumption. Though much of the research works are proposed in IoT for creating an anisotropic environment, aggregation, processing and dissemination focus on the data needs to be improved. Data Aggregation, Processing, and Dissemination are the significant landmarks in Data Management of IoT environment. In this chapter, Sect. 16.2 describes the IoT data and its types, characteristics and aggregation. Section 16.3 explains in detail about the Data Management, Data Management Issues and Challenges. Section 16.4 brings a discussion on data aggregation and dissemination. The chapter concludes with the description on Smart home and smart city framework.

16.2 IoT Data

In IoT the sensors detect and respond to the input from the physical environment. The output of the sensor transmits signals called as sensor data and that is used for further processing.

16.2.1 Types of Data

The sensor data is classified depending upon application in which IoT is used [1]. Depends upon the classification of the data, IoT data can be categorized into discrete, continuous, auto generated and humans input. Further, the data is categorized based on applications such as environmental data, positional and, sensor data, historical data, RFID, descriptive data, address/unique identifiers, physics models, and command data.

RFID Data
RFID data helps to identify and track radio signal waves that transmit and receive data through the tags attached with the objects. It encompass IC and Antenna to store and transmit signals. The RFID reader read the data and communicates wirelessly with the tag associated/attached with the object. It incorporates cheaper technology that causes many to use in the applications such as passport, logistics, supply chain management, road tracking and health care systems.

Access and Unique Identifier
Objects are identified with unique IP address. The number of objects used in IoT application proportionally increases the number of Identifiers. In the early stage, IPV4 is the protocol used with 32 bit address. IPV6 has advantage over IPV4 with 128 bit address, larger address space than IPV4. Identification is enhanced through a hierarchy naming structure defined by Internet Assigned Number Authority (IANA) that domain names and internet protocol related assignments, management of root zone and allocation of global IP address.

Descriptive Data About Objects, Process and Systems
The power of IoT comes from the usage of data or metadata, systems and the objects involved in the process. Data about data is metadata, that access appropriate data with the additional definition present with the metadata information.

Positional Data and Pervasive Environmental Data
Global Positioning System (GPS) and Local Positioning Systems (LPS) are used to locate a particular tagged object. Implementation of GPS is done with the help of multiple satellites sending signals to the control unit of the objects to locate its positions. Local Positioning system works in the similar fashion with minimal coverage. In the small areas, positions can be obtained from locally placed sensors and transmitters and they in turn used to locate the position by collaborating with GPS. IoT components present in the object may be of static or mobile. In such case, positional data play a significant role and a challenging one to locate the object. A new type of information named pervasive location information that describes each environment that is unobtrusively available to support interactions with the surroundings. Such information is location dependent. The concept of Internet of Places is readily available to pick up the information, precise to the location. Ambient Technologies, Geographical Information Systems and Mobile computing make use of such available information for further processing.

Sensors Data-Multi Dimensional Time Series Data
Data enters to the IoT through wireless sensor network. Weather, temperature, and noise are few of the monitoring systems that use wireless sensor networks to monitor the environment. Data may be captured either continuously or at regular intervals or when it is queried. Sensors and Grid technology are used to capture vast amount of data quickly, but querying and mining be achieved only during the real time analysis.

Historical Data
Data becomes historical as time passes and the volume becomes a challenge. During the design of the application decision on how and which data should be retained is determined. Depends upon the scenario of the system either frequently referred data for querying or structures with minimal access is retained. In either cases time needs to be captures to resolve the issues like loss of data, inaccurate recording and missing information. Data archiving successfully offer solutions to adapt IoT.

Physics Models
The physics model representing, the modeling and simulation of physical scenarios using the model templates for reality. For example force, instance gravity, magnetism, sound and light. The IoT based applications can access these models, use it in algorithms, deploy them in games and computer aided engineering arenas with the objective of enhancing its functionality.

Actuators and Command Data
The IoT use actuators of the device to control remote devices by accepting the command given from the remote place. To do this, an internet enabled actuators should show the state of the device thus by saying whether it is ready to use or not. Using an appropriate interface and the language one might easily control the device to implement the action. Since there are many devices participating in the IoT have different origins, defining a common command interface across the system is not possible. So standardizing the command/control data and interface is the most challenging task.

16.2.2 IoT Data Characteristics

While considering IoT data characteristics Velocity, Volume, Variety, Variability, and Veracity are the 5V's are considered to describe the characteristics of IoT Data [2–4]. Data derived from the Tags are substantially very large that describes the volume of the data generated. As Sensors interact with RFID tags generate large amount of data results in fulfilling the digital processing feasibility. Velocity of the data depends on the type of the sensors being used. Data source and the type of the sensor used to collect the data determine the velocity of the data. Variety of data emitted through the tags is structured, unstructured, semi-structured and mixed data.

Data collected should be stored and should have a database design that dynamically adapts the data format needed for further processing. Veracity ensures unauthorized access and offers secured services to ensure authenticate access to the data thus by ensuring trusted service. Improvements brought on the quality of the sensor also improves the veracity of the data in IoT. The data dynamicity is described by the term variability which refers the variation in data while processing or analyzing.

16.2.3 IoT Data Challenges

Role of sensors in IoT becomes inevitable in the recent growth in technology. Data generated through the sensor is increasing at a huge exponential rate. Exponential growth of the data may increase problems in addressing the issues of Heterogeneity, Scalability, Timeliness, Complexity and Privacy of the data in handling with very large data set, will slow down the progress in all the phases of data processing pipeline. With the wide-range of increase in data generated through IoT based applications is complex, less structured and becomes mandate to process it quickly to meet out the enormous requirements in turn create challenges in traditional database. To provide/deliver continual services to research community, cross-discipline collaborations with adequate governance model, needs to consolidate e-Infrastructure platforms by upgrading the architectures. Such huge data generated have to manage and analyze it by deploying distributed architectures and processing the data in parallel. The management of huge data categorizes its challenges in populating, querying and managing the database. Above all addressing the problems in data communication and cost of communication becomes key issue in handling the data along with the predicted issues. Network features like bandwidth and latency gains the momentum in addressing data communication between client and the data server and to minimize the communication cost that is higher than the processing cost require additional storage to reduce the communication cost relatively.

16.3 IoT Data Management

Growing technology increases in use of sensors surround people and their living. IoT works together with people, homes, factories, industries, workplaces, farms, vehicles and cities. Emergence of IoT plays role in product design, health monitoring, weather forecast, wearable devices to track the behavior/location of a person, tracking of goods, fire safety and beyond. All these devices create noise by transmitting and receiving huge amount of information. Considering these data for further processing may require the data to be managed by means of designing, developing and executing data management architectures. Further, defining policies, protocols and procedures that suits for processing should be well defined.

Challenges in managing, displaying, extracting from data stored on server for IoT applications takes longer time, so for data processing, a separate layer is used to 'cache' the fields of frequently referred database queries [4]. Focus on research areas of data management to optimize the communication overhead and impact on energy consumption over storage management was illustrated along with the life cycle of data management of internet is discussed [5]. In [6], the proposed method is used to design the structured layer for the heterogeneous mobile data sources. This structured layer is the solution for the problem of enabling query of frequently updated data from mobile sensing sources. Also this method is used to querying frequently updated time stamped and structured data from data sources. The author [7] highlights the data management solutions, design primitives, data management frame work for IoT along with the design elements that offer comprehensive IoT data management solutions. The multi-sensor object tracking (MSoT) data is efficiently stored on HDF's using read/write [8]. The memory-write throughput, disk-write throughputs are described for performance measures. The author [9] proposed a framework called DeCloud-Real Base to resolve the issues in handling large amount of data using traditional data storage and query processing. The author [10] focuses data stream processing, data storage models, complex event processing and searching are described in the paper entitled "When things matter: A data centric view of the Internet of Things".

16.3.1 Data Management Life Cycle

The process of categorizing the data and to use the components for developing the life cycle of data management is referred as Data Management Life Cycle. Data management cycle has identified stages Data Collection, Data Process, Store and Secure, Data usage, Data share, Data Communication, Archive, reuse/repurpose and destroy [11, 12].

Data Collection
In Data Management Life Cycle the first phase is considered to be the Data Collection. Data Collection collect the data to perform operation, planning and to address the issues or objectives. There are several techniques and methods used for data collection. Based on the data collection system design, it meets the requirement of both the internal and external users. Data collection method is determined based on data quantity, period of data collection, funding available, querying and target population.

Data Process
Data processing transforms the data collected into meaningful information. Initially the data collected may not be ready to use as they may contain inconsistent or anomalies. Such data must be cleaned to improve the quality of the data. To address these issues we should determine/define the data quality metrics, techniques for ensuring data quality and strategies/techniques for data processing. Identifying the

erroneous data and its impact is carried out by the quality metrics factors. To ensure safety and traffic data, data quality assurance process should investigate and assess the agencies of transportation. Data processing should be capable of handling complex data sources, quantum of information and use of advanced data processing tools to edit, code, handle missing data, fabricate estimates and projections, analyze and interpret the data. Utilization of Technological advances, increase large amount of data while collecting data from information sensing devices need to have processing capabilities and technical skills to handle the data effectively.

Data Storage and Secure
Enforcing security gives greater confidence in using the data without malicious, fraudulent or erroneous data. This level focuses on storage cost, maintenance and retention policies. Rapid growth in data volume increases greater demand of cost-effective storage technologies. Many users utilize storage services by purchasing access rights from the cloud service providers for computing and storing their data instead of maintaining the storage services by themselves. Though there are security issues exist with the cloud-based computing, cloud service providers should ensure to overcome cyber security attack issues and data availability for cloud server downtime.

Data Usage
Data is often used to plan, design, construct, study, operate and monitor the system in numerous ways. Use of data for different purpose makes data an asset. Moreover use of data, creates challenges namely analytic capability, data availability, enforce security for valid data usage and privacy/proprietary restrictions to access collected data throughout the data management life-cycle from data collection to data destruction. To address the foresaid challenges it is important to determine the demand of information and then prioritize them according to the need.

Share and Communicate
Sharing of data can improve the participants/researchers/agencies in making decision and gives a comprehensive picture to determine their decisions. While sharing, the data gathered from several sources need to ensure and produce more accurate, timely managed, quality and clarity information. Through relevant agreement sharing and release of information need to restrict the availability of the data. Issues need to be addressed during sharing are communication and transparency, coordination with agency, cost and shared data maintenance, interoperability across systems and data access.

Data Archive
Data archiving is the process of identifying and removing inactive data and storing the inactive data in specialized archival systems or data bank or data centre. There are various issues in reviewing data archiving relies on the storage cost, IT infrastructure, cost benefit analysis and data backup need. To implement the requirements of data archiving, the process should encompass staffing for maintenance and report preparation, software for archival processing, storage for keeping archived data and a database for structured data.

Reuse/Repurpose or Destroy
Data management life cycle becomes circular when data is either processed for reuse/repurpose or destroyed. Data reuse, use the same data for the purpose defined earlier whereas data repurpose use the same dataset for the purpose not defined earlier or a new purpose to solve new problem. Data destruction removes the data from the physical storage and makes the data unreadable or irretrievable.

16.3.2 IoT Data Life Cycle Management

The flow of traditional data spans fixed boundaries where as IoT platform moves data across many layers. Data moves from one layer to another establish relationship among alternate stages or combining one or more stages. IoT Data Lifecycle management is almost similar to data management life cycles described earlier. IoT Data Lifecycle management has stages creation, collation, storage, processing, retention, archival purging and cleansing. The aim of the data Lifecycle management strategy is to provide framework that help the organizations to receive the maximum value. The stages creation, collation, storage, cleansing, processing and retention are presented in data life cycle management.

Creation stage helps the business process to create data by the selection of known and trusted device and appropriate end-user utilities. Data created should be ready for further processing, optimizing transformation and cleansing efforts. Collation stage is similar to data collection of Data management life cycle to collect the relevant data and present according to the business need. Mode of data collection is carried out either in batches or near real-time. Real time should be defined to ensure standardized practices. Storage stage is a critical layer that offers security to the data and to accommodate growing data. This stage is also almost similar to data storage layer described earlier. Storage-as-service scenario is applied in this stage acknowledge that the IoT data is best stored across large distributed storage technologies and offer best solutions for storing IoT data for short term and long term strategies.

Cleansing rules are collection specific and they are applied to get relevant information by ensuring data relevance and integrity. Cleansing is one way of purifying the data thus by employing the transformation process should extract the relevant data during processing through retention of critical parameters. Processing adopts the principles of processing data that are collected through various modes and fulfills the requirement characteristics. Assuring the data quality requirement, processing might identify irrelevant information thus by deploying tools and strategies relevant to growing technology. The processing may incorporate parallel processing techniques to ensure optimized performance and cost.

Data can be classified and identified by the organizations as relevant, irrelevant, useful and potentially useful data to ensure optimal use of data. Based on the business need, they system should devise a criteria for data retention, spanning duration, volume, and frequency. Archiving process removes irrelevant/unused data

and place them in a separate location makes the business process to work more effectively with the active data set. Archival mechanism should ensure cost effectiveness and yield ease access of data by categorizing the archival modes as frequency of data access, duration of data access and most important data. Purging is performed on archived data to prevent business risk. Data governance policies ensure purging mechanism and the mode of purging should be clearly articulated.

16.3.3 IoT Data Management Issues, Strategies and Solutions

Organizations facing key issues during the IoT data lifecycle management are lack of standardized enterprise view of data, lack of governance and ownership of data access, Uncontrolled or unauthorized access to data, evolving compliance requirements, lack of standards across data format, exchange and storage mechanism, Restrictive relational database management system capabilities and Lack of standardized nomenclature.

Edge Computing
Ted Friedman says that "many of the same data management infrastructure tools and technologies are applied to more traditional use cases can be leveraged in some fashion to support IoT". In edge computing, the data occurs near the data source or at the computer network edge. The edge computing is also called as fog computing in which, IoT process the data locally requires no storage space, process the data faster than centralized system and meets the challenges in security.

Data Governance
When data need to be secured, defining accessibility rights become mandatory. Granting permission, may permit or having control over managing data to the user to process the information through data governance to ease the security risks. Data Governance becomes mandatory for all the end users of systems. For consumer satisfaction, educating consumers to govern the data individually becomes dominant thus by making data governance as a common household term.

Metadata Management
Data about data is metadata. In IoT data, metadata has significant role that describes the context of the data. Many automated systems offer many solutions for the system thus by defining the context, extract meaningful insights, possible to aggregate, organize, analyze and govern the data quickly. Managing such details is essential to provide solution to operate/function, locate the data, decision making on desired scenarios or situations.

Edge computing, Data Governance and Metadata management have offered significant contribution to provide the data with higher usability, security, scalability and agility. In 2019, Ted Friedman, illustrates that more than one third of the

IoT solutions are cast off before their exploitation due to lack of data management and analytics capabilities adapted to IoT. Moreover, he suggested for IoT to thrive should have modern infrastructures and technologies to support data management and create new policies to improve data management capabilities.

Data Aggregation and Dissemination are the significant landmarks to Data Management in restricted energy of sensor nodes and decentralized nature of IoT environment. Hence in the following sections both the techniques are presented.

16.4 Data Dissemination and Aggregation

Sensor nodes used in IOT environment are having limited capability to process and prone to have low battery power. The lifetime of the sensor network depends on the restricted battery power of the sensor nodes. The data aggregation and dissemination are play vital role to increase the lifetime of the sensor networks by eliminating the redundant information from sensor nodes by data aggregation and forwards the needy information to the base station or destination by data dissemination process. Different data aggregation and dissemination techniques/algorithms are introduced depending upon the structure of the IoT sensor networks. The structure of the sensor network is classified as

- Flat networks
- Hierarchical Networks
  - Cluster Network
  - Chain based network
  - Tree based network
  - Grid based network.

16.4.1 Flat Networks

Each node in the flat networks having the same battery power and also plays the same role in the network. The schematic architecture of flat network is as shown in Fig. 16.2. Ex: Sensors used in Home automation.

In this flat network, the sink sends a query through flooding to the sensor nodes and sensors that having matched data with the query sends reply to the sink/base station.

Due to unwanted communication and excessive computational burdens, the sink node gets faster running down in its batter power. Thus the decaying performance of the sink node affects the whole network functionality. Depending upon the application, there are different protocols have been proposed [13, 14]. In the following subsection, a few protocols are briefly discussed with their merits and demerits.

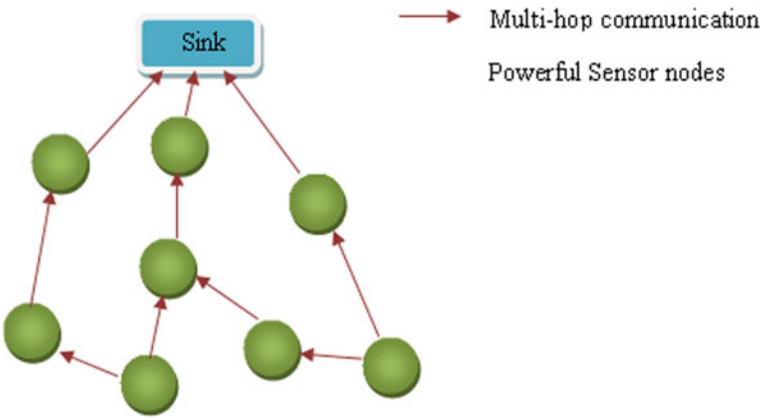


Fig. 16.2 Schematic architecture of flat network

Flooding

In flooding protocol, a source node broadcasts a copy of information to all its nearby nodes as shown in Fig. 16.3. The neighboring nodes forward the copy of information to their neighbors. The destination node receives the copy and it does not broadcast to its neighbors [15]. A round is defined as the time taken by a group of nodes to receive information and forward that information on their neighbors. Flooding is simple but it has problem of energy consumption and sudden failure to operate and collapse in data forwarding.

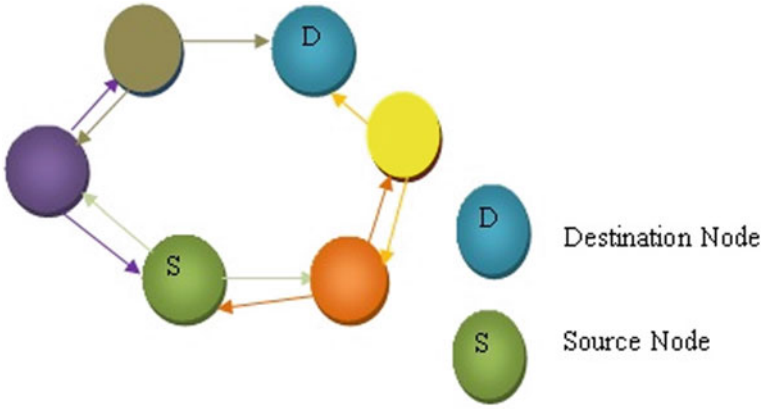


Fig. 16.3 Schematic diagram of flooding protocol

Gossiping

In gossiping protocol, the information forwarded to one selected neighbor and thus it avoids the implosion [16]. It disseminates the information slowly with slow rate of energy dissipation [17, 18].

SPIN (Sensor Protocol for Information via Negotiation)

SPIN is the data centric routing protocol and it is classified under push based diffusion protocol. Figure 16.4 shows the schematic diagram of SPIN protocol.

The resource adaptation and negotiation are the two main features of SPIN. In this protocol the information is using high-level descriptors or metadata. When a sensor node finds new data then that node advertises the new data to its neighboring nodes in the network using metadata.

Those nodes are interested with the new data then interested nodes are sending request to initiating node. Finally the initiating node sends the new data to the interested nodes. Thus metadata negotiation solves the problem of flooding protocol like forwarding the redundant information to all nodes. Also in SPIN protocol, each node verifies its battery resource (power) before it transmits the information. If the node finds its battery power is low then it cannot complete the particular task.

Directed Diffusion

Directed diffusion (DD) is one of the energy efficient protocols. It is a typical scheme of two phase pull diffusion. The DD protocol is the data-centric and application specific protocol. In this protocol, the sink requests the information by broadcasting the interests in the network. The interest describes the required task for which the network is implemented. The geographical area of sink, unique ID, interval and duration are the attribute values used to define the interest. Each receiving node in the network derives the gradient from interest request. The gradient is the reply link with information like data rate, duration and expired time. This process is continued until the source node describes the gradient. So, several paths can be determined between source and sink. The sink resends the interest to the source using reinforcement. Hence reinforcing source send the data to sink more frequently i.e. with low latency.

One-Phase Pull Diffusion

The Directed diffusion protocol is not applicable to the network with many sources and sinks. One-phase pull diffusion eliminates the gradient reply link to the sink as

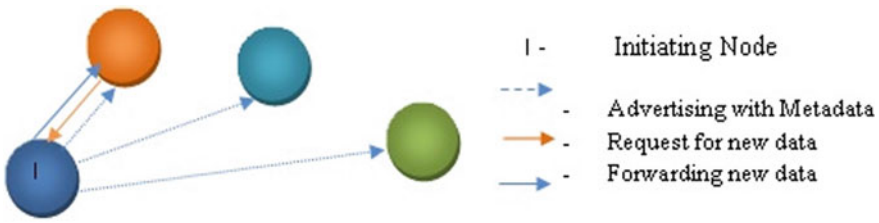


Fig. 16.4 Schematic diagram of SPIN protocol

Table 16.1 Data aggregation and dissemination protocols in flat networks

S. no.	Protocol	Merits	Demerits
1.	Flooding	Simple	Energy consumption and implosion
2.	Gossiping	i. No implosion ii. Low decaying of Energy	More time taken to reach destination
3.	SPIN	i. No implosion ii. Low energy consumption than flooding protocol iii. Energy aware nodes	Inability to guarantee data delivery
4.	Directed diffusion	i. No implosion ii. Low energy consumption than flooding protocol	Applicable only to network with few sinks base stations
5.	One-phase pull diffusion	i. No implosion ii. Low energy consumption than DD iii. Applicable to network with more sources and sinks	Excessive control overhead when a diffusion method is wrongly choosen
6.	Rum or routing	Energy efficiency, no implosion	–
7.	Gradient-based routing	Improves network lifetime	–

in DD. The interest request messages send by sink to establish gradients. But the source does not send the gradient reply link and it only transmits information with low latency. Thus, the one-phase pull diffusion is used to control the network with many sources and sinks. Also the energy conservation of each node is reduced.

In Table 16.1 the list of protocols used for data aggregation and dissemination are listed with their merits and demerits.

Rumor Routing

Rumor routing protocol is described small deviation in DD protocol. It is between query flooding and event flooding. When a sensor node finds a new event then the event is listed in table. The rumor routing utilizes the agent which is long-lived data packet. The agent carries the information about new event and propagates through the network to distant nodes. If any sensor node rise query related to the new event then the node know the route and respond to the query using event table. So, in this protocol, the flooding is avoided which results in improved energy efficiency.

Gradient Based Routing

This gradient based routing is one of the types of DD protocol. The objective of this protocol is to improve the life time of the network by uniformly distribute the traffic. Each node of the network can calculate the number of hops(N) to reach the sink. Here the gradient means the difference between one node's N value and its neighbor node's N value. The information is forwarded in the path of highest gradient.

16.4.2 Hierarchical Networks

The hierarchical network is also called as cluster based network in which the network is divided into number of clusters. During the data aggregation, the data fusion process is performed in each cluster by the cluster head/special node. Unlike hierarchical network, here the energy efficiency is achieved by eliminating the unwanted communication and computational burdens to the sink. The subset of hierarchical network is called as cluster based network in which the network is divided into number of clusters as shown in Fig. 16.5.

Cluster Networks
In cluster networks the sensor nodes are clustered depending upon distance, type of sensors or for which application the sensors are used.

Low Energy Adaptive Clustering Hierarchy (LEACH)
LEACH is a first clustering protocol. This protocol is suitable for the applications of continuous monitoring and data reporting. The LEACH protocol has the following two phases

i. Setup phase
ii. Steady phase.

In setup phase the sensors are arranged as number of clusters and select the cluster head of each cluster themselves. The steady state phase involves the data aggregation in cluster head and transmits the data from cluster head to sinks. The procedure steps to select the cluster head are as follows

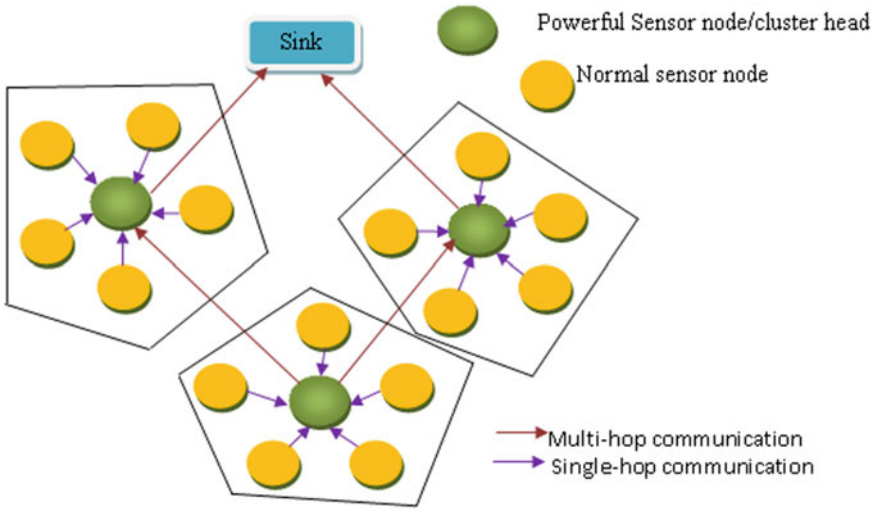


Fig. 16.5 Schematic architecture of hierarchical network

i. Consider 'P' is the predetermined fraction of nodes in the cluster.
ii. Consider 'R' is the random number between 0 and 1.
iii. Calculate the threshold value of the sensor node 'i' using the following equation

$$T_i = \frac{P}{1 - P\left(R \bmod \left(\frac{1}{P}\right)\right)} \tag{16.1}$$

iv. Compare the random number R with the threshold value T_i
If $R > T_i$, then ith sensor is chosen as cluster head.

Depending upon optimum cluster head selection, the LEACH protocol extended as the following approaches with respect to reduce the energy

i. E-LEACH (Energy-LEACH)
ii. TL-LEACH (Two Level-LEACH)
iii. M-LEACH (Multi hop Communication-LEACH)
iv. LEACH-C (LEACH-Centralized)
v. V-LEACH (Vice Cluster Head-LEACH).

Hybrid Energy Efficient Distributed Clustering Approach (HEED)
The main objective of the HEED protocol is to improve the lifetime of the network by establishing proficient clusters [19]. In the HEED protocol, each node (i) in the cluster needs to calculate the probability which is defined as

$$p_{i = C \times \frac{E_{residual}}{E_{max}}} \tag{16.2}$$

where

C is the initial percentage of the cluster head (assigned by user)
$E_{residual}$ is the present residual energy of the node
E_{max} is the energy level at initial stage.

If $p_i = 1$, then the ith node is selected as cluster head. If the probability $p_i < 1$ then the ith node consider as tentative cluster head, then this iteration continuous for all the nodes in the cluster. Now, parameter called the Average Minimum Reachability Power (AMRP) is used to select the cluster head from tentative set of cluster heads. The average minimum power required to reach the cluster head within cluster is called AMRP. The node with minimum value of AMRP is selected as cluster head from tentative cluster head set.

The merits and demerits of data aggregation and dissemination protocols used in clustering network is listed in Table 16.2.

Clustered Diffusion with Dynamic Data Aggregation (CLUDDA)
The CLUDDA is the hybrid approach which combines the process of aggregation and diffusion. It is possible for adaptive data aggregation in new/unfamiliar environment. The query cache is used in cluster head and gateways. The query cache is

Table 16.2 Data aggregation and dissemination protocols in clustering network

S. no.	Protocol	Merits	Discussion
1.	LEACH	Improves data accuracy and lifetime of the network	Assumption on every node in the cluster has enough energy to act as CH and to forward the data. This is not valid for energy constrained sensors
2.	HEED	Improves the network lifetime	Inter cluster communication is not possible
3.	CLUDDA	Dynamic data aggregation and also data aggregation in unfamiliar environment	The memory requirement for the query cache

having the information about the node where the data is aggregated and addresses of the neighboring nodes where the data are originated [20].

Chain Based Networks

In cluster based sensor network, if the cluster head is farthest distance from the sensors then it will increase the energy consumption for communication between them. So, further improvement in energy efficiency can be obtained by chain based data aggregation technique. The sensors transmit the data to close neighbors. Thus the sensors form chain between the source and sink. The architecture of chain based network is as shown in Fig. 16.6.

Figure 16.7 represents the chain based data aggregation using protocol called PEGASIS (Power Efficient data GAthering protocol for Sensor Information Systems) proposed in [21].

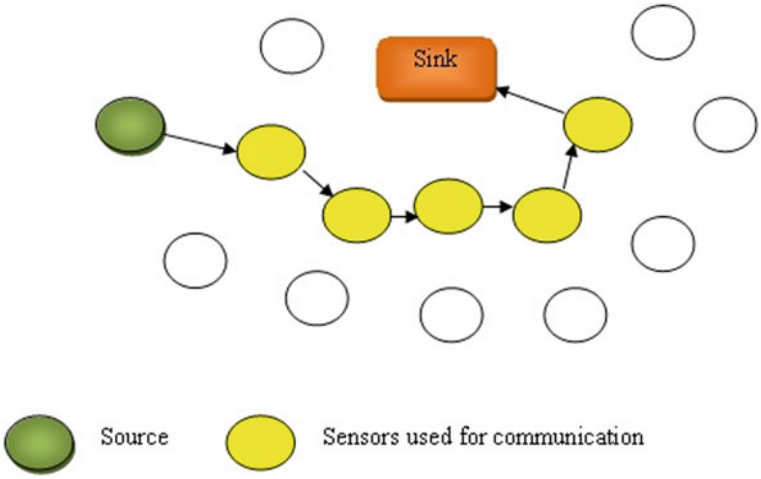


Fig. 16.6 Data aggregation and dissemination in chain based network

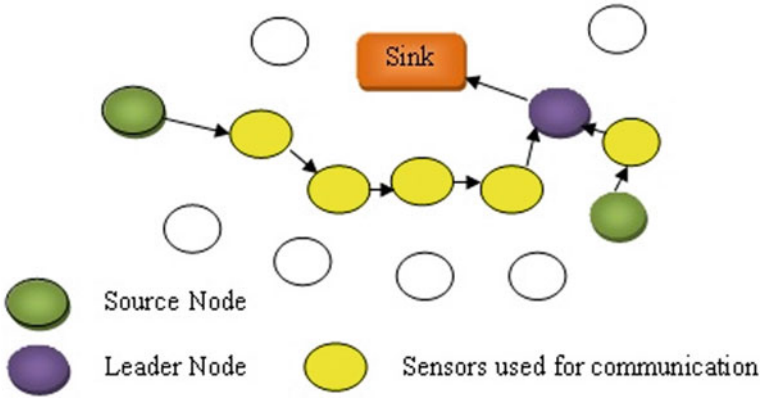


Fig. 16.7 PEGASIS protocol

In PEGASIS, greedy algorithm is used to form chain by determining nearest sensor nodes. In this network, all the sensors have the knowledge about the whole network. During each aggregation round, the information transmitted to closest sensor which receives and fuse the data itself and fused data is retransmitted to next closest sensor until it reach the leader node. The leader node aggregates all the data and transmits to the sink. The schematic diagram of chain based data aggregation using PEGASIS protocol is as shown in Fig. 16.7.

Tree Based Data Aggregation

The sensor nodes are arranged as tree with root nodes and branch nodes. The branch nodes aggregate the data and transmit the useful data to root node. The main objective of this network is to develop an energy efficient data aggregation tree structure. The schematic diagram of tree based data aggregation is as shown in Fig. 16.8. The tree based data aggregation is suitable for in-network data aggregation

Grid-Based Data Aggregation

Grid is a network of lines that cross each other to form a series of square or rectangle region. In grid-based data aggregation technique, a set of sensors are assigned as aggregators in each grid as shown in Fig. 16.9. The aggregator in grid based data aggregation is similar to cluster head in cluster based data aggregation. The cluster head is fixed in the cluster, but the aggregator is dynamic selection which is depending upon the mobility of the network. Hence, this grid-based data aggregation is suitable for mobile environments.

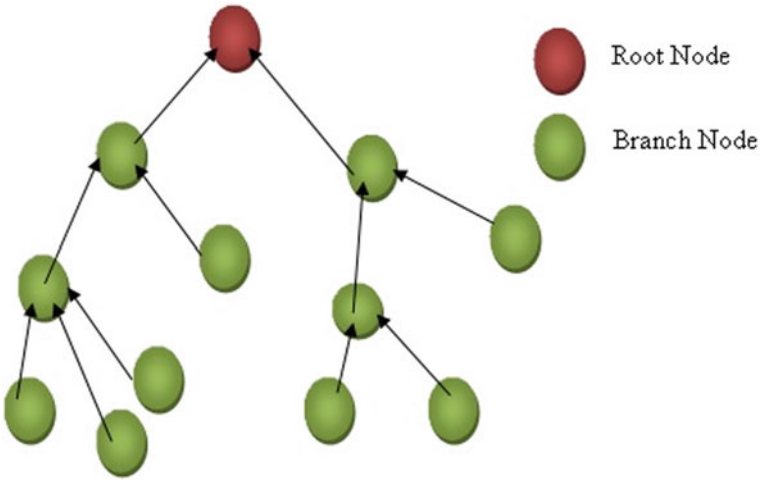


Fig. 16.8 Tree based data aggregation

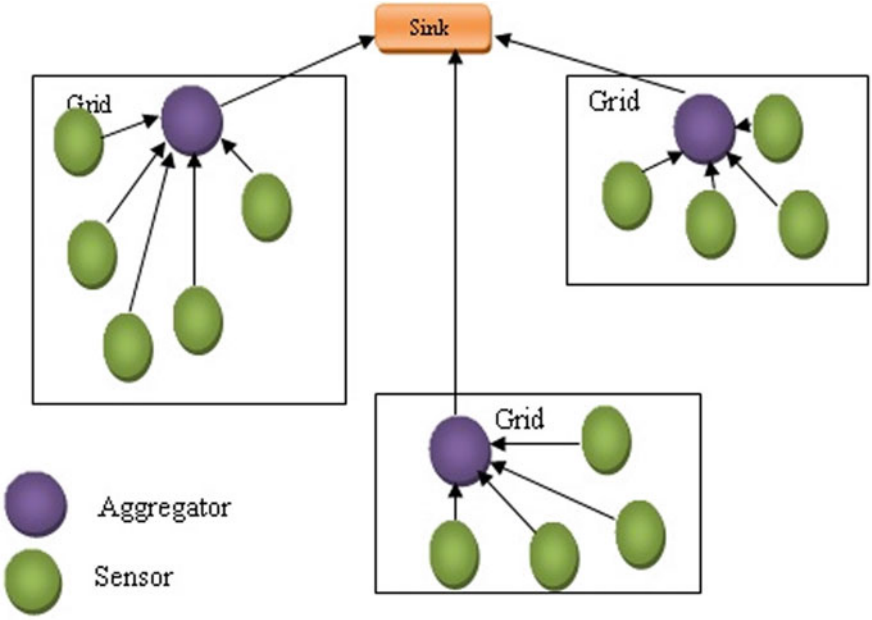


Fig. 16.9 Grid based data aggregation

16.4.3 Performance Measures

There are three typical performance measures used in data aggregation algorithms. The performance measures are data accuracy, latency and Network lifetime. All these performance measures are highly correlated with the application in which IOT used.

Energy Efficiency
Energy efficiency of the IOT sensor network is described by the quantity called network lifetime. The IOT network functionality has to be extended as long as possible. The energy efficient data aggregation method improves the functionality of the network.

Network Lifetime
If the application needs the data from all sensors in the IOT network, then the life time is defined as the number of rounds till the first sensor die. For some applications, it is not necessary to operate all the sensor together. In this kind of network lifetime is defined as the d % of sensors are drained to its energy below operated level. The value 'd' is specified by the network designer during implementation. The network lifetime is improved by data aggregation algorithm. The data aggregation algorithm is used to optimize the energy utilization and it makes the network energy drainage uniformly.

Data Accuracy
Data accuracy differs in its definition based on IoT network designed for particular application. For example, the data accuracy is defined as the estimation of target at the sink (Target localization problem).

Latency
Latency is defined as the time difference between the data received at the sink and the data generated at the source node. The delay exist in data aggregation, routing and data transmission is called Latency. The latency is expressed as

$$\tau = t_D - t_S \tag{16.3}$$

where

$$t_D = receiving\ time\ at\ destination\ node$$
$$t_S = transmitting\ time\ at\ source\ node$$

Merits of Data Aggregation

- It is used to improve the energy efficiency of the sensors.
- It is used to decay the traffic in the IoT sensor network.
- It offers to improve the accuracy of data which is collected from the whole IoT network.
- The redundant data collected from various sensor nodes is reduced by this data aggregation algorithm called sparse data aggregation.

Data Aggregation Procedure has its Own Disadvantages Some are Listed Below

- In cluster based aggregation algorithm, a cluster head from each cluster is used to aggregate data and forward it to the base station/sink. There is the possible to attach the cluster head by suspicious attacker.
- There is no guarantee for data accuracy if the cluster head is compromised with attack.

16.5 Smart Home—Gateway Framework

Smart home is that, controlling of electronic devices and other home appliances using computer or smart phone by remotely. In smart homes data collection and awareness are the main functions. In smart home, smart gateway collects and senses data from the various home appliances and send to the cloud services. Once the data is collected, optimization can be done in cloud services based on the user Quality of Experience [22, 23]. To achieve good user QoS large amount of data is collected. In cloud services controlling methods are carried out based on the status received from the smart gateway and the feedback send back to the smartgateway.

Smart home gateway framework has the following three layers

1. Smart home infrastructure layer
2. Samrt gateway layer
3. Smart home cloud layer.

16.5.1 Infrastructure Layer

Smart home layer consists of electronic devices like TV, Radio and other home appliances. These devices need entrance to the external network as internet through smart gateway. Example: For the following smart with related parameters are used as input data for the smart gateway (Table 16.3).

16.5.2 The Smart Gateway Layer

In smart gateway layer, smart gateway acts as a host for the Home Gateway Unit (HGU) as shown in Fig. 16.10. The main functions of data collection and awareness can be performed by HGU.

Table 16.3 Smart devices with the associated parameters in smart home

Device	Parameter
Television	Channel
	Volume
	Power
Gate and door	Movement
	Distance
FM stereo	Power
	Volume
	Station
Alarm clock	Power
Curtain	Movement
Refrigerator	Power

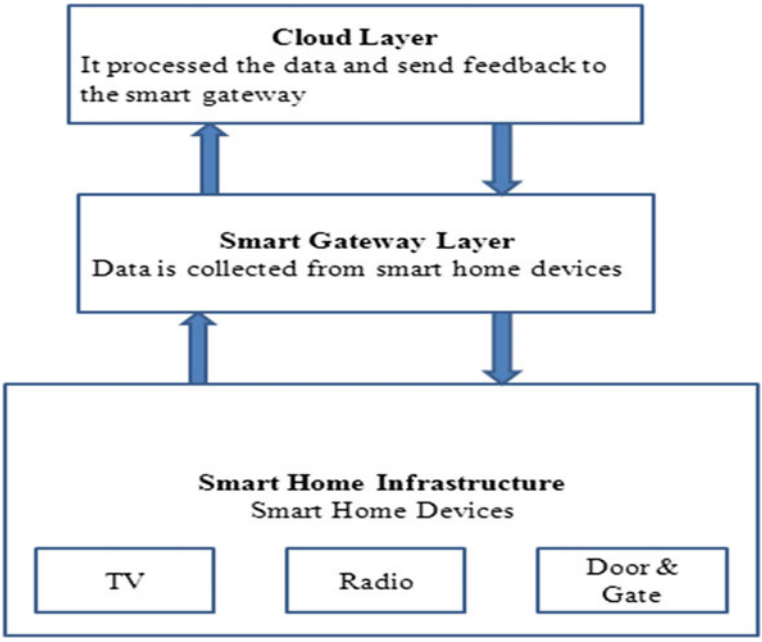


Fig. 16.10 Smart gateway data collection and awareness framework

16.5.3 The Cloud Layer

Cloud Layer is responsible to carry out the following major functions.

1. To store the data from smart gateway cloud is used.
2. To receive the status of each HGU also cloud is used.
3. Once the data is collected, based on the status received from HGU optimization is done at cloud end and feedback send to the smart gateway.

The home appliances can be controlled based on the feedback received from cloud layer. This system improves the efficiency of the building in the way of energy saving, environmental blow and assure security. Various kind of sever has been involved in IoT technologies. Based on our requirement anyone of server can be used for our applications. Some of the servers for IoT platform are Cisco, Google Cloud's, Microsoft Azure IoT Suite, AWS, IBM Watson etc.

16.6 Smart City

Smart city is that, a city that uses information and communication technologies to improve the operational efficiency and increase the quality of services of a city. In earlier days, small installations were done with the IOT applications i.e., smart home. Later large scale installations were worked out with the help of IOT i.e., smart city [24]. In smart city, scalability in IOT infrastructure is the main thing because various sensors being involved from various information sources. The framework structure of smart city is presented in Fig. 16.11.

Comparing with smart home, large amount of data need to be processed in smart city because more number of sensors are installed in several information sources and applications. If different kind of data is received from different sources then we need to convert all the data into a common form. Some of the specific examples for the information sources are

- Street and traffic lights
- Transportation
- Parking
- Infrastructure and maintenance
- Waste management (including waste water)
- Air quality
- Crime
- Architecture
- Energy usage and distribution
- Traffic flow
- Pedestrian and bicycle needs.

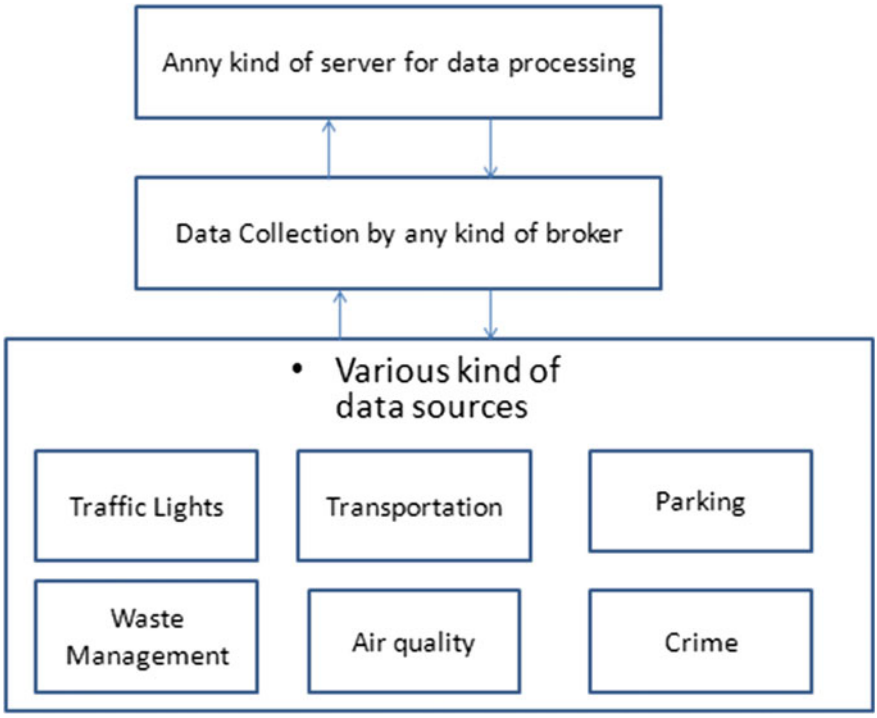


Fig. 16.11 Framework for smart city

Data is collected from information sources by any kind of broker. Then the collected data is sent to cloud server. In market many of cloud servers are available with its own merits and demerits. Based on our needs anyone of server can be selected for our applications. In addition to data storage, some controlling measures are taken in server part. The device can be controlled based on the feedback received from the cloud server.

16.7 Conclusion

This chapter brings out the significance of IoT data management by describing the fundamentals of data management, data aggregation and dissemination. In data management, the data types and the issues in handling the IoT data along with its challenges and characteristics are portrayed. Further discussion on data management life cycle and IoT data management life cycle illustrate its significance. Stating the issues, providing solutions and offering strategies in handling IoT data

management principles are elaborated. Data dissemination on various networks is illustrated clearly. Finally the chapter concludes with an application of IoT Data Management in Smart Home and Smart City.

References

1. Cooper, J., James, A.: Challenges for database management in the Internet of Things. IETE Techn. Rev. **26**, 320–329 (2009)
2. Sabrina, B., Djallel, E.B., Azeddine, B., Homero, T.C.: Big data challenges and data aggregation strategies in wireless sensor networks. IEEE Access Spec. Sect. Real-Time Edge Anal. Big Data Int. Things **6**, 20558–20571 (2018)
3. Tole, A.A.: Big data challenges. Database Syst. J. **4**, 31–40 (2013)
4. Catalin, C., Monica, C.: Large data management in IoT application. In: IEEE Conference, pp. 1–5 (2016)
5. Abu, E.M.: Data management for the Internet of Things: green directions. IEEE, pp. 386–390 (2012)
6. Yuchao, Z., Suparna, D., Wei, W., Klaus, M.: Enabling query of frequently updated data from mobile sensing sources. Inst. Commun., pp. 946–952 (2014)
7. Mervat, A.E., Mohammad, H., Najah, A.A.: Data management for the Internet of Things: design primitives and solution. J. Sens. **13**, 15582–15612 (2013)
8. Efficient storage of multi-sensor object-tracking data: Xingjun, H., Hao, H., Peiquan, J., Lihua. Y. IEEE Trans. Parall. Distrib. Syst. **99**, 1–5 (2001)
9. Lu, T., Fang, J., Cong, L.: A unified storage and query optimization framework for sensor data. In: Web Information System and Application Conference, vol. 13: 229–234 (2015)
10. Qin, Q., Sheng, Q.Z., Falkner, N.J.K., Dustdar, S., Wang, H., Vasilakos, V.A.: When things matter: a data-centric view of the Internet of Things. CoRR **1**, 1–10 (2014)
11. Kristi, M., Matt, M., Maarit, M., Boya, D.: Data management life cycle. PRC **1**, 17–84 (2018)
12. Vinod, V.N., Nanda Kishor, R.: Getting the most out of IoT with an effective data lifecycle management strategy. White paper
13. Heinzelman, W.R., Chandrakasan, A.P., Balakrishnan, H.: An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wireless Commun. **1**, 660–670 (2002)
14. Ramesh, R., Pramod, K.V.: Data aggregation techniques in sensor networks: a survey. SURFACE **1**, 1–30 (2008)
15. Paruchuri, V., Durresi, A., Dash, D.S., Jain, R.: Optimal flooding protocol for routing in ad-hoc networks. In: IEEE Wireless Communications and Networking Conference, pp. 93–102
16. Jelasity, M., Babaoglu, O.: T-Man: Gossip-Based Overlay Topology Management. Engineering Self-Organising Systems, pp. 1–15. Springer (2006)
17. Jelasity, M., Montresor, A., Babaoglu, O.: Gossip-based aggregation in large dynamic networks. ACM Trans. Comput. Syst. **23**, 219–252 (2005)
18. Jelasity, M., Voulgaris, S., Guerraoui, R., Kermarrec, A.-M., Van Steen, M.: Gossip-based peer sampling. ACM Trans. Comput. Syst. (TOCS) **25**, 1–8 (2007)
19. Younis, O., Fahmy, S.: HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans. Mob. Comput. **3**, 366–379 (2004)
20. Chatterjea, S., Havinga, P.: A Dynamic data aggregation scheme for wireless sensor networks. Proc. Progr. Res. Integr. Syst. Circ. **1**, 1–12 (2003)
21. Payal, J., Anu, C.: The comparison between leach protocol and pegasis protocol based on lifetime of wireless sensor networks. Int. J. Comput. Sci. Mob. Comput. **6**, 15–19 (2017)

22. Halvorsen, H.P., Jonsaas, A., Mylvaganam, S., Timmerberg, J., Thiriet, J.C.: Case studies in IoT-smart-home solutions pedagogical perspective with industrial applications and some latest developments. In: The 27th EAEEIE Annual Conference, pp. 1–8 (2017)
23. Ruben, C.H., Rafael, T., Maristela, T.H., Robson, O.A., Luis, J.G.V., Kim, T.H.: Distributed data service for data management in Internet of Things middleware. J. Sens. **17**, 1–25 (2017)
24. Yasir, M., Farhan, A., Ibrar, Y., Asma, A., Muhammad, I., Sghaier, G.: Internet-of-Things based smart cities: recent advances and challenges. IEEE Commun. Mag. **1**, 1–14 (2017)

Chapter 17
Online Social Network Analysis (OSNA) Based Approach for Interconnecting Complex Systems of Internet of Things (SIoT)

Meenu Chopra and Cosmena Mahapatra

Abstract SIoT (Social Internet of Things) is a concept of IoT in which the objects mimic the relationships that human form thus forming their own relationship sets. It is an upcoming area of pragmatic research and ill now much work has been left to simulations only. The concept behind SIoT architecture is to form two different layers, one of IoT objects and the other of people who are going to use it. These objects are ruled by rules made by people; to protect the privacy of the users. Firstly we would in this paper discuss the pragmatic implementation scenario of a SIoT platform. This is done by analyzing the various IoT research work till date and in turn listing out the major characteristics that could be reused for our research. Secondly, we shall discuss in detail how the IoT objects form inter-relationships autonomously. Here we shall take up various concepts of relationship formation such as Parental Object Relationship, Co-Location Objects Relationship, Co-Work Object Relationship, Ownership Objects Relationship and Social Object Relationship. Thirdly, we discuss the interlinking of IoT with the established concept of social networking analysis (SNA), wherein we would be interlinking objects of IoT with the rules built thorough SNA, thus forming a human bound relationship with their objects. And finally, we discuss the new challenges and open issues of SIoT with the architectural elements that will pave the way toward this future-driven SIoT paradigm.

Keywords Online social networks analysis (OSNA) · IoT platforms · Social networks · SIoT · Recommender systems

M. Chopra (✉) · C. Mahapatra (✉)
IT, Vivekananda Institute of Professional Studies, GGSIPU, New Delhi, Delhi, India
e-mail: meenu.mehta.20@gmail.com

C. Mahapatra
e-mail: cosmenamahapatra1@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_17

17.1 Introduction

The scope of "connections" in modern society have enlarged the circle of an internet user to include not only people but things too culminating into the creation of Internet of Things (IoT). Smart objects having distinctive addressing designs make up the IoT set up. These objects are in turn made up of countless elements that interact with each other in diverse ways on the basis of their individual conditions, actions and potential, to deliver various services to the end-users by means of established communication procedures. This interaction will encompass things alongside people to create the IoT scenario that provides objects an equivalent virtual entity. These units will generate and expend services, cooperate to achieve shared objectives and need to be incorporated with other services.

For these objects to communicate effectively there is a requirement to create novel patterns and prototypes. Evidence suggests that much accurate solutions are obtained when many individuals, linked in a social network, are present rather than a single person. Authors in [1] presented how conversations are not just limited to humans but extend to objects also. Similarly, [2] takes into account the existence of objects with people in the social network which result in setting up of Internet of Things. These networks are crucial source of information to research the interrelations and fruition of objects in IoT.

IoT is successfully merging with the model of social network, as depicted in [3], enabling an individual to offer assistance, provided by own smart objects, to other people or things in his/her network. This convergence which is thus called Social IoT or SIoT, was officially promulgated in [4, 5]. It hence has been described as a social network which allows every node to act as an object in order to form independent social relationship with other things in the network, based on the rules laid down by the proprietor. This further proves effective in solving issues of navigating the network as well as finding an information or service through navigating the network of "friend" objects. Latter is significant as it absolves the need to depend on classical internet search tools which lack the ability to size up to upcoming future devices.

Though many practical considerations of IoT have been proposed in research such as [6, 7], SIoT has been restricted to theoretical scrutiny. This paper intends to present a probable application for the SIoT, in which objects are capable of forming independent relations and group creation, and their capability to generate and use various services. Further, few applications are proposed to elucidate the advantages of these platform.

17.2 Background

This section focuses on SIoT Methodology in detail.

17.2.1 Importance of SIoT Characteristics

Atzori et al. [8] has proposed an SIoT model in which the objects imitate the actions of a human to form their own social network in accordance with the defined rules of the owner. Just like humans establish relationships with family, objects construct parental object relations with objects having similar features like belonging to same batch of manufacturing (the production batch acts as a family). Similarly to how humans bond over location or a common place like accommodation and workplace, objects also create co-location and co-work relationships. Another kind of relation, called social object relationship, gets formed when these objects are brought together, either intermittently or regularly, due to relations between the owners. Such instances arise when devices and sensors of friends get related. Last, if multiple devices, like smart phone, tablets and game consoles, are owned by the user, ownership-object relation can get established among them.

17.2.2 IoT Platforms

Study of IoT [9] reveals 10 different forms of platforms having certain common characteristics, namely:

- HTTP protocol is used to send and receive the data. This enables increased interoperability between the platforms.
- There is no direct communication between the servers. Instead objects use an intermediate server.
- The sent data is kept tracked through a "data point" that is associated with every object.
- Data is sent and received through POST and GET.
- Each data point is given a tag.
- Internal search engine is used to find data point through tags.
- Each object is identifiable by its API Key.

Owing to storage and processing of large amount of data, IoT is being implemented for the production of such platforms that serve the purpose of data logging. A well known European platform, Cosm (formerly called Pachube) is capable of storing and processing real-time data that is distributed for free use to manage many of devices on daily basis. A remarkable presentation of Cosm's ability was

demonstrated to the world when it visualized data representing the level of radiation near the nuclear reactor of Japan in year 2011.

Nimbits [10], an which is a web application is capable of providing multifarious functions like mathematical calculations, email alerts and difficult problems on API Wolfram Alpha, besides gathering and dispensing data. Data points can be defined by the user to share it further. Its assimilation with Twitter, Facebook and Google+ helps in number of functions like organization of data points, sharing of sensor diagrams and activating alarms.

Paraimpu [11], a Web of Things platform, permit joining together of sensors, actuators and other internet apps for flowing the data among many objects [12]. Furthermore, incorporating it with Twitter assist the user to acquire and operate data from a network friend.

Another application which is a part of IoBridge [7] and is called "ThingSpeak" [13], shares its characteristics, makes use of HTTP communication to enable users for storage and retrieval of data from objects. Plus, applications having various pairs of A.P.I keys like G.P.S tracking and data logging can be created. Besides performing functions like average, sum, round and time-scale, ThingSpeak integrates data representation in various files form.

Nevertheless, none of these platforms are capable of predicting any "social relationship" between the objects. Also, the objects are incapable of independent communication even if they are combined with the human social networks.

17.2.3 Classification of Web Services

Commonly used, Web Services are development procedure using standard protocol like HTTP [14] for interoperable and distributed apps. Web Services or WSs are classified into categories, namely WS-* and REST (Representational State Transfer). WS-* operates its functions and interfaces through Web Services Description Language (WDSL) file. SOAP encapsulates the communications by HTTP protocol. WS-* is employed in high level projects as interoperability with other applications is not a significant mat ter. Also, it delivers superior outcomes for WSN solutions [15] and applications with sophisticated security needs [16].

When resources are used to represent the objects that are given unique identification by the Uniform Resource Identifiers (URIs), it forms the basis of RESTful architecture. Any of the methods like GET, DELETE, POST and PUT could be used to retrieve, edit, remove or publish object information through the HTTP protocol. Negotiated format like XML or JSON are used to encapsulate the payload of the message. It makes the RESTful architecture light and measurable to completely fit with the current set of rules governing the internet.

In order to be congruent with the current IoT platform and to offer a future realization, this paper has incorporated RESTful approach and used CSV, XML or JSON format to represent the entity in SIoT.

17.3 Platform Implementation

The major functions of SIoT platform needed to run basic applications will be explained through description of its implementation.

17.3.1 Server Architecture

The important components forming the platform are depicted in [17]. The data is transferred across many networks through the network layer. The core layer is formed by the application layer which in turn has three sub layers. IoT applications and middleware functionalities are developed in Application layer. The proposed platform is in infant stages; therefore all functions have not been implemented. Also, the vertical applications are precise.

To store and manage varied data types like humidity, latitude, longitude and temperature, the Base layer is formed. The capacity for objects' memory is total 16 data fields; out of which 12 are of fixed type while other 4 are for future purpose. For instance, we can fix field 1 to track temperature, field 2 for keeping check on voltage data, field 3 for xyz data, field 4 for abc data and so on. The last four fields are kept empty to allow client application developers to decide and fill. Functionalities like Object Profiling, for configuration of object information; ID Management, for allocating a distinct ID for "object identification"; "Owner Control", which gives control to the user to allocate actions to the objects; and Relationship Management for ding and running the relationships of each object are all include in the Component Sub layer.

Functionalities like "Service Discovery" and "Service Composition" (SD & SC), and the Trustworthiness Management (TM), as mentioned in [18] have not been implemented but offered by specific vertical application.

The interfaces and the read/write API keys or other such service APIs are located in the Interface Sub layer (Fig. 17.1).

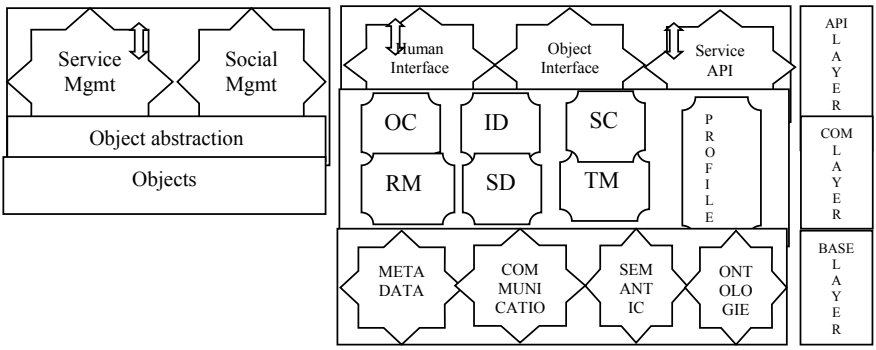


Fig. 17.1 SLOT architecture: server-side (right) and client side (left) [17]

17.3.2 Functionalities of the Server

For the RESTful architecture, an URI is related to each resource. The modeling of resources is as follows:

1. Objects like Smart phone, laptop or sensor is identified as a channel in the server.
2. Depending upon the number of sensors, there could be one or more fields associated with each device. Every field is labeled with a data point.

The profiling module gets activated whenever user wants to register a new channel. It enables the owner to enter the object characteristics like name, description and mobility. Devices having adequate computation abilities like a smart phone or a tablet factory written information saved in them such as brand information and MAC address. This helps in shortening the registration procedure which benefits the owner. Ultimately, during registration of the fixed device like a printer or a desktop, if location of the object is inserted, it would help in establishing relationships based on relationships like co-location.

The owner has the choice of selecting the relationships which an object can form as well as identify its peer objects and field as well as sensors which need to be activated. Upon completion of registration, a unique ID is allotted to the object by the ID management.

Management of social relationships formed by objects is done by RM in two ways, namely:

1. Profiling Relationship, and
2. Dynamic Relationship.

Profiling: These are the relationships that are based on the objects profile and independent of owner behavior. There are further relationships under this category, viz. Ownership Object Relations (OOR), Co-Location Object Relations (CLOR) and Parental Object Relation (POR). OOR is formed between the objects that are registered in the SIoT by the same user. POR is created when the object value is same as that of attribute model. Last, CLOR gets activated when the two objects share a fixed location i.e. have the same numeric ID.

Dynamic: During the interaction of users and objects, if the rules mentioned in are satisfied, dynamic relationship is formed. Under this group, Co-Work Object Relations (CWOR) and Social Object Relations (SOR) exist. The specific requirement in such a case is that server should identify the location of the two objects as same despite being present beyond the visible range (Figs. 17.2 and 17.3).

Whenever new object registration takes place in a SIoT platform or information pertaining to the object like its location or IDs (such as MAC address or RFID id) is shared, the RM module gets activated. In case a device is visible through MAC address or RFID in dynamic relationships, the RM Module gets activated.

For storing of friendship request, the devices are required to be visible in two separate 30-min periods within a gap of at least 8 h. Server manages each pass in the process of friendship request. Devices are expected to send only the sensor data. For

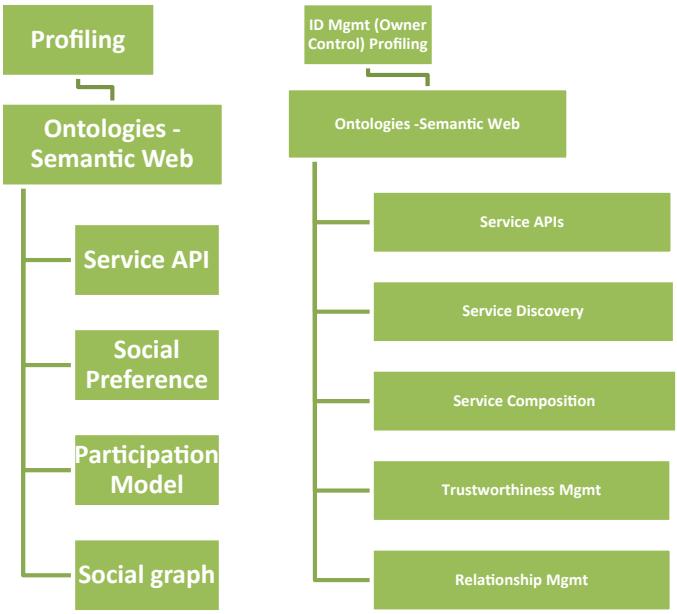


Fig. 17.2 (Left side) depicts basic components of the online social networks for the humans and (Right side) for the objects [17]

illustration, as depicted in Figure Numbered 3, device number 2 is recognized by the device 1 which updates the information at the server regarding the relative position (object), especially the data field storing MAC address. This data is considered as a significant occurrence and registered object is cross checked for its MAC address. In such a scenario, the RM Module verifies the data to ascertain the creation of a new dynamic relationship. Subsequently, device 1 friendship request is stored and a new relation gets created only when device 2 also performs a friendship request.

The write-API key is used whenever there is a need for the object to send or retrieve data, pertaining to it, to the server.

On the other hand, when there is a requirement to fetch data related to friends from the server, the read-API key of the object is used for which the data is retrieved. Though the read-API key is known to the object and its friends, it can be shared in circumstances where data from friend of a friend is needed. There can be two ways in which data from the servers can be acquired:

1. Pull: Each object needs data at regular periods.
2. Push: Available data is sent from the server to objects. For this, every device needs a HTTP daemon that is always listening. Smart devices like smartphones, tablets or laptop, push system of the device's operating system can be utilized.

If an object is registered as public, the only thing that other objects require to retrieve information about it is its ID number. At the same time, if information is

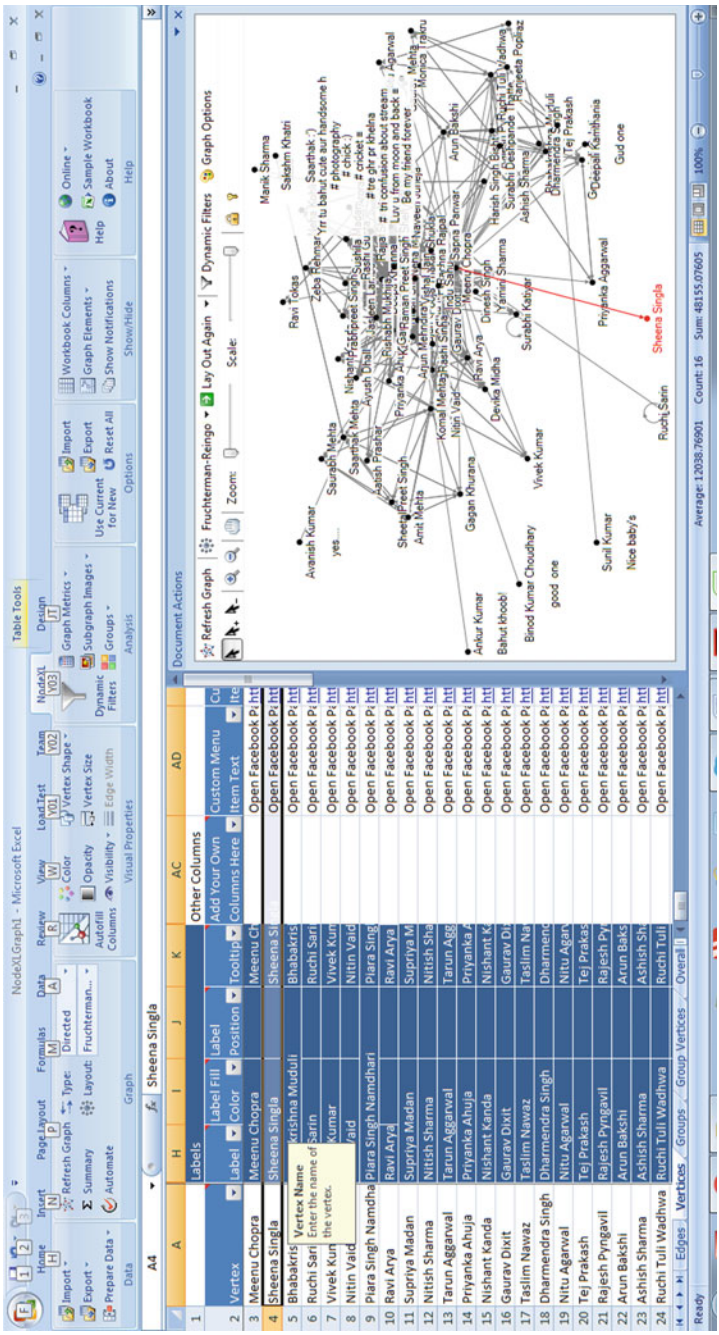


Fig. 17.3 A social networking analysis in Facebook academic higher education networks

needed about a private object, the read-API key of the object is also wanted. Any device can extract the ID list and read-API keys of its friends in any of the format, JSON, XML or CSV, through write-API key by a POST to the REST resource friendships.

On the contrary, in the Push method, the available data is sent straight to all the objects that make up the friendship list. Similarly, as soon as new friendship is created, an updated list is sent to the new object.

17.3.3 Groups Management

The current relationships include many objects which can pose problems related to time taken for service discovery as all objects cannot be useful with regards to a particular request. For instance, in a big corporation, there is a co-work relationship between all the devices such as printers etc. are used by employee of the company. If we group all these devices in accordance to different departments, it would be much useful for management. Hence, it is essential to split these social relationships into groups. Just like humans form various groups based on shared interest (football, politics, fashion etc.), Social Network objects can form own groups depending upon the applications being used. Three kinds of solutions are possible to implement, which are as follows:

The downside is apparent when different devices end up creating different groups because of the application. The groups should be co-incident because in case a file is outdated or obsolete, it will pose a problem.

Client-side groups management. Without much user involvement, an application should be able to form many groups. For this to happen, verification of some conditions, pertaining to a particular use case is needed. The conditions defined for SN is not restricted to just the fields of the device, i.e. its sensors, but will extend to other information too. To illustrate, application can differentiate between devices belonging to the employees of various departments. It will first make sure whether all the devices have a CWOR, followed by verifying the file for employee ID to correlate the groups employee devices. The advantage of this strategy is creation of groups that are fitting to the requirements of the application. The downside is apparent when different devices end up creating different groups because of the application. The groups should be co-incident because in case a file is outdated or obsolete, it will pose a problem. The workload offered to SN devices also see a stark increase when such a solution is put.

Server-side groups management. Under this solution manual creation of groups and setting of their governing rules is done, as per the field related to the device. Devices that meet the established ground rules are connected by the server into a group, in a similar fashion to how dynamic relationships are formed by the RM module. The benefit of this solution is lighter workload of the devices, though excessive disintegration of the groups due to creation of different groups, having different rules, by the users. Also, super users need to be recognized for group creation.

Hybrid solution. Though the server manages the groups, client is the one who define the rules through the fields presented by each device.

A research tool which is network based and identifies the various interlinking structure has become an established methodology to be effectively used in multiple fields of study such as meta-physics [19] to Machine Learning [20] and humanities [21]. Social network analysis (SNA) may be defined in following way:

> Social network analysts (SNA) seek to describe networks of relations as fully as possible, tease out the prominent patterns in such networks, trace the flow of information (and other resources) through them, and discover what effects these relations and networks have on people and organizations. [22]

The interlinking of people and their various objects are a major aspect of study in the "social network analysis". Not only interrelatedness is a crucial part, the effects of this connection is also underlined as a specific property that gets identified through network analysis. The interrelation between the nodes (that can be objects, people, properties of the objects or people) has been defined in the following way:

> To discover how A, who is in touch with B and C, is affected by the relation between B and C demands the use of the [social] network concept. [23]

SNA has long since been used as potent tool to depict the dynamics between various social groups used in context of group dynamics. Specifically, [24] research has inlays group inter relationships through the size of members. It has further studied the patterns exhibited by objects in terms of mobility and their stability in the network. The study concluded that in larger groups membership changes were observed as compared to smaller groups where membership persisted for a larger time period.

The greatest challenge that SIoT field sees, is to handle dynamically changing rules which will affect group membership and their relations (objects to objects and people to objects) with each others. This is because like in any social network relationship groups in SIoT would also have to implement rules on the interactions of objects which will govern the privacy and the rights of people for which they have been formed, yet the rules must be flexible enough to allow the objects to form autonomous relationship among each other so as to provide seamless services.

17.4 Social Network Analysis

A research tool which is network based and identifies the various interlinking structure has become an established methodology to be effectively used in multiple fields of study such as meta-physics [19] to Machine Learning [20] and humanities [21]. Social network analysis (SNA) may be defined in following way:

> Social network analysts (SNA) seek to describe networks of relations as fully as possible, tease out the prominent patterns in such networks, trace the flow of information (and other

> resources) through them, and discover what effects these relations and networks have on people and organizations. [22]

The interlinking of people and their various objects are a major aspect of study in the "social network analysis". Not only interrelatedness is a crucial part, the effects of this connection is also underlined as a specific property that gets identified through network analysis. The interrelation between the nodes (that can be objects, people, properties of the objects or people) has been defined in the following way:

> To discover how A, who is in touch with B and C, is affected by the relation between B and C demands the use of the [social] network concept. [23]

SNA has long since been used as potent tool to depict the dynamics between various social groups used in context of group dynamics. Specifically, [24] research has inlays group inter relationships through the size of members. It has further studied the patterns exhibited by objects in terms of mobility and their stability in the network. The study concluded that in larger groups membership changes were observed as compared to smaller groups where membership persisted for a larger time period.

The greatest challenge that SIoT field sees, is to handle dynamically changing rules which will affect group membership and their relations (objects to objects and people to objects) with each others. This is because like in any social network relationship groups in SIoT would also have to implement rules on the interactions of objects which will govern the privacy and the rights of people for which they have been formed, yet the rules must be flexible enough to allow the objects to form autonomous relationship among each other so as to provide seamless services.

17.5 Parameters of Social Network Analysis

There are various parameters which may be utilized to measure the various underlying properties of SNA for SIoT [22].

Specifically:

– Unit of Analysis

Unit of analysis depicts the relationship between objects of SIoT as they mimic the SNA. Thus this linear structure of objects enables the network to build attributes of objects which reflect the inter-relationship exchanges between the SIoT objects. By building the a network where the interactions have been defined in a top down approach, the network is able to predict correctly the crucial connections in the network objects.

– Relations

Three parameters namely, content, direction and strength, define relations. Among these, the resources exchanged forms the content. As in the case of IoT in SIoT too,

the relations of objects have different edge properties. These properties make the edges directional (Bi-directional or Uni-directional) they may also exhibit non directional properties.

– Ties

Ties depict the type of relations objects have with each other. In context of SIoT, the ties reflect the intensity and types of exchanges between objects.

– Multiplexity

Multiplexity is concept where objects form multiple ties between objects of various types objects which are interconnected with each other.

– Composition

Composition is a very important property of the SNA network and hence can automatically be implemented in SIoT. Composition allows objects of different types to coexist with each other. Composition is based on properties or attributes of the nodes; there can be multiple types of composition of objects.

By different composition we mean that the objects may be a part of ego network where the authority lies with a centrally acting object and all other objects are interrelated through it, or the composition may be that of a whole network where all the objects in the network are interlinked with each other.

17.6 Applications of Social Applications

In SIoT we can make use of Social Network ontologies which are bipartite in nature be converted to tripartite ontologies, the above move would help in linking objects in SIoT with greater autonomy [25] by making use of folksonomy semantics which gets generated through the analysis of tripartite graph.

Since the Objects in SIoT would communicate with each other in the same way as humans would, it becomes imperative that the communication and relation formation forms it basis from SNA applications such as recommender systems. The SNA data may further be used to discover patterns which emerge from investigation of flow of information as well as thrust factor computed from online exchange systems [26].

We may make use of a study which has proposed the use of multiple networks such as using data mining to mine text information through emails, web or even one to one sensor communications in order to generate a rich and powerful information data set of object behaviors viz a viz their behavioral of people making use of them [27, 28].

By studying the various applications it is easily deducible that a social network only for IoT objects may form the basis for a revolutionary change is coming years [29].

17.7 SIoT

This section addresses the three questions that concern the fundamentals of SIoT and how it contributes to the latest know-how. The questions are examined in detail to find appropriate answers to them.

17.7.1 Why Are the SN Principles Being Incorporated with Real Ubiquitous Computing?

A group of communicating entities [30, 31] is referred to as Community of Interest, COI, that can also include communicating entities involved in wanted communication, called "good COI" [32]. A number of resources are shared among individuals in these COI. This sharing could be both online and offline, pertaining to social relationships, interests and multimedia or contextual resources. Beside these, physical devices and objects like appliances used in offices and home could also be shared. Just as social relationships and contextual information are fruitful for enhancing collaboration for shared advantages, [33] the principle of SIoT extend this to include the real world's contextual data and physical entities, with the social capital. This helps in arriving at a better representation of the users' requirements and goals.

In Ubiquitous Computing, varied interacting models of physical devices (called as things) [34] and humans, i.e. between humans and humans or humans and things or things and things, can be identified. The things collect and manage data coming from many sources in order to direct both the physical processes and the exchanges with the users. Through the communicating models, many services and applications directed at individuals and social communities are supported. The services based on the information generated from many thing to thing interactions are exploited by the users based on some trust. This assumes a fundamental significance in Ubiquitous Computing environment. As a result, the next wave of SIoT encompasses the close exchange between humans and things. This results in offering of optimized best services, with improved QoE, to the users. Developed on the foundation of trust, there is a shift in social relationships from thing-to-thing to human-to-thing. This denotes the changing scenario of users who are not only expending the services but contributing in creation of these too. This change has brought up fresh conundrums with respect to context, communications and advantages. This chapter is concerned with following advantages—improvement in QoE and the cooperation between humans and things within the communities. Increased sharing and storing of social information and contextual data in social communities have made the individuals making these communities dynamic. There is cooperation for common goals like publishing of data and content for day to day needs. In SIoT, the fundamental provider of generation and consumption of services are users and devices. The cycle starts from the individuals and their communities by pulling together all the

social data. This information is communicated with the physical devices next. This creates a collection of services that can be utilized by the individuals and the communities for better cooperation than before. The model of Ubiquitous Computing [35] is designed to provide the computational power to all the members of the society for their advantage [36]. However, the intent may become fruitless if adequate understanding of the society's needs is not done. Integrating the social relationships of online SN with the contextual information of online SNs.

17.7.2 SIoT as the Next Step

Upcoming prospects of Ubiquitous Computing offer a variety of smart services and applications that will assist people and organizations to deal with numerous hindrances that crop up during interaction. It will result in seamless connections among all at any given place and time. The novelty of IoT [30, 37] lies in establishing communication with the physical world through the devices by sensing or actuating. On the other hand, SIoT model extends this to the arena where questions are asked about the reason and method of using these services and applications.

To achieve the objective, as shown in Fig. 17.1, either there could be an increase in connectivity (socialization) or improvement in pervasiveness (availability).

In order to settle on all the properties of real ubiquitous computing in our future daily life with high QoE, we need to improve the connectivity of all the relationships between humans and things. As described earlier, each person in society performs the role of a consumer and a producer both, during the process of communication with the others. Further, information could be either provided on proactive or reactive basis by the SNs in both online and physical world. The individuals collaborate to exchange information on requirements, interests, geographic or demographic characteristics, relationship traits etc. QoE can be improved through manipulation of these features, either by storing, processing or utilizing.

In an all-encompassing environment, any device can help the users to access the services whenever and wherever they want through their chosen network of communication. Through the purview of SIoT, there is a merging of all the physical, real and virtual things into the model.

Through their common interests and needs, whenever the users engage in daily interaction in SIoT, they unintentionally assist in making positive changes in QoE. Furthermore, to suit the goals driven from humans there would be association between things of diverse nature. Hence, humans and things would cease to exist independently inside the network and rather have their goals interconnected in order to form the model of SIoT. This leads to close association between humans and things for their increased accessibility and lucidity. As a result, there is a highly pervasive environment which is the core foundation of forthcoming ubiquitous computing systems.

17.7.3 The Important Outlook of Future-Driven SIoT

For the achievement of the proper execution of a faultless assimilation of the social and IoT worlds and to derive the advantages offered by the SIoT visualization as described above, certain viewpoints have to be regarded. Figure 17.1 demonstrates the outlook and historical evolution of ubiquitous computing system.

1. Interactivity Perspective: There can be two types of pairing between humans and things in IoT, namely, human to human, and thing to thing. These pairings can be attained either through the usual way of physical interaction among humans or through many computer networks, in regards to things. In existing state of affairs, almost all the input is centered on a distinct form of communication for a particular time; whereas this chapter is dedicated to implementing human to thing interactions for realizing the holistic vision of SIoT. This methodology paves way to higher level of pervasiveness in IoT and offer hope to solve numerous issues pertaining to networking and communication [38–42].
2. Collaboration Perspective: This viewpoint is focused on complete integration of social and IoT worlds and is therefore significant as it encourages collaboration between humans and things. The roles played by humans and things are surveyed. Keeping social values in consideration, humans and things are allowed to either act as a producer or a consumer in order to increase the association among all the members and also positively enhancing the QoE [43–48].
3. Handled-Data Perspective: The data acquisition and its handling need consideration in all-encompassing environment. Data acquisition can be classified into two classes—Proactive and Reactive. Crawling techniques, algorithms related to learning or data analysis come under Proactive while acquisition of data in a real-time manner through data mining and query techniques falls under the ambit of Reactive. Either of the method can be used for data acquisition in SIoT [49–53].

For example, we can gather information on user location either through an on-demand query which will give the current location or through learning and analyzing which will find the historical trajectory. In addition, this characteristic could contribute in monitoring of temperature by things.

17.8 Current Trends: IoT Is Becoming Social

The concept of amalgamating social aspects with the IoT to form SIoT is fairly novel and under the early stages of study. Nevertheless, some explorations in this field has shown promising results in connecting people via SNs and distributed sensors or embedded devices, in order to improve services and applications. Study [54] proposed the IoT framework enriched with communication characteristics of Twitter to allow information sharing related to current undertakings. On a similar note [55], WSN based approach was mixed with Twitter approach in order to share

sensory data and resources. On the other hand, IoT structure can be recognized as a social organization support to merge ubiquitous IoT framework [56]. Beside this, there are other methods presented in research that broadens the IoT via SNs application programming interfaces (APIs). For example, a platform to allow individuals share their WWW-enabled devices for others' benefit has also been proposed [57].

17.8.1 SIoT Paradigm

SIoT framework can be understood as an interactive environment characterized by exchange of information between people and smart devices. Above this structure, many application and services can be included depending on Web technologies. However, certain basic components are necessary to constitute the foundation of SIoT, namely, social role, intelligence, socialized devices and everything as a service.

(1) Social Role: As presented in [5, 58, 59], through users' SN, the social role arises which is brought into the IoT world for assured navigation in network as well as effective service discovery. Likewise, as shown in [60], trendy online SNs and their APIs endorse social role in order to sustain a social framework and associations with smart objects. Further, the trust instituted by the community forms the basis of sharing smart objects within the given framework. On another note, many service operations like geolocation of data or publishing the status or update of devices can be achieved through SN accounts of users [61]. The social role has been demonstrated in [62] by using the SNs as a medium to direct smart objects.

(2) Intelligence: It is an integral part of SIoT paradigm as important functions like starting, updating and terminating the relationships of the objects cannot be done without it [58]. Not limited to this, [60] demonstrated how this concept can be exploited for dynamic thing to thing service discovery where there is an understanding between smart objects regarding their services in an automated manner. Further, as [63] shows, intelligence can be executed as a middleware comprising of many technologies like ontologies, techniques used in processing user-generated content and recommendation techniques. To summarize, evidence has presented intelligence as a critical decision maker for using the services.

(3) Socialized Objects: The objects in SIoT have been concepted to act like socialized devices [5, 58–60] and are a part of a very complex domain where they would have to formulate relationships among each other over the internet within the rules defined by people who shall be their end users [64]. Supports the use of SNA in creation of smart object networks and is further supported by the study in which the social objects make use of protocols of the web to communicate with their counterparts.

(4) Everything as a Service: The concept of SN and IoT stitched together has captured the research minds of SIoT experts, Objects together with their relationships integrated together have given rise to the idea of offering Smart objects as a service to the end users. These services can be integrated with other services being offered on the web. Thus, the these smart services are being offered under the tag of everything as a service.

17.8.2 Architecture and General Trends

In order to sum up the visualization of our future-driven SIoT, following parts of the architecture are taken into consideration: (a) Actor (Smart things & Users); (b) an intelligent system for managing different interactions among actors; (c) a media or interface to allow actors interact; and (d) availability of Internet for open access among the entities. Each of the components is described in detail [65].

(a) Actors—SIoT framework imply a collaborative environment that favor equal participation of both humans and things in their activities of data publishing and receiving of directive commands to manage the produced data. The data can be used for profiling or as simple answers to users'/devices' queries. The queries could be related to searching the nearest node, the most dependable node or service or for getting updates regarding weather or a particular device. In response, humans and things get the services or the suggestions for services to use in order to satisfy present circumstances and strategic purpose like an efficient power design to be used in a smart grid for a smart home.
(b) Intelligent system—All the interactions by actors are managed and coordinated by it. The major sub systems like service and applications management, recommendation, service discovery and search, and data and context management are taken together as a part of intelligent system.
(c) Interface—It makes possible every interaction within the system through it and facilitates entry of information and queries. It is also required for generating output when control commands or services are used.
(d) Internet—In order to make the smart devices and their services available to the users and smooth interaction with other devices and services, a communication media is needed which is fulfilled by internet.

17.8.3 Enabling Technologies

A certain level of technological advancement is required to construct a functional platform for successful implementation of prerequisites and achievement of SIoT. For creating an entity like a user and device in the network that are exclusive and

recoverable, a distinct identifier is mapped to every component. Besides the public profile that end users will make use of, there is a need for an addressing strategy in the system to allow different management tasks like identity allotment and verification for ensuring recognition of diverse individual identities.

For the development of hardware, current scenario offers many devices which can be accommodated to be a part of SIoT. Some of the good devices can be found among sensor and actuator devices from WSN, M2M, domotic etc. that easily form a part of the new framework.

Still, there is no direct connectivity of internet with these devices and hence a gateway is required to transmit their data and receive commands. SIoT offers features that are accessible through web services, hence using web-enabled devices have the potential to deploy and make full use of this structure. Furthermore, it is imperative to address certain issues in deployment of new hardware, like energy efficiency, adjustable and re-designable interfaces, and ability to follow multiple protocols.

Another matter that needs attention from the start is the manner in which this diverse and large network of users and devices will interact. Any growth channelized towards improvement of operations among the users and devices form a significant support system of the SIoT design. Then again, the focus should be on efficient use of energy through resourceful cooperation between operating system, communication protocols and algorithms that will determine the energy savings during foundation of SIoT. For the growth of this technology, it will be more favorable to employ lightweight and open middleware platforms along with self-adjustable software.

After that, there is analysis of few but significant research and development issues that will aid in advancing this technology and help in the futuristic deployment on enormous level as well as daily implementation of the SIoT network.

17.8.4 Open Research Issues

For realizing the framework of SIoT, many issues have to be dealt with before implementing the technology on a global scale.

Interoperability, Data Management and Signal Processing: IoT devices demonstrate heterogeneous characters like varying information processing and intercommunication abilities, along with user characteristics and data, associations and competency arising from the SNs. This makes imperative for the system to manage different data types thereby providing interoperability within the components. To assist communication and collaboration, general principles of practice and criterion are required [56]. This issue is brought into line with the identification requirement as discussed earlier, as it is necessary to identify every component of SIoT system before initiating interoperability among them.

After achieving interoperability in the network, there is another challenge of data management i.e. the way to manage data arising from devices and users. In fact, the problem can be summed up in two categories—storing of data and management of data. The issue concerning storage is that it becomes impractical to gather all SIoT data in an exclusive server, making it imperative to put forward distributed approaches to create an effective storage system. In respect of data management, metadata structures as recommended by Metadata Standards3 can be the foundation for defining data structures. Next, other proposed standards of W3C4 like Resource Description Framework (RDF), DARPA Agent Markup Language (DAML), or Ontology Working Language (OWL) will come to aid in giving meaning to the data obtained from users and devices.

Then there is advanced data analysis like the ones proposed for Big Data [57] and intelligent approaches that can be used for providing usefulness to the SIoT thereby imparting significant and costly data to users and devices.

(1) Discovery and Search Engines: Keeping in mind the large amount of data concerning SIoT, it is important to keep the applications, services and accessible data within reach. Also, while working with huge data size, it is obligatory to use searching and discovery method. Many of the current approaches for discovery used in web services like UDDI, DPWS (device profile for web services) or RESTful-based [5, 58] can be accustomed to manage the many SIoT needs linked to data, services and applications lookup, and discovery.
(2) Energy management: There is typically a lot of movement in devices that form SIoT without having access to unrestricted power supply. Likewise, users also bear battery operated hand-held devices. Hence, conserving energy is a prime issue in the structure and function of SIoT and there should be an effort to efficiently manage energy at various levels, from M2M device communications to interface design. Energy optimization has to be considered at every stage in devising SIoT technology. Although the techniques employed for harvesting energy have not yet been very successful in providing enough reserve, many approaches suggested for WSNs and low power tools can be adjusted to meet some of the requirements like scalability, availability and heterogeneity of the SIT model.
(3) Security, Privacy and Trust: It is perhaps the most sensitive prerequisite in making SIoT a success. Any SIoT platform lacking the necessary features of user privacy, secured communication and reliable connection will not be considered as a well-founded technology and thus will lose public acceptance. Techniques that promise security of data and user privacy in other frameworks can be used again for the SIoT support, keeping in mind the exclusive needs of this framework. Characteristics that will generate trust among the users for the SIoT environment are efficient systems for data secrecy and veracity, along with effectual ID management and discretion.
(4) Self-Operation, Management and Organization: SIoT, as mentioned before, is assumed to be a global technology made up of myriad devices and users.

While figuring the kind of large-scale management this vast platform would require, it becomes clear that mechanized operations that are pre-set would be required at most levels.

Characteristics like self-organization, self-management, self-operation, self-healing and self-protection are critical components of SIoT. It is not just the automated network management which assumes significance but autonomic data analysis, and service discovery and composition also supplement in improving the experience of the user. Yet again, the approaches used in other technologies can be adjusted to initiate automation of SIoT network operations.

(5) Heterogeneity: SIoT will comprise of sensors, actuators, ID-tags, smart phones, tablets, computers etc. All the brands and technologies irrespective of their differences would need to work towards a shared goal of providing users with sophisticated services and applications. To achieve this, there is a need to merge different types of devices, technologies and services [5]. Different technologies communicate among themselves for ensuring interoperability at the devices' level. Applications could become diverse owing to features like bandwidth, latency, reliability, availability etc. and therefore needs an open system for support.

The need to include heterogeneous devices may impact the system performance negatively on the whole, in relation to an extremely optimized vertical design. However, the comprehensive functionality presented by the SIoT environment has the capacity to offset this limitation. Innovative models handling heterogeneous technologies resourcefully will prove advantageous in deployment of SIoT.

(6) Interactions and Interfaces: The SIoT network will be directed towards satisfying users with a superior experience of consuming and producing both data and services appearing from other users and devices.

Nevertheless, the way users and devices act together is still a wide opened task to be handled. A few probable interactions between the different elements were proposed in [25, 59], however, a majority of them centre on particular applications only. A universal set of communication has to be delineated along with techniques to handle these interactions. For instance, users can extract data from their self-owned devices but the process of extraction from other users' devices is not comprehensible. The issues of privacy come into focus like free access to personal device and sensitive information about current location. Issues about sharing anonymous data also come into focus.

(7) Service Management (Discovery and Composition): Current scenario offers many approaches for determining and executing service composition in the IoT framework [5]. There is a need to introduce new capabilities in the SIoT which can be fulfilled through intelligent approaches providing superior functionality. Semantic-compliant approaches, capable of managing context

and data meaning, can be merged with SOA (service-oriented architecture)-based systems and DPWS [60] are fruitful for implementing service management in the SIoT.

(8) Application Development: The functionalities offered by SIoT will become pointless if there are no applications utilizing them. The process of application development varies in accordance to the circumstances; like concerned devices and services. Another important determinant in the process is the set of users being targeted. Using open APIs is supportive and through users, there will be new cases which will assist in creating an SIoT that is within reach and practical.

(9) New Business Models & Stakeholders: During SIoT foundation, the influential point is how to derive advantages from the technology. During the designing process of a beneficial platform, involving a comfortable relation between both stakeholders and users to create a collaborative framework, certain considerations are kept into focus. First, striking and valuable services and applications should be offered to arouse public interest. Second, to enhance cooperation, such business models should be selected that are non-conflicting. Third, encourage customer participation for enhanced experience, and finally, appropriate number of customers should be targeted.
Once the customers are convinced of benefits the SIoT applications would bring to them, other strategies like sales and marketing, R and D, advertising, application fees, profit-making schemes etc. can be embarked upon [61].

(10) Fault Tolerance: It is necessary that the components that form the heterogeneous SIoT structure should be reliable in their functions, especially in today's ever-changing and transforming environment [56]. Resourceful adjustment to difficult circumstances will help in forming a reliable platform. Also, an accurate architectural organization that can support duplication at multiple levels will assist in giving dependable data to the end users.
Semantics and Context Management: The goal of SIoT is to offer utility in different scenarios, for which many devices can be utilized for varying reasons at one particular time. Therefore, the capacity to accurately handle the current context will aid in enhanced system performance that is more usable through provision of definite access and data interpretation. Interoperability between the components can be made easy through inclusion of SIoT users' description and features of devices. This can be done by semantic approaches oriented to RDF and OWL [62].

17.8.5 Discussion—Challenges and Issues

Literature has substantiated many a times how SIoT is the forthcoming stride in the evolutionary stages of ubiquitous computing. Nevertheless, there are many questions and issues that warrant research community's attention to establish this

technology on a mature scale. This section focuses on chief areas of research that will be contributory in creation of SIoT technology [65–71].

To begin with, an SIoT structure having general features is described, based on an integrating model of many architectural elements mentioned in the literature. There after, the technological development is reviewed regarding both software and hardware components that make the functioning of the framework a success. Lastly, the non-functional requisites forming the fundamental component of the SIoT ecosystem is discussed [72–76].

17.9 Conclusion

SIoT is a field which encompasses Social Networks and Internet of Things together into a platform that gives rise to the concept of Smart Objects and services offered by them. In our study we have extensively studied the various parameters of social network which can be fused together in a syntactical way to form smart object grid where the objects form a autonomous relationship with each other which reflects the interaction of human being on any social networking site. The complexity of the suggested method involves framing rules for objects of IoT in such a way that they retain their autonomous identity yet they are governed by the rules framed by their users for security and privacy.

Various applications of SIoT such as smart home, assisted living, smart city, smart parking, SIoT enabled smart health applications etc. require the use of SIoT platform which is user centric as well as cost effective in execution. It is also required that the SIoT platform makes available the IoT data which is generated by other devices so that they can be used in an non vertical manner by other IoT devices interlinked with each other through recommender systems. The recommender system will help in building profiles of users which will help a new IoT device to make use of it for providing better services. In the end it is concluded that the SIoT platforms powered by social networking syntax and semantics will ensure a better world for its end users.

References

1. Mendes, P.: Social-driven internet of connected objects. In: Proceedings of the International Conference, Smart Objects with the Internet Workshop (2011)
2. Ding, L., Shi, P., Liu, B.: The clustering of internet, Internet of Things and social network. In: Proceedings of the 3rd International Symposium on Knowledge Acquisition and Modeling (2010)
3. Guinard, D., Fischer, M., Trifa, V.: In: PERCOM workshops, pp. 702–707 (2010)
4. Kosmatos, E., Tselikas, N.D., Boucouvalas, A.C.: Integrating RFIDs and smart objects into a unified Internet of Things architecture. Adv. Int. Things **1**(1), 5–12 (2011)

5. Atzori, L., Iera, A., Morabito, G.: SIoT: giving a social structure to the Internet of Things. IEEE Commun. Lett. **15**(11), 1193–1195 (2011)
6. Cosm. [Online]. Available: http://cosm.com (2013)
7. Iobridge: [Online]. Available: http://www.iobridge.com (2013)
8. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The Social Internet of Things (SIoT)–when social networks meet the Internet of Things: concept, architecture and network characterization. Comput. Netw. (2012)
9. Postscapes: [Online]. Available: http://www.postscapes.com (2013)
10. Nimbits: [Online]. Available: http://www.nimbits.com (2013)
11. Paraimpu: [Online]. Available: http://www.paraimpu.com (2013)
12. Piras, A., Carboni, D., Pintus, A.: A platform to collect, manage and share heterogeneous sensor data. In: Ninth International Conference on Networked Sensing Systems (INSS), pp. 1–2 (2012)
13. Thingspeak: [Online]. Available: http://www.thingspeak.com (2013)
14. Castellani, A., Bui, N., Casari, P., Rossi, M., Shelby, Z., Zorzi, M.: Architecture and protocols for the Internet of Things: a case study. In: 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 678–683 (2010)
15. Guinard, D., Ion, I., Mayer, S.: In search of an Internet of Things service architecture: rest or WS-*? a developers perspective. In: Mobile and Ubiquitous Systems: Computing, Networking, and Services, pp. 326–337 (2012)
16. Priyantha, N.B., Kansal, A., Goraczko, M., Zhao, F.: Tiny web services: design and implementation of interoperable and evolvable sensor networks. In: Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems, pp. 253–266. ACM, New York, USA [Online]. Available: http://doi.acm.org/10.1145/1460412.1460438 (2008)
17. Chopra, M., Mahapatra, C.: Amalgam of online social networks and Internet of Things. J. Adv. Res. Dyn. Control Syst. (Scopus) (2018)
18. Nitti, M., Girau, R., Atzori, L., Iera, A., Morabito, G.: A subjective model for trustworthiness evaluation in the Social Internet of Things. In: Personal Indoor and Mobile Radio Communications (PIMRC), IEEE 23rd International Symposium, pp. 18–23 (2012)
19. Barabási, A.-L., Réka, A.: Emergence of scaling in random networks. Science **286**, 509–512 (1999)
20. Adamic, L., Adar, E.: Friends and neighbors on the web. Soc. Netw. **25**(3), 211–230 (2003)
21. Monge, P.R., Contractor, N.S.: Theories of Communication Networks. Oxford University Press (2003)
22. Garton, L., Haythornthwaite, C., Wellman, B.: Studying online social networks. J. Comput. Med. Commun. **3**(0) (1997)
23. Barnes, J.A.: Social Networks. Addison-Wesley, Reading, MA (1972)
24. Palla, G., Barabasi, A.-L., Vicsek, T.: Nature **446**, 664 (2007)
25. Mika, P.: Ontologies are us: a unified model of social networks and semantics. In: The Semantic Web. ISWC, Lecture Notes in Computer Science, vol. 3729, pp. 522–536 (2005)
26. Staab, S., Domingos, P., Mike, P., Golbeck, J., Ding, Li, Finin, T., Joshi, A., Nowak, A., Wallacher, R.R.: Social network applied. IEEE Intell. Syst. **20**(1), 80–93 (2005)
27. Matsuo, Y., Hamasaki, M., Takeda, H., Mori, J., Bollegala, D., Nakamura, Y., Nishimura, T., Hasida, K., Ishizuka, M.: Spinning multiple social networks for semantic web. In: Proceedings of the AAAI-06 (2006)
28. Mori, J., Tsujishita, T., Matsuo, Y., Ishizuka, M.: Extracting Relations in Social Networks from the Web Using Similarity Between Collective Contexts. The Semantic Web—ISWC (2006)
29. Toral, S., Bessis, N., Martinez-Torres, R., Franc, F., Barrero, F., Xhafa, F.: An exploratory social network analysis of academic research networks. In: Third IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS-2011), pp. 21–26 (2011)
30. Ismael, P.-L.: ITU internet report 2005: the Internet of Things. International Telecommunication Union (ITU), Geneva, Switzerland (2005)

31. Conti, J.: The Internet of Things. Commun. Eng. **4**(6), 20–25 (2006)
32. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
33. Vermesan, O., et al.: Internet of Things strategic research roadmap. Internet of Things: Global Technological and Societal Trends, Aalborg, pp. 9–52. River Publishers, Denmark (2011)
34. Bogdanowicz, M., Scapolo, F., Leijten, J., Burgelman, J.-C.: Scenarios for Ambient Intelligence. Office for the Official Publications of the European Community, Luxembourg (2001)
35. Weiser, M.: The computer for the 21st Century. Sci. Amer. **265**(3), 94–104 (1991)
36. Zheng, J., Simplot-Ryl, D., Bisdikian, C., Mouftah, H.: The Internet of Things. IEEE Commun. Mag. **49**(11), 30–31 (2011)
37. Yan, L., Zhang, Y., Yang, L.T., Ning, H.: The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems. CRC Press, Boca Raton, FL, USA (2008)
38. Bessis, N., Asimakopoulou, E., Norrington, P., Thomas, S., Varaganti, R.: A next generation technology victim location and low level assessment framework for occupational disasters caused by natural hazards. Int. J. Distrib. Syst. Technol. IGI **2**(1), 43–53 (2011)
39. Bessis, N., Asimakopoulou, E., French, T., Norrington, P., Xhafa, F.: The big picture, from grids and clouds to crowds: a data collective computational intelligence case proposal for managing disasters. In: 5th IEEE International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC-2010), pp. 351–356. Japan (2010). ISBN: 978-0-7695-4237-9
40. Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor network survey. Comput. Netw. **52**(12), 2292–2330 (2008)
41. Akyildiz, F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
42. Latré, B., Braem, B., Moerman, I., Blondia, C., Demeester, P.: A survey on wireless body area networks. Wireless Netw. **17**(1), 1–18 (2011)
43. Hartenstein, H., Laberteaux, K.P.: A tutorial survey on vehicular ad hoc networks. IEEE Commun. Mag. **46**(6), 164–171 (2008)
44. Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., Oliveira, A.: Smart cities and the future internet: towards cooperation frameworks for open innovation. The Future Internet, pp. 431–446. Springer, Berlin, Heidelberg (2011)
45. Bassi, A., Horn, G.: Internet of Things in 2020: A Roadmap For The Future. European Commission Information Society and Media, Brussels, Belgium (2008)
46. Bandyopadhyay, D., Sen, J.: Internet of Things: applications and challenges in technology and standardization. Wireless Pers. Commun. **58**(1), 49–69 (2011)
47. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of Things: vision, applications and research challenges. Ad Hoc Netw. **10**(7), 1497–1516 (2012)
48. Chopra, M., Dave, M., Madan, M.: Social network analysis (SNA): In: Facebook higher education groups through NASA (network analysis software applications). Int. J. Artif. Intell. Knowl. Discov. (IJAIKD) (2015)
49. Meenu, C., Meenu, D., Madan, M.: Analysing online groups or the communities in social media networks by algorithmic approach. In: Computer Society of India (CSI). Springer (2017)
50. Meenu, C., Meenu, D., Mamta, M.: The mesoscopic structural analysis of communities within Facebook higher education online groups. Int. J. Inf. Commun. Comput. Technol. JIIMS-8i, **3** (2) (2016)
51. Meenu, D., Meenu, C., Mamta, M.: Predictions and recommendations for the higher education institutions (HEI's) by exploring and analysing social networks on Facebook. In: International Conference on Computing for Sustainable Global Development, IndiaCom, Bharati VidyaPeeth. IEEE Explore (2016)
52. Meenu, C., Mamta, M.: Social media analysis (SNA) using online students opinions on academic determination in higher education. Online Int. Interdisc. Res. J. (OIIRI) **V**(special issue) ISSN 2249-9598 (2015)

53. Chopra, M., Dave, M., Madan, M.: Flipped classroom: the right solution to competent higher education institutions (HEIs). Int. J. Artif. Intell. Knowl. Discov. (IJAIKD) **5**(3) (2015)
54. Kranz, M., Roalter, L., Michahelles, F.: Things that twitter: social networks and the Internet of Things. In: Proceedings of the What can the Internet of Things do for the Citizen (CIoT) Workshop 8th International Conference on Pervasive Computing (Pervasive), pp. 1–10 (2010)
55. Baqer, M., Kamal, A.: S-sensors: integrating physical world inputs with social networks using wireless sensor networks. In: Proceedings of the 5th International Conference on Intelligence Sensor, Sensor Network and Information Processing (ISSNIP), pp. 213–218 (2009)
56. Ning, H., Wang, Z.: Future Internet of Things architecture: like mankind neural system or social organization framework? IEEE Commun. Lett. **15**(4), 461–463 (2011)
57. Baqer, M.: Enabling collaboration and coordination of wireless sensor networks via social networks. In: Proceedings of the 6th IEEE International Conference on Distribution on Computing in Sensor System Workshops (DCOSSW), pp. 1–2 (2010)
58. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The Social Internet of Things (SIoT)—when social networks meet the Internet of Things: concept, architecture and network characterization. Comput. Netw. **56**(16), 3594–3608 (2012)
59. Atzori, L., Carboni, D., Iera, A.: Smart things in the social loop: paradigms, technologies, and potentials. Ad Hoc Netw. **18**, 121–132 (2014)
60. Guinard, D.: A web of things application architecture: integrating the realworld into the web. Ph.D. dissertation. ETH Zurich, Zurich, Switzerland (2011)
61. Pintus, A., Carboni, D., Piras, A.: PARAIMPU: a platform for a social web of things. In: Proceedings of the 21st International Conference on Companion World Wide Web, pp. 401–404 (2012)
62. Zhang, A., Cheng, C., Ji, Y.: Architecture design for social web of things. In: Proceedings of the 1st International Workshop Context Discovery Data Mining, p. 3 (2012)
63. Console, L.: Interacting with social networks of intelligent things and people in the work of gastronomy. ACM Trans. Interact. Intell. Syst. (TIIS) (to be published)
64. Vazquez, I., Lopez-De-Ipina, D.: Social devices: autonomous artifacts that communicate on the internet. The Internet of Things, pp. 308–324. Springer, Berlin, Germany (2008)
65. Meenu, C., Mamta, M.: Network analysis by using various models of the online social media networks. Int. J. Adv. Res. Comput. Sci. **6**(1), 111–116 (2015)
66. Guinard, D., Fischer, M., Trifa, V.: Sharing using social networks in a composable web of things. In: Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications. Workshops (PERCOM), pp. 702–707 (2010)
67. Semmelhack, P.: Social Machines: How to Develop Connected Products That Change Customers' Lives. Wiley, Hoboken, NJ, USA (2013)
68. Lee, G.M., Rhee, W.S., Crespi, N.: Proposal of a new work item on social and device networking. In: ITU Telecommun. Standard. Sector, SG13 Rapporteur Group Meeting. Geneva, Switzerland (2013)
69. Meenu, C., Mamta, M.: Social network wrappers (SNWs): an approach used for exploiting and mining social media platforms. Int. J. Comput. Appl. **97**(17), 31–34 (2014)
70. Meenu, C., Mamta, M.: To investigate relationships through text, link and spacial-temporal information in social media networks. Int. J. Sci. Technol. Res. (IJSTR) **4**(3) (2015)
71. Chopra, M., Madan, M.: Using mining predict relationships on the social media network: Facebook (FB) international. J. Adv. Res. Artif. Intell. (IJARAI) **4**(4) (2015)
72. Meenu, C., Mamta, M.: The education gets the facelift by going social. Int. J. Appl. Innov. Eng. Manag. **2**(12), 50–53 (2013). ISSN 2319-4847
73. Chopra, M., Madan, M., Dave, M., Mahapatra, C.: Trends and pattern analysis of social networks. In: Banati, H., Bhattacharyya, S., Mani, A., Köppen, M. (eds.) Hybrid Intelligence for Social Networks, pp. 537–570. Springer, Cham (2017)
74. Chopra, M., Mahapatra, C.: Comparative analysis of network analysis software applications. Vivekananda J. Res. (VJR) **6**(2), 122–133 (2017). ISSN 2319-8702

75. Chopra, M., Madan, M., Dave, M.: Analyzing online groups or the communities in social media networks by algorithmic approach. In: ICT Based Innovations. Advances in Intelligent Systems and Computing. Springer (2017)
76. Chopra, M.: Mahapatra, C: Implementing big data analytics through network analysis software applications in strategizing higher learning institutions. In: Big Data Processing Using Spark in Cloud. Studies in Big Data, vol. 43. Springer, Singapore (2018)

Chapter 18
IoT Data Management—Security Aspects of Information Linkage in IoT Systems

Mohd Abdul Ahad, Gautami Tripathi, Sherin Zafar and Faraz Doja

Abstract The rapid pace of data generation requires tools and techniques for its efficient handling and storage. With the emergence of Internet of Things (IoT) technology, we have witnessed a total paradigm shift in computing techniques. The world is steadily moving towards the realization of Nanotechnology wherein the computing devices are getting miniaturized yet providing powerful computing capabilities. IoT is finding its ways in almost every sphere of computing and related services. A typical Internet of Things (IoT) ecosystem consists of thousands of miniature chips, devices and objects forming systems and subsystems which generates huge amount of data and information. The data from these devices interacts with each other to provide services to the users. However, these interactions sometimes may lead to unintended data leakages and security breaches thus compromising the security and privacy of the stakeholders. The most pertinent factor which comes as a hindrance is the varied nature of the data captured and processed by IoT devices. Since individual IoT devices are largely of different make, model and manufacturer, they capture and process data in their respective formats. Therefore it is essential to devise mechanisms, tools and techniques for standardizing the data captured from different IoT devices. The security of the data and the privacy of the users and devices are the other two important factors which must be addressed in order to develop an effective and efficient IoT ecosystem. Therefore, it is imperative to develop tools, techniques and architectures to ensure privacy preserved, secured and efficient data integration and information linkage among the participating devices in an IoT ecosystem. This chapter provides a

M. A. Ahad (✉) · G. Tripathi · S. Zafar · F. Doja
Department of Computer Science and Engineering, School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi 110062, India
e-mail: itsmeahad@gmail.com

G. Tripathi
e-mail: gautami1489@gmail.com

S. Zafar
e-mail: zafarsherin@gmail.com

F. Doja
e-mail: farazdoja91@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_18

detailed overview of IoT ecosystem primarily focusing on the aspects of data management, privacy and security of data along with the various security aspects of information linkage in a typical IoT ecosystem and proposes an improved architecture for a secure and privacy preserved IoT ecosystem. The chapter also provides state-of-the-art review of the latest researches about effective data management in IoT ecosystem. Finally the issues and challenges present in effective data management, information linkage and security of IoT devices and system are highlighted along with the future research directions.

Keywords Data management · IoT · Wrapper layer · Security · Information linkage · Sensor · Actuator · Big data

18.1 Introduction

IoT has emerged as a new and promising technology in recent years. This novel paradigm in the field of modern wireless telecommunication aims at connecting and facilitating interaction among objects of everyday life with an objective to set them as a single entity [1, 2]. The past decade has seen significant researches in an attempt to study the range and domain of IoT applications in the development of smart-cities, smart devices and appliances, smart healthcare, smart agriculture, sophisticated miniature sensors, visual display units and smart transportation etc. The current trend in the field shows that in near future IoT will facilitate the generation of large volumes and variety of data that will open new horizon of information to provide better services to people, businesses and public administrations. Figure 18.1 shows the number of IoT devices that will be connected worldwide by 2025 as per "Statista Research Department website" [3].

This IoT technology has unprecedented applications in varied domains including home automation, smart and predictive healthcare, smart designing, sustainable and intelligent power management, smart grids, smart transportation, smart agriculture and smart education. The broad application area and scope of this budding technology comes with a number of challenges and issues that needs to be catered. The major technological challenges in the field include security, connectivity, interoperability, standards, compatibility and longevity, intelligent analysis & actions. Apart from these, some other challenges are mobility, reliability, scalability, management and availability.

With the advent of technology, IoT systems are slowly coming into the mainstream for computing and servicing facilities. Since this technology depends mainly on the wireless networking and sensors for connection and communication among objects, the selection of these wireless networks and sensors plays a vital role in the success of an IoT system. For every device working in this automated environment, there is a possibility of an unintentional leakage of data and information, revealing insights about the user, subject and its surroundings [4]. This situation may lead to serious security threats. This chapter proposes a novel architecture for a secured and

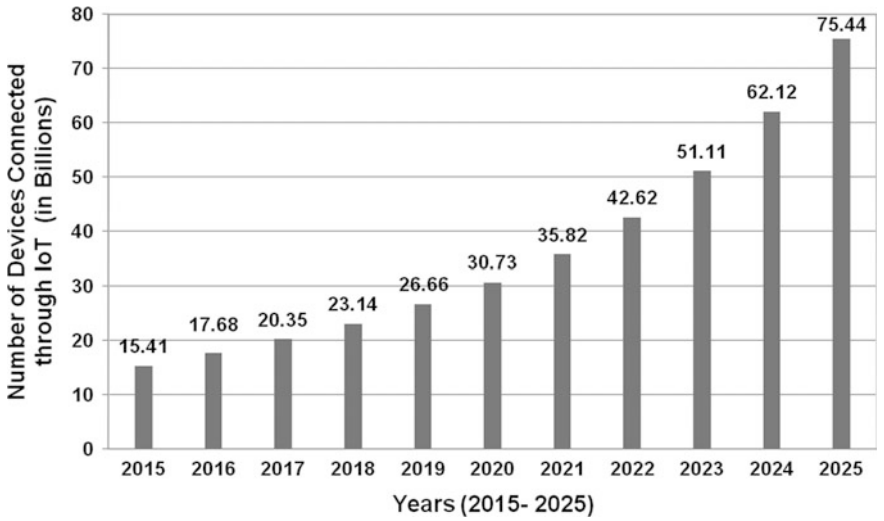


Fig. 18.1 Projected number of devices using IoT technology

privacy preserved IoT ecosystem by identifying the various security aspects of information linkage among connected devices and objects that aims to overcome the data leakage (leading to security threats) during the data integration phase. IoT is a dynamic and worldwide system foundation, wherein every participating entity of the IoT ecosystem is recognizable, independent, and self-configurable. Each entity needs to connect and communicate among them and associate with each other by following predefined sets of protocols. They are also responsible for responding to occasions and activating activities to perform the requested and intended services. IoT technology aimed to create an umbrella under which agreeable administrations and applications are developed among devices and components. At the focal point of these IoT components is the abundance of data that can be interlinked and accessible through the combination of information that is created progressively just as information put away in perpetual stores. This data can provide unprecedented insights into the systems and its users. These insights can be used to provide novel correlations and mine unknown values from the data. A complete administration system of information that is created and put away by the items inside IoT is created along these lines of objectives [1, 2].

Information is an expansive idea alluding to the designs, practices, and methods for legitimate administration of the information lifecycle necessities of a specific framework. With regards to IoT, information should go about as a layer between the items and gadgets creating the applications for examination and administrations. The gadgets themselves can be orchestrated into subsystems or subspaces with independent administration and inward progressive administration. IoT information has unique qualities that cannot be arranged and managed using classical database schemas. A huge volume of heterogeneous, spilling and topographically scattered

continuous information will be generated by many assorted gadgets occasionally sending perceptions about certain observed phenomenon or revealing the event of certain or strange occasions of intrigue.

The information of IoT devices is either possessed by individual associations or open proprietors and they can be stored at local servers or on the cloud. Associations or individual clients approach these vaults by means of questions and inquiries and choose which storehouses hold the required information, and chose the path to procure the information.

18.1.1 Organization of the Chapter

The current chapter is organized into 8 sections. The first section provides an overview of the IoT technology, its architecture and historical background and working principles. Section 2 provides the state-of-the-art reviews of IoT technology specifically focusing on the data management designs, issues and challenges. Section 3 talks about the security aspects of the information linkages in IoT ecosystem. It further provides a use case of a smart home environment using IoT devices. The fourth section provides an introduction and architecture of data management in IoT ecosystem. The various issues and challenges in data management are also highlighted here. Section 5 provides the various applications of IoT. Section 6 highlights the need of sustainable approaches for IoT data management. Section 7 presents the proposed architectural framework for managing IoT big data in an effective and energy efficient manner. The final Sect. 8 concludes the chapter. It also provides the future research directions in IoT data management.

18.1.2 IoT Ecosystem

The IoT ecosystem consists of a vast network of real world objects, sensors and actuators which are connected together to form a single entity which is more intelligent and capable of interacting with the end-users, external environment and among each other. A number of protocols govern this successful interconnection of objects ensuring the standardization, reliability, interoperability, compatibility and a better performance on a universal scale. Figure 18.2 shows the various components of an IoT ecosystem [5, 6].

The network provides a wireless communication medium and its underlined protocols that connect together various objects of everyday life. Sensors are used for data collection and actuators are used when a device needs to be switched on/off thus triggering various devices into operations based on the requirements. Thus, sensors and actuators together provide maximum automation forming the backbone of an IoT ecosystem. Platform provides a middleware to facilitate connection and interoperability amongst various IoT components. Data from multiple objects is

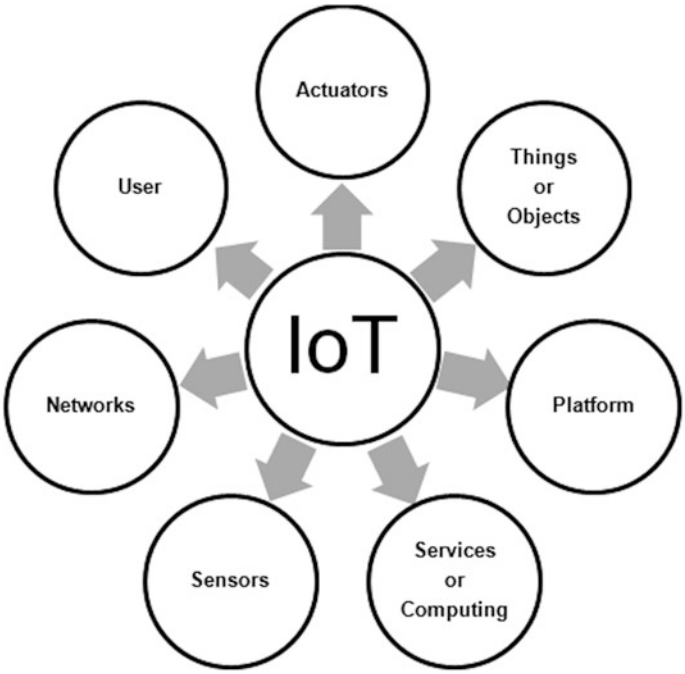


Fig. 18.2 Components of IoT ecosystem

integrated and analyzed to make intelligent decisions. In a classical IoT ecosystem mainly three types of communication occur namely: "device to device (D2D)", "device to server (D2S)" and "server to server (S2S)". The data generated by the sensors is communicated to a data centre or a cloud where it is integrated with other data as per requirements. This functionality can be represented in a multi-layer architecture with each layer being governed by a set of protocols. Figure 18.3 shows the various protocols in an IoT ecosystem.

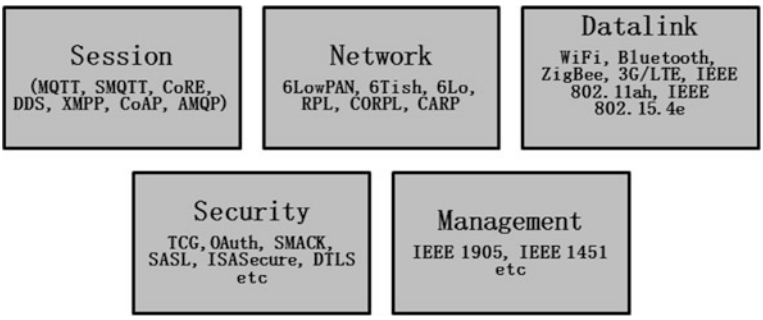


Fig. 18.3 IoT protocols [7]

The data link layer protocols define the frame type, formats and standards, communication strategies among the nodes, synchronization standards and efficient bidirectional packet exchanges. The network layer is being divided into two parts. The routing part is responsible for reliable transfer of data packets from source to destination. "Routing protocol for Low Power and Lossy networks (RPL)" is the most commonly used protocol in IoT applications. The session layer employs a number of protocols to define standards for secure message passing. "Message Queuing Telemetry Transport (MQTT)" is the prominently used protocol in IoT because of its power efficiency and low overhead. However these protocols are application specific and their choice may vary with different organizational needs and applications. The diversity of protocols and standards at multiple layers makes management protocols an important part of IoT ecosystem. The main objective of these protocols is to provide an interconnection of heterogeneous data links and a smart transducer interface. Another major aspect of an IoT ecosystem is security. The security protocols in IoT aims at ensuring the confidentiality, authentication, privacy, access mechanisms and synchronization of the data and the participating devices.

18.1.3 IoT—A Historical Overview

The term "Internet of Things (IoT)" was first coined by Kevin Ashton in his presentation made to "Procter & Gamble" in 1999. Although the term IoT has gained popularity in the recent past, similar concepts had already existed in with the machines communicating with each other since the telegraph was developed in 1830s. One such example of a similar concept is seen at the Carnegie Mellon University where a Coca Cola machine used internet to connect to the refrigerator unit to check for the available drinks. The significant components of IoT like the internet, IPv6, sensor technologies etc., have also existed for a long time. A similar concept was also presented in 1999 in a book by MIT Professor Neil Gershenfeld titled "When things start to think". Machine to machine (M2M) communication was also based on similar concept where machines connect to each other over a network without any human interactions. IoT technology came as one step ahead of M2M communication where all entities like devices, people, systems, and applications are connected together to form one single network. Today, Internet of things is one of the fastest growing technologies with widespread usage and application domains. With the increasing technological advancements and penetration of these technologies in day to day life the IoT concept has a way to go forward.

18.1.3.1 Working of the IoT Eco-System

The IoT of things ecosystem consists of connected entities that use modern day technologies like wireless sensor networks, embedded systems, internet etc. to

communicate, collect and share data and act accordingly. The working of a typical IoT system can be categorized based on the technology used at different steps. The major IoT components that define the working of any IoT based systems are:

Sensors: sensors are used to collect data from the several connected devices and the environment. This data forms the base for future applications like analytics, decision making, AI, ML etc.
Connectivity: the data collected by sensors is moved to the cloud storage. This movement is facilitated by the connectivity provided by the various mediums of communications and transport.
Data Processing: The data collected at the cloud storage undergoes analysis and analytics for servicing the users.
User Interface: the generated information after several rounds of analysis and analytics is provided to the end users by means of a well defined interface.

18.1.4 Issues and Challenges in IoT Ecosystem

The increasing popularity of IoT technology has brought together a myriad of devices connected together and generating volumes of data that is beyond astounding. Today, IoT has become one of the major contributors of data. The growth of the technology, its application areas and widespread implementation has raised serious concerns to reevaluate the existing data management strategies from the point of scale, integration, security and data gravity [8–13].

Some of the major challenges and issues are

- Integrating the IoT Data

One of the major challenges that service providers face today is to integrate the IoT data with other enterprise data sources. Today, many technologies are providing analytics on the enterprise IoT data but what about the data generated outside of IoT ecosystem. For efficient analytics and decision making there is a need to combine and correlate the entire organizational data generated from all sources.

- Scalability of the Infrastructure

The rate at which data is generated today has raised serious concerns about the capabilities of the existing IoT infrastructure. In the past, the decreasing cost and size of the storage facilities has somewhat alleviated the issue of the data explosion but the current state of the IoT data generation has posed a much needed requirement of renewing the entire data lifecycle. Today, organizations are opting for the cloud technology for their storage requirements but the challenge remains how to support and keep pace with the increasing applications, operations, varieties and sources of data and the heterogeneity of the systems.

- Security and reliability

The large volumes of personal user information collected through multiple IoT devices raises concerns related to the privacy of the collected data and information leakage. Since most IoT devices are interconnected and works in collaboration with each other, it becomes easier for cybercriminals to penetrate into the data pool via any of the devices. Moreover, in worst situations the hackers can take control of the device and manipulate the data.

- Data Governance

With thousands of data sources available and millions of devices connected to the IoT network, the generated pool of data is highly heterogeneous in nature which requires an efficient and standardized data governance system. Data governance ensures a well defines association of organizational tasks by making the information logical and organization specific. But today, with the amount of data generated, it had become a major challenge to ensure efficient data governance.

- Data Ownership

The amount of data and velocity at which the gets transferred from one location to another, it become very crucial to identify who owns the data when it in transit. This is particularly important when there is a data breach or theft.

- Lack of Skilled Workforce

Since the technology is changing so rapidly, there is a huge scarcity of workforce responsible for handling this technology. Thus organizations are not able to widely adopt this technology.

- Lack of Awareness

Smaller organizations are not able to exploit the advantages of IoT technology because of several reasons like: lack of infrastructure, lack of skilled workforce, accessibility etc.

18.2 Related Works

IoT has brought a complete paradigm shift and has a great potential to transform the lives of the human beings. Everyday use objects, appliances and devices are networked together under the umbrella of IoT and can be controlled remotely using smart phones. Furthermore, with the presence of sensors and actuators, these objects and devices are trained to act and respond automatically according to the situations with the help of powerful artificial intelligence mechanism. The rapidly growing usage and popularity of this technology has raised concerns related to the security and privacy aspects of the devices connected to an IoT ecosystem and the

data generated. The last few years have seen many researches in the area of security aspects of Internet of Things.

The authors in [8] propose a mechanism for "distributed traffic monitoring" of the IoT devices using a SDN gateway. This mechanism was able to detect the anomalous behavior and take corrective measures to ensure optimal data transfer. The study in [9] provides a security analysis of IoT protocols and explored the CoAP security aspects over DTLS. They also highlighted the issues and proposed solutions for the same. The authors in [10] presented a system called IoT Sentinel that can automatically identify the types of devices that are connected to the IoT system and enforce the rules governing the communication so as to minimize the security issues. In [11] the authors discusses the security issues related to IoT and cloud computing. Further they discussed how the cloud computing can enhance the IoT technology by combining the two and examining their common features and the advantages of their integration. The researchers in [12] put forth an IoT architecture based on the light weight bit coin that maintains the security and privacy aspects of traditional bit coins while eliminating the overheads. In [13] the authors presented potential research areas related to how fog computing can enhance the security aspects of IoT system. They further proposes a mechanism to improve the security among IoT devices by using fog computing. The authors in [14] considered 8 IoT frameworks for presenting a survey on the security of IoT frameworks. The work presented in [15] proposes a scheme for "Smart Home Systems" which are energy efficient, secure and uses privacy preserving communication protocols. Chaotic systems are used to generate secret keys for symmetric encryption to secure the transmissions within the "Smart Home Systems". In [16], the authors performs a network wide address shuffling process using the "address shuffling algorithm" with "HMAC (AShA)" which is successful in performing a "global collision free address renewal" on the networks with more than 2000 nodes and 16 bit addresses. The authors in [17] presented the machine learning based solutions for IoT security with an emphasis on "authentication", "access mechanism" and "malware detection". They also highlighted the challenges in implementing these ML based security techniques in practical IoT systems. The authors in [18] uses edge computing to present a reconfigurable security framework for IoT systems that claims to overcome the security challenges for IoT like high computation cost, key management and deploying new security system in IoT. In [19] the authors have used the "InterPlanetary File System" and "Block chain" technology to develop an IoT security model that helps to avoid the security risks of traditional IoT architectures. The authors in [20] used the "X.509 authentication mechanism" to enhance the security of an IoT system. In [21] the authors have mentioned the advantages of using cloud platform for IOT based data management like low cost, scalability and anywhere access among others. The authors in [22] have mentioned that only a few enterprises will have sufficient storage to house all the data which has been collected from the various sensors. Also, the data created through IoT even though valuable exposed many avenues for potential security threats to take advantage.

In [23] the authors had suggested an architecture for cloud based IoT computing using "Aneka" a.NET based "Platform-as-a-service (PaaS)" and "Microsoft Azure" a cloud platform. This architecture has many advantages like multiple programming models, runtime execution and scheduling capabilities among others. The authors in [24] have discussed the various challenges faced with the use of RFID tags like electromagnetic interference making it difficult for the RFID readers to read the tags. Unprotected RFID tags are exposed to eavesdropping. Another issue is the integration of RFID system with existing applications requiring the need to develop an effective RFID middleware. In [25] the authors have mentioned several challenges facing big IOT data analytics like privacy concerns with people being reluctant to use these systems due to weak service-level agreements. Data mining relevant information and integration of the data is a challenge with the data produced through sensors due to the diversity of the data. Another challenge which has been mentioned is the visualization of the data due to high dimensionality. In [26] the authors discussed low cost technology implementation for monitoring of home conditions by using "ZigBee sensor network" along with in house developed sensors to monitor water, temperature and electrical appliances. Through experimental evaluation it was concluded that the system achieved an overall reliability of 97%. In [27], the authors discussed the three separate layers for IoT Architecture namely the "Perception Layer" which deals with collecting data from sensors, "Network layer" which is involved in transmission of data over the internet and "Application layer" which ensures the high quality of data. In Perception layer the strength of the wireless network leads to susceptibility to attack which can be resolved using encryption. In Network layer attackers can eavesdrop on confidential data, this can be addressed by using software which responds to abnormal traffic. Application layer has its own set of challenges chiefly what data is available to which user. This can be achieved by using software tools which control data. The authors in [28] discussed the challenges with managing data for smart cities using cloud computing chiefly latency and security. They further go on to mention that fog computing achieves higher speed and more security on the account of the fact that data is being processed within the device itself without the need for it to be transferred to cloud for processing. In [29] the authors discussed the use of cloud manufacturing (CMfg) for IoT systems. A five layer architecture is discussed composed of Resource layer consisting of manufacturing resources and computational resources, perception layer which includes sensors and adapters, Network layer to transfer the data between devices, Service layer and Application layer which aids in the use of CMfg services. The authors is [30] discussed that mobile devices can be used to solve many purposes in the Shanxi province in China like they could be used to monitor environment pollution, security monitoring. Also, smart power meters can be created by installing a SIM card in the meter.

Although many techniques are proposed to mitigate the security concerns in an IoT ecosystem yet we are far from achieving a perfectly secure and privacy preserved IoT system. In our approach we have tried to gain insights from the previous researches and aimed to step forward in the direction of achieving a perfectly secure and privacy preserved IoT ecosystem.

18.3 Security Aspects of Information Linkage in IoT Systems

This section provides the security aspects of an IoT ecosystem that are vital to privacy and must be addressed while creating any IoT system. Figure 18.4 presents the different components of "security aspects of information linkage" in IoT systems.

User Privacy: It means that the user's personal information like locations and demographics must not be compromised at any point of time. This is pertinent for ensuring that the user profiling of any type cannot be done.
Data Privacy: The data originated from individual participating devices or objects should not be exposed to other objects. This means that the data of one IoT device should not be exposed to other IoT devices until shared voluntarily.
Device privacy: Every individual IoT device in an IoT system is equally important. It must be ensured that the device(s) should not be exposed to any external threats and if so, mechanisms must be in place to counter such situations.
Accessibility: There should be controlled access to the devices and objects. Any unauthorized or unauthentic access must be prevented and reported.

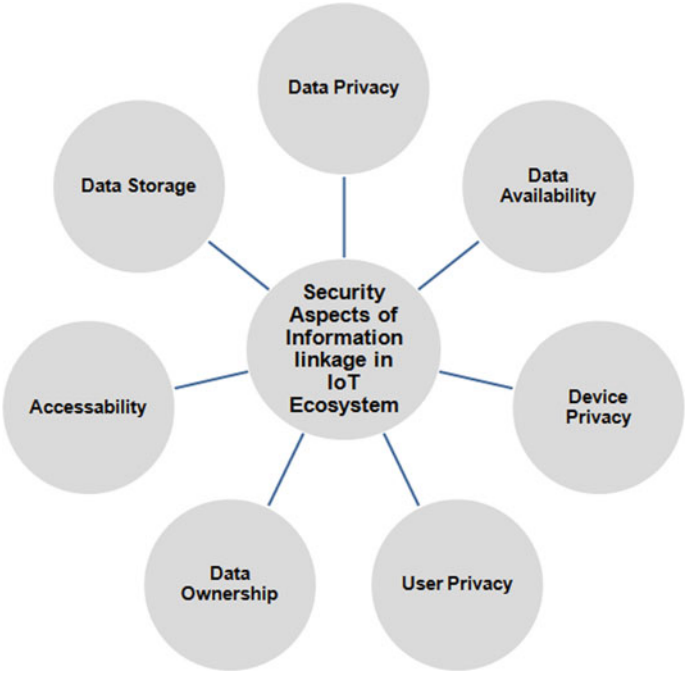


Fig. 18.4 Security aspects of information linkage in IoT systems

Data Ownership: Data ownership is a critical aspect during the information linkage phase in IoT system. The questions like "who owns what data and at what time" must be clearly identifiable otherwise there are chances of user repudiation regarding the ownership of the data in case of any data related crimes.
Data Availability: When data is generated from multiple sources and is being integrated, there are chances that there is a delay in retrieving the intended data for servicing the user request. Since IoT is largely a real time system, it is expected to service the user request instantaneously as and when required. Therefore techniques must be devised to ensure timely availability of the data. Furthermore, it must also be ensured that a legitimate device(s) is providing a legitimate data to the legitimate user.
Data Storage: Since the data from multiple sources are collected and stored at multiple sites in a distributed manner. It is imperative to ensure that the stored data remain protected from any kind of threats. Such type of storage systems and mechanisms must be devised which ensure full protection of data and information stored within them.

18.3.1 Scenario of a Smart Home: A Practical Case for Demonstrating the Need for Securing Data During Information Linkage Phase

A smart home is one where every object, appliance, system or device (like fans, tube-lights, Tvs, fridge, ACs, Microwaves, PCs, CCTVs, Washing machines, Electricity meters, geysers, Doors, Windows, Alarms, water taps etc.) is equipped with multiple chips and sensors allowing communication and information sharing for efficient decision making. These chips and sensors store a huge amount of data and information which enables them to take appropriate decisions as per the requirements of the users. These objects, systems or devices are connected using wireless medium like wireless sensors network (WSN), Bluetooth, infrared etc. The sensors sense the surroundings and acts accordingly to provide the intended services to the users. They work using a very strong Artificial Intelligence System. Figure 18.5 present a typical Smart home workflow scenario [4]. There can be multiple scenarios in a smart home. In one such scenario we can have a situation in which the devices in the smart home belongs to the same manufacturer while in another case they might belong to multiple manufacturers. In case of devices belonging to multiple manufacturers, there is a need of complex data integration and management techniques as different devices have different build, make, versions, data handling and storage formats as well as metadata requiring different sets of protocols for local data handling, connection and communications. The data originating from different devices, systems and subsystems are coalesced,

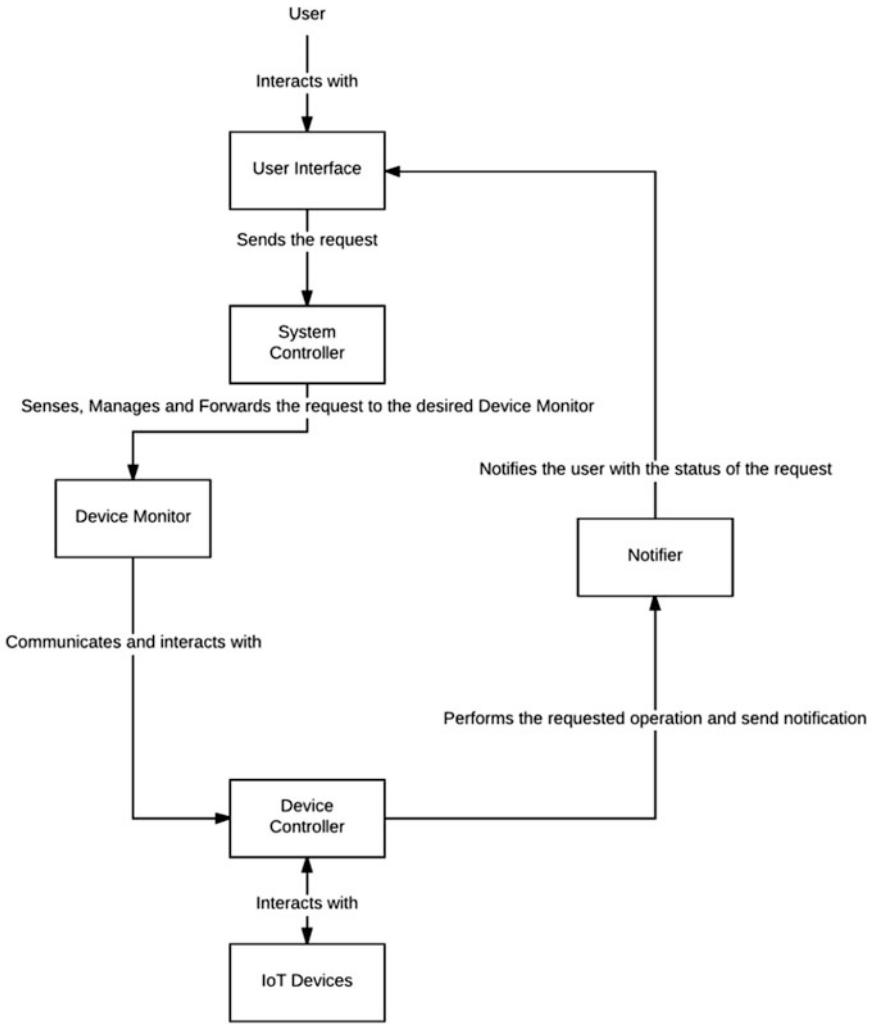


Fig. 18.5 IoT based smart home

aggregated, integrated, mapped and correlated to ensure quality and effectiveness of the requested services.

Now let us consider a situation where the user is out for work and an unauthorized person hacks into the system and gains access to the home. Inside the home, the kids are playing. There are fair chances that the intruder may harm the kids apart from stealing valuables from the home. In another situation, a user Mr. X has a heart disease and he has a pacemaker installed in his body, if the intruder hacks into it and stops it. What will happen to Mr. X? He will surely die. There can also be situations where an intruder might gain access to the information stored in

the IoT systems allowing him an access to vital personal and financial information about the user. These intruders can very easily profile the users and use the sensitive personal and financial information for their own good causing serious harm to the user. Once a user's profiling is done, all the information related to his daily routine, habits, schedules and other personal and sensitive information will be exposed thus compromising the security and privacy of the user. Think about a situation where the intruder knows at what time you wake up, what route you follow to go to the office, how much time you take commuting and what are your hobbies? Such situations can have catastrophic outcomes as the personal and private life of the user is totally exposed.

This is just one example where IoT is used. Today the application areas of IoT are increasing rapidly as the technology provides innumerable services to the users. But with all those advantages there are chances of security and privacy breaches. To overcome and prevent such haunting and catastrophic situations, it is pertinent to develop tools and techniques such that the user privacy and security should never be compromised. This chapter proposes an architecture that aims to overcome the above mentioned limitations and provides privacy preserved and secured IoT system.

18.4 Data Management in IoT

The data collected using IoT devices is largely in different formats and is rapidly evolving. The main concern with IoT is the real-time handling of the requests to provide instantaneous services to the users. This means that the data captured by various sensors embedded in the IoT devices needs to be handled in real-time also. This poses a real challenge for the data management software and tools. The classical big data management approaches cannot be directly applied for managing IoT data and thus we need specialized mechanisms and tools to handle such rapidly generated data which is primarily unstructured. Since the sensors have the ability to sense and capture the surrounding environment of the target location or object there are chances that a large amount of noises are also captured in the process. Now in order to make any sense out of the captured data, it is imperative to remove noises and other disturbances from the data and that too in a real-time manner. Secondly effective mining of the relevant data also poses a huge challenge. Real-time data mining techniques must be adopted to mine the desired data from the gigantic volumes of data captured by the sensors. Finally in order to extract value from the data it is necessary to convert the data captured from several sources into a standard format. Once the data is converted into the standard format it becomes easier to apply analytics on the data to delve deep into the data for extracting valuable insights. These insights can be very useful for providing user centric personalized services [25, 31–35].

Apart from the real time analysis, it is equally important to store the IoT data so that unidentified patterns and correlation among the data can be identified to

provide better services to the users and take informed and data driven decisions. Archival data provides a very strong means to unfold several baffling correlations and inter-linkages among the various entities of the IoT ecosystem.

For effectively managing the insertion, deletion, updation and processing of the IoT data, new database designs must be proposed addressing the following vital driving factors.

1. Adaptable Data model: With IoT, the data is always evolving and novel formats and structures of data are being identified every other day. The database must be adaptable to such changes.
2. Flexibility: The database must be flexible to incorporate any changes in the design and data model at any stage.
3. Scalability: With such deluge of IoT data being generated every passing data, the data storage systems must have the ability to incorporate the storage of such huge data sets. A good distributed environment with optimal synchronization and consistency is required to realize these kinds of systems.
4. Cohesive: The database must be able to present a holistic view of the overall structure and the data stored in it.

Figure 18.6 given below provides a structure of a typical IoT data management system.

18.5 Applications of IoT

With is innumerable benefits, IoT has found its applications in almost all domain of computing and other societal domains [31–34]. Figure 18.7 presents the various applications of IoT.

- Smart cities: The emergence of the concept of smart cities is one of the most talked about application of IoT. According to a report in [36], 20% of the IoT based projects are dedicated to the development of smart cities. Ever since IoT was conceived there has been an upward trend in the development of smart cities, many countries are now adopting this technology for transforming their cities to Smart cities. Intel and Siemens have developed a smart parking solution deployed in the city of Berlin [37]. Another such example is the Smart dustbins in Dublin [38]. One of the major aspects of a smart city revolves around its security systems. One such example is the City Pulse IoT project in Eindhoven [39].
- Smart education: The Implementation of IoT in the education sector has resulted in the development of smart learning environments that helps to create efficient, better and easy learning processes. The interconnection of entities in the education domain can help the teachers to better track the progress of the students by remotely monitoring their assignments, homework and other activities. The students can equally benefit from the system by getting an easy access to their

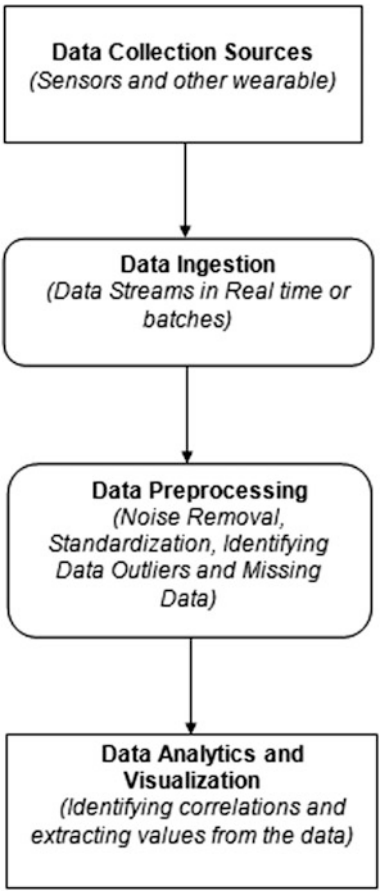


Fig. 18.6 Typical architecture of IoT data management system

academic entries on the go. Parents can also track the academic growth of their wards and can easily reach out to the teachers for discussions.

- Smart healthcare (IoMT): Internet of Medical Things has realized the concept of smart healthcare where all entities and stakeholders are connected together form a smart healthcare ecosystem. IoMT had transformed the way healthcare industry works. The different aspects of healthcare like research, medical equipments, patient monitoring systems, medical information distribution, nursing, emergency care, blood banks, pharmacy etc. can be brought together under the umbrella of Medical IoT to empower the medical fraternity to provide a better way of living and state-of-the-art medical facilities.
- Smart Transportation: Smart transportation systems are one of the most beneficial real life applications of IoT technology. IoT has completely revolutionized the modern transport systems by using sensors, mobile applications, smart traffic lights etc. some of the major aspects of smart transportation systems include:

  - Smart traffic lights
  - Smart roads
  - Smart Traffic management
  - Pedestrian Monitoring
  - Bicycle monitoring
  - Smart Navigation
  - Traffic rules implementation
  - Road safety.

- Smart Homes: In 1923 the "famous architect Le Corbusier" described home as a "machine to live in" [40]. Today, with the advent of the IoT technology this metaphor has turned into a reality. The concept of smart home brings together all the household entities like electric and electronic equipments, smart doors, security systems, fire alarms etc. together and facilitates the communication among them. These entities once connected can share data, communicate and can be remotely monitored and accessed thus providing full automation. One such example of a smart home is the "Jarvis" [41].
- Smart Supply chains: IoT has revolutionized the supply chains by providing the operational efficiencies and revenue opportunities. IoT Supply chain offers services like:

  - Asset monitoring and tracking
  - Scheduled Maintenance
  - Inventory Management
  - Warehouse Management
  - Prevention against product substitution and counterfeit
  - Tracking Damaged goods
  - Logistics management.

- Smart Agriculture: The increased demand for food products has led to the concept of smart farming where all agricultural entities and stakeholders are connected together to form the agricultural IoT. Smart farming allows minimizing wastage and increasing production and provides a clean and sustainable way of producing food. The different aspects of the agriculture IoT includes:

  - Precision farming
  - Smart irrigation
  - Livestock monitoring
  - Soil monitoring
  - Crop monitoring
  - Smart Greenhouses
  - Agricultural drones.

- Wearable Devices: The wearable devices domain is one of the early applications of Internet of Things technology. Today, it is a common sight to see devices like fitness bands, heart rate monitors, smart watches, blood glucose level monitors etc. These devices form a connected network with other smart devices like smart

phones, smart weighing scales, Gym equipments etc. to monitor the overall vitals.

- Industrial IoT (IIoT): The adoption of IoT technology in the industrial sector has led to the rise of Industrial IoT. Today, connected industrial entities are providing great potential for smarter machinery and sustainable potential across all industries. IoT had penetrated into the sector and transformed the traditional manufacturing processes to new smart process to meet the growing production needs. One such example is the Predix platform [42] that provides leading IIoT capabilities like asset connectivity, analysis and analytics, edge computing, machine learning etc. Today IIoT is providing solutions for all domains of industry like:
  - Quality Control
  - Supply chain optimization
  - Logistics optimization
  - Smart Inventory management
  - Product Flow
  - Safety and security.
- Smart Energy: The advances in the IoT technology have initiated the smart grid projects that provide efficient energy solutions by facilitating the development of smart energy resources like wind, solar hydro etc. Smart meters allow the consumers to monitor their energy consumption thus helping to limit the usage. Today, many cities have already initiated the pilot projects to enable their energy sector with IoT. The Pecan street project in Austin, Texas has already received a funding of US$ 10.4 million [43]. Boulder, Colorado had adopted a smart grid system connecting more than 16,000 m to form the world's first fully functional smart grid city [43, 44].

18.6 Sustainable Data Management in IoT

Big data technology is considered as a blessing to the modern day computing paradigms. Intelligent management and processing of big data can open new horizons for the organizations, industries as well as governments. In a nutshell, big data may be defined as any large amount of data that is not manageable by existing computing devices exclusively. These types of data require specialized sets of computing and management devices, tools and techniques. With such rapid advancements in every field of computing, the data is being generated at an exponential rate while the data management devices are not complementing at the same rate and thus there lies a decent gap between the two. Extensive researches are going around the globe in order to find compelling solutions to effectively manage this big data [25, 31–34]. However, with the race of finding out faster solutions the

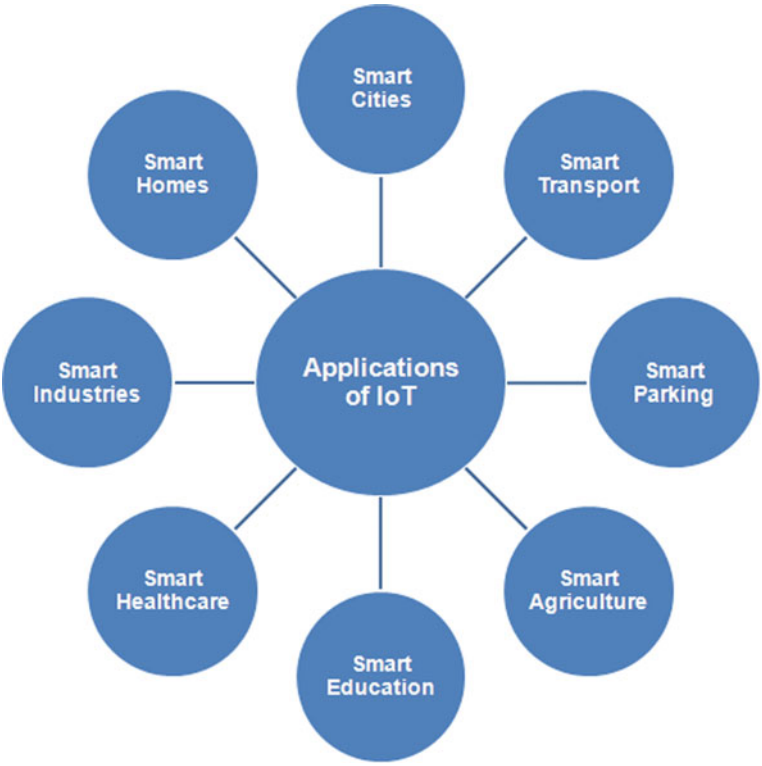


Fig. 18.7 Applications of IoT

organizations look for greedy algorithmic approaches and the after effects of these solutions are often neglected. Although there are solutions which provides decent results in terms for effective big data management, but sometimes have adverse effects on the environment. The drastically changing environment and extreme weather events occurring around the globe are the result of such irresponsible activities and over exploitation of natural resources by human beings. If we didn't stop now, there will come a time when we will not be able to rectify the damage done to the environment. The United Nations have also realized this catastrophic phenomenon and thus came up with 17 sustainable development goals (SDG) to be achieved by 2030. With this aim of attaining an environment friendly and sustainable development environment, novel computing techniques are required to develop solutions for effective and efficient big data management.

With the advent of IoT, we are in an era of information age. The information generated through IoT devices is individually very small but collectively they constitute a massive datasets. The classical big data handling mechanism fails to provide effective and efficient management of these large number of very small size files generated by IoT devices and systems. Devising sustainable tools, techniques

and mechanism for effective and efficient management of IoT big data requires a complete restructuring and revamping of the existing computing methodologies. Some of the best practices for achieving sustainable data management approaches include:

- Using blockchain based approaches throughout the life cycle of the solution development [35, 45–47].
- Using solar powered computing devices.
- Using energy efficient peripheral devices.
- Optimally Identify useful data and dark data.
- Effective clustering of similar type of data.
- Devising time efficient algorithms.
- Finding out means of converting natural phenomenon to create sustainable solutions like using fog to generate water, night glowing trees to replace street lights, using 100% recyclable and biodegradable components to construct devices and solutions.

18.7 Effective Data Management and Information Linkage: The Proposed Architecture

In this chapter a "secure and privacy preserved framework for IoT based systems" is proposed. The core idea is to ensure the "security and privacy of the data and information" transferred through IoT devices. It is an extension of the "RBSEE architecture" [48] for effectively handling data generated through IoT devices. Here the concept of wrapper layer is proposed, wherein the different devices, systems and subsystems will interact with each other under the umbrella of the common wrapper layer without compromising on the security of the data being shared. It will be the duty of the wrapper layer to maintain the confidentiality and integrity of the data at all times during the connection, communication and transfer process. The wrapper layer ensure that the communicating devices share only the minimal mandatory information required, thus preventing any unintentional disclosure of data (giving insights about the subject and its whereabouts) which may cause serious security concerns. The wrapper layer works as a middleware interface between the various devices (along with their local protocols) and the end users.

Figure 18.8 presents the architecture of an IoT system using the concept of wrapper layer. On every request of the user, the wrapper layer is triggered by the participating devices so that the data and information required for servicing the intended request must be captured by the IoT devices as per the instructions of the wrapper layer.

To do so, the wrapper layer collects the required data from individual participating devices, encrypts it and then integrates it with the data of the other participating devices. Also the wrapper layer anonymizes the identity of the individual

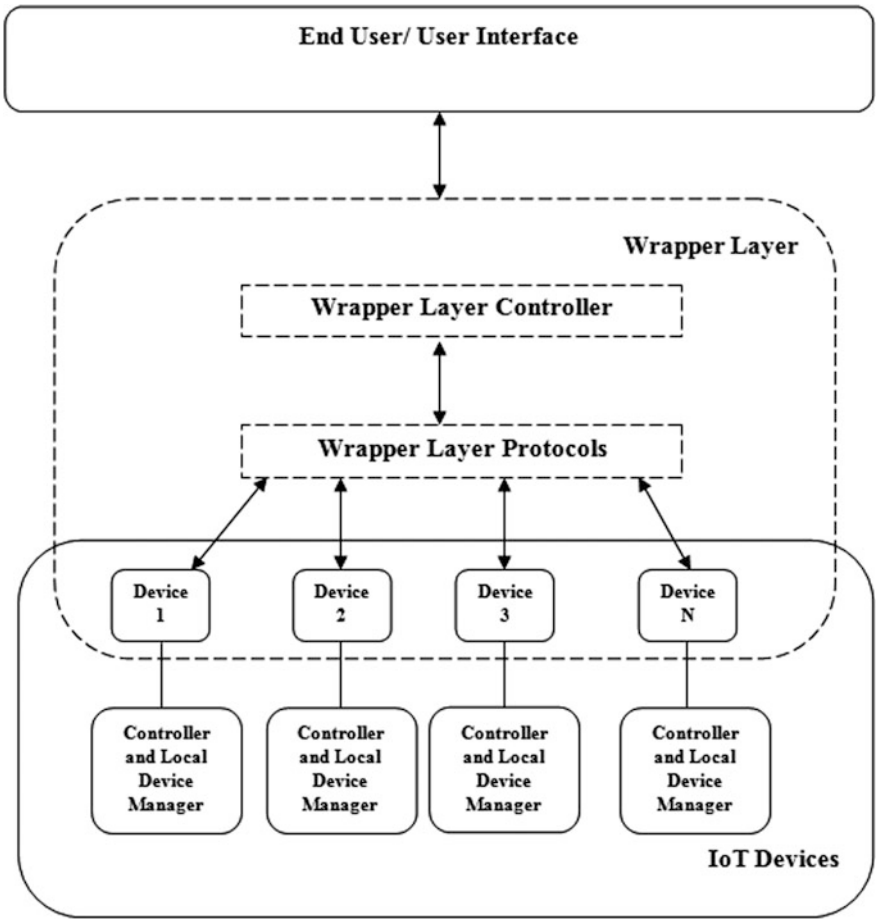


Fig. 18.8 Architecture of IoT system showing the concept of wrapper layer

device so that the devices are not aware of what data is being shared and with whom.

The end user interacts with the IoT system through the user interface. In order to service the user's requests, the wrapper layer performs the following stepwise operations.

1. Identify the types of the service requested.
2. Discover the device(s) which will perform the requested service.
3. Identify the information gathered from individual device which is required to perform the desired operation.
4. Integrates the information from the multiple devices (if required).
5. Instruct the IoT device(s) to perform the requested service.

The wrapper layer is responsible for encrypting and decrypting the information captured by the individual IoT devices. It also standardizes the varied information collected from multiple sources. Figure 18.9 provides the architectural framework of the IoT based home automation system as presented in Fig. 18.8 using the proposed wrapper layer.

Every data and request that passes through the wrapper layer is encrypted in such a way that only the intended users and devices are able to decrypt and analyze it. In order to do so the initial registering of the individual devices with the IoT system also requires storing of the device_id along with other metadata information about the device. The information about all the participating devices of the IoT system is stored in the system controller. Once the data is captured by the individual IoT

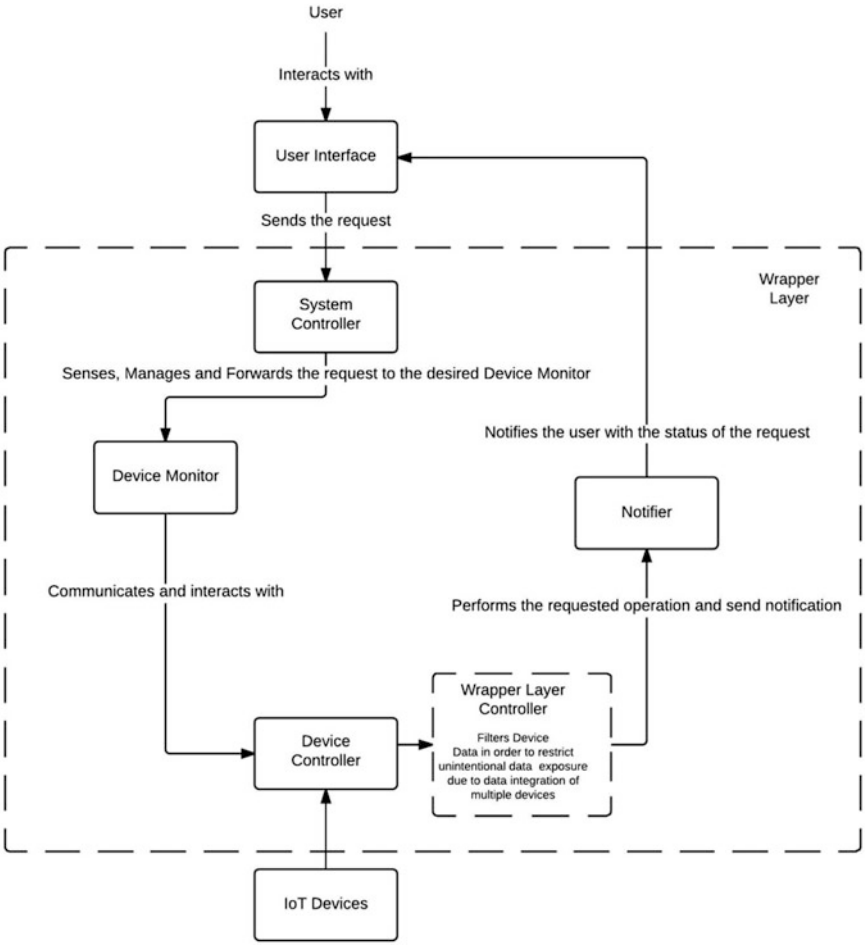


Fig. 18.9 IoT based smart home with the proposed wrapper layer

device, it gets encrypted using the device_id as the encryption key. We propose to use "Twofish cryptographic technique" to secure the data captured by the IoT devices. Since "Twofish is a symmetric key cryptographic technique", only a single key is needed to encrypt and decrypt the data. Another vital reason for selecting Twofish technique is its intricate internal structure with simple implementations which is extremely difficult to break. Also since the device_id is stored in the system controller, it can easily be used to decrypt the data of the individual IoT devices as and when required. Therefore, the introduction of wrapper layer helps to eliminate any security and privacy breaches in an IoT system.

18.8 Conclusion and Future Research Directions

Today, IoT is slowly coming to its pinnacle with its integration in almost all spheres of life. It has penetrated deeply in chores of daily lives. Ranging from smart homes, smart transport and smart healthcare, everything which was once considered as a human fantasy is coming to reality. With such widespread applications and millions of connected devices, IoT contributed to a significant percentage of the data generated. Although the integration of multiple devices into the network generates large volumes of data to provide a number of intelligent services but it also brings with it a challenge to manage such huge volumes of IoT data and to protect the privacy and handle the prospective attacks like denial of service, jamming, spoofing and eavesdropping. This chapter discusses the IoT ecosystem and its applications with a focus on the various security aspects of information linkage in detail. The chapter further presents in detail the concept of data management in IoT and proposes an architecture for efficient data management and information linkage. The Scenario of a smart home is discussed to show the applicability of the proposed architecture. The various application areas of IoT are discussed. With all these unprecedented applications and advantages of IoT technology, a large section of society is still reluctant to completely depend on such computing technology [4]. In earlier times, technological mistakes had chances for rolling back and rectification without causing much damage to the stakeholders because of the limited scope. But today, with such rapid technological advancements and widespread scope and dependencies, even a small mistake can prove to be devastating and can cause serious harm to the systems and the consumers. The users need to understand the risks associated with such technologies. Achieving security between multiple devices connected to an IoT ecosystem is a challenging task as different devices may have different communication standards, protocols and constraints. It should be the duty of the IoT solution providers to sensitize the stakeholders about the advantages, applications and the risks associated with such advanced technologies, only then we can think about realizing a true sustainable computing environment.

This chapter is an attempt to highlight the data management in IoT domain and the related challenges and provide a solution to the security issues of an IoT ecosystem by introducing the concept of wrapper layer and encryption of the data

captured by the individual IoT devices. The proposed architecture is an initial step towards addressing the issues related to the IoT data management and information linkage. In future researches needs to be directed towards catering the issues of IoT data management focusing on the various challenges faced by the IoT ecosystem and the security aspects of adopting the IoT model.

References

1. Ashton, K.: That 'Internet of Things' thing. RFID J. **22**(7), 97–114 (2009)
2. Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S.: Vision and challenges for realising the Internet of Things. Cluster of european research projects on the Internet of Things. Eur. Comm. **3**(3), 34–36 (2010)
3. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
4. Madaan, N., Ahad, M.A., Sastry, S.M.: Data integration in IoT ecosystem: information linkage as a privacy threat. Comput. Law Secur. Rev. **34**(1), 125–133 (2018)
5. https://www.computer.org/web/sensing-iot/content?g=53926943&type=article&urlTitle=what-are-the-components-of-iot-
6. Congizant 20–20 Insight: https://www.cognizant.com/InsightsWhitepapers/the-internet-of-things-qa-unleashed-codex1233.pdf (2015)
7. https://www.cse.wustl.edu/∼jain/cse570–15/ftp/iot_prot/
8. Bull, P., Austin, R., Popov, E., Sharma, M., Watson, R.: Flow based security for IoT devices using an SDN gateway. In: IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 157–163 (2016)
9. Rahman, R.A., Shah, B.: Security analysis of IoT protocols: a focus in CoAP. In: IEEE 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), pp. 1–7 (2016)
10. Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A. R., Tarkoma, S.: IoT sentinel: automated device-type identification for security enforcement in IoT. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pp. 2177–2184 (2017)
11. Stergiou, C., Psannis, K.E., Kim, B.G., Gupta, B.: Secure integration of IoT and cloud computing. Future Gener. Comput. Syst. **78**, 964–975 (2018)
12. Dorri, A., Kanhere, S.S., Jurdak, R.: (2017) Towards an optimized blockchain for IoT. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, pp. 173–178
13. Alrawais, A., Alhothaily, A., Hu, C., Cheng, X.: Fog computing for the internet of things: security and privacy issues. IEEE Internet Comput. **21**(2), 34–42 (2017)
14. Ammar, M., Russello, G., Crispo, B.: Internet of Things: a survey on the security of IoT frameworks. J. Inf. Secur. Appl. **38**, 8–27 (2018)
15. Song, T., Li, R., Mei, B., Yu, J., Xing, X., Cheng, X.: A privacy preserving communication protocol for IoT applications in smart homes. IEEE Internet Things J. **4**(6), 1844–1852 (2017)
16. Nizzi, F., Pecorella, T., Esposito, F., Pierucci, L., Fantacci, R.: IoT security via address shuffling: the easy way. IEEE Internet Things J. (2019)
17. Xiao, L., Wan, X., Lu, X., Zhang, Y., Wu, D.: IoT security techniques based on machine learning: how do IoT devices use AI to enhance security? IEEE Signal Process. Mag. **35**(5), 41–49 (2018)
18. Hsu, R.H., Lee, J., Quek, T.Q., Chen, J.C.: Reconfigurable security: edge-computing-based framework for IoT. IEEE Netw. **32**(5), 92–99 (2018)
19. Wang, Z., Dong, X., Li, Y., Fang, L., Chen, P.: IoT security model and performance evaluation: a blockchain approach. In: 2018 International Conference on Network Infrastructure and Digital Content (IC-NIDC), pp. 260–264 (2018)

20. Karthikeyan, S., Patan, R., Balamurugan, B. (2019). Enhancement of security in the Internet of Things (IoT) by using X. 509 authentication mechanism. In: Recent Trends in Communication, Computing, and Electronics, pp. 217–225. Springer, Singapore
21. Sheng, Z., Mahapatra, C., Zhu, C., Leung, V.C.: Recent advances in industrial wireless sensor networks toward efficient management in IoT. IEEE Access **3**, 622–637 (2015)
22. Lee, I., Lee, K.: The Internet of Things (IoT): applications, investments, and challenges for enterprises. Bus. Horiz. **58**(4), 431–440 (2015)
23. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
24. Jia, X., Feng, Q., Fan, T., Lei, Q.: RFID technology and its applications in Internet of Things (IoT). In: 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet) (2012)
25. Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I.A.T., Siddiqa, A., Yaqoob, I.: Big IoT data analytics: architecture, opportunities, and open research challenges. IEEE Access **5**, 5247–5261 (2017)
26. Kelly, S.D.T., Suryadevara, N.K., Mukhopadhyay, S.C.: Towards the implementation of IoT for environmental condition monitoring in homes. IEEE Sens. J. **13**(10), 3846–3853 (2013)
27. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I.: Internet of Things (IoT) security: current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (2015)
28. Jaradat, M., Jarrah, M., Bousselham, A., Jararweh, Y., Al-Ayyoub, M.: The internet of energy: smart sensor networks and big data management for smart grid. Proc. Comput. Sci. **56**, 592–597 (2015)
29. Tao, F., Zuo, Y., Da Li, X., Zhang, L.: IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing. IEEE Trans. Ind. Inf. **10**(2), 1547–1557 (2014)
30. Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., Liu, W.: Study and application on the architecture and key technologies for IOT. In: 2011 International Conference on Multimedia Technology (2011)
31. Xu, B., Da Xu, L., Cai, H., Xie, C., Hu, J., Bu, F.: Ubiquitous data accessing method in IoT-based information system for emergency medical services. IEEE Trans. Ind. Inf. **10**(2), 1578–1586 (2014)
32. Bohli, J.M., Skarmeta, A., Moreno, M.V., García, D., Langendörfer, P.: SMARTIE project: secure IoT data management for smart cities. In: 2015 International Conference on Recent Advances in Internet of Things (RIoT), pp. 1–6 (2015)
33. Li, T., Liu, Y., Tian, Y., Shen, S., Mao, W.: A storage solution for massive IoT data based on nosql. In: 2012 IEEE International Conference on Green Computing and Communications, pp. 50–57 (2012)
34. Ma, M., Wang, P., Chu, C.H.: Data management for internet of things: challenges, approaches and opportunities. In: 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, pp. 1144–1151 (2013)
35. Mishra, N., Lin, C.C., Chang, H.T.: A cognitive adopted framework for IoT big-data management and knowledge discovery prospective. Int. J. Distrib. Sens. Netw. **11**(10), 718390 (2015)
36. https://iot-analytics.com/top-10-iot-project-application-areas-q3–2016/
37. https://www.intel.com/content/www/us/en/internet-of-things/solution-briefs/iot-siemens-smart-parking-brief.html
38. http://smartdublin.ie/smartstories/smart-bins/
39. https://atos.net/content/dam/global/your-business/atos-ph-eindhoven-case-study-lowres.pdf
40. https://placeexploration.com/2015/10/28/a-house-is-a-machine-for-living-in/
41. https://www.cnet.com/news/zuckerberg-shows-off-jarvis-his-smart-home-ai/
42. https://www.ge.com/digital/iiot-platform

43. https://www.usnews.com/news/energy/slideshows/10-cities-adopting-smart-grid-technology/2
44. https://www.powermag.com/boulder-to-be-first-smart-grid-city/
45. Abu-Elkheir, M., Hayajneh, M., Ali, N.: Data management for the internet of things: design primitives and solution. Sensors **13**(11), 15582–15612 (2013)
46. Ma, Y., Rao, J., Hu, W., Meng, X., Han, X., Zhang, Y., Chai, Y., Liu, C.: An efficient index for massive IOT data in cloud environment. In: Proceedings of the 21st ACM International Conference on Information and Knowledge Management, pp. 2129–2133 (2012)
47. Shafagh, H., Burkhalter, L., Hithnawi, A., Duquennoy, S.: Towards blockchain-based auditable storage and sharing of IoT data. In: Proceedings of the 2017 on Cloud Computing Security Workshop, pp. 45–50. ACM (2017)
48. Ahad, M.A., Biswas, R.: Request-based, secured and energy-efficient (RBSEE) architecture for handling IoT big data. J. Inf. Sci. https://doi.org/10.1177/0165551518787699

Part VI
Security and Privacy Issues in IoT

Chapter 19
IoT Security: A Comprehensive View

Sumit Singh Dhanda, Brahmjit Singh and Poonam Jindal

Abstract With the advent of the Internet of Things (IoT), security has become a big concern as the size of the internet has engulfed all of the earth. IoT has given the internet the way and means to act which make the security scenario all the more difficult. Security has been the main concern in any network. Size of the network has a direct relation with the probability of a security breach. With the advent of the Internet of Things (IoT) era, the size of the network has extended beyond all the limits that have ever existed. It has spread all over the world. Perception layer that is the lowermost layer in IoT architecture is characterized by wireless sensor networks (WSN) and resource-constrained embedded devices. These devices are fairly limited in terms of memory, computation, power, and energy. It makes them vulnerable to a large number of attacks. Information security is of utmost importance as IoT systems automate critical applications such as traffic control etc. A number of solutions have been provided by the engineers and researchers such as blockchains, Intrusion detection systems, Lightweight cryptography, and various protocols, etc.

Keywords IoT · Blockchain · Lightweight cryptography · Intruder detection systems

S. S. Dhanda (✉) · B. Singh · P. Jindal
Department of Electronics & Communication Engineering,
National Institute of Technology, Kurukshetra, Haryana 136119, India
e-mail: dhandasumit@gmail.com

B. Singh
e-mail: brahmjit.s@gmail.com

P. Jindal
e-mail: poonamjindal81@nitkkr.ac.in

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_19

19.1 Introduction

The vision that was proposed by Kevin Aston in 1999 have been realized today in the form of the Internet of Things and it will soon engulf the entire planet. As a result, the number of connected objects will soon be enormous e.g. 50 billion in 2020 [1]. As per Chen et al. [2] in 2014 there were at least 9 billion interconnected devices in China alone, the number will touch the 24 billion in 2020. Cisco IBSG considers it as that point of time when connected objects will surpass the number of people. In 2003 the people living on the earth were 6.3 billion while the number of devices that were connected to the internet was 500 million. CISCO IBSG predicted in its report in 2011 that in the year 2015 the number of connected devices will increase from 25 billion to 50 billion in 2020 [3, 4]. The Internet of things paradigm benefits all daily life aspects by connecting any device at any place that too any time.

In the Internet, security has always been the prime concern of the network designers and research. IoT is being used for providing the important services in our day to day life such as intelligent buildings, intelligent transportation system, etc. apart from this any application under cyber-physical systems e.g. nuclear power plants, etc. also come under the same umbrella. These applications are very critical in nature. Any compromise of information or network can prove to be life-threatening. Moreover, the resource constraint nature of the devices makes them vulnerable to many security threats. These devices cannot be secured by the old methods of network security as it can affect the lifetime of the network negatively. This also makes these devices a potential vulnerability for the entire network. Mainly there is the following concern in any network regarding security, privacy, confidentiality, integrity, availability.

A systems robustness depends upon the choice of design. IoT system design depends upon the type of architecture it chooses. A lot of have been directed towards standardizing the architecture of IoT. IoT architecture is comprised of a number of layers and a five-layer architecture best describes it. IoT security has been the main factor that has been listed in each of the architecture that has been purposed by various agencies. IoT-A and IoT-RA, RAMI 4.0 etc. [5–12] are the reference architecture given by various bodies.

Intruder detection systems (IDS) and intrusion prevention systems (IPS) are being used now a days to prevent any unauthorized access to a system [13]. It address the issue of authorized access control in security. IPS using honeypots are a technology to thwart such type of attacks by malicious users.

Another technology that has been considered for the trusted transactions in the IoT systems is blockchain [14]. It provides a secure transaction between two parties which is verified by multiple parties on a network. It also provides a secure storage capacity for the data.

All of these technologies and solutions have been used in the society. But all these have one thing in common that is cryptography. With the IoT at the helm most of the connected devices are resource constraint. These devices can not use the typical old cryptographic primitives as they consume lots of power, memory and

computational resources, use of lightweight cryptographic technique on one hand can help these devices achieve confidentiality, integrity on the other it can also help in the easy and fast implementation of other security solutions. A number of problems and their solutions have been described by the researchers. We will discuss all the issues related to it in details but intruder detection systems, lightweight cryptographic primitives, RPL are a few to name.

In this chapter, security requirements for IoT and available solutions are discussed. Section 19.2 discusses IoT architecture and elaborates how it affects security requirements. Security threats have been presented in Sect. 19.3. Section 19.4 provides a brief detailing about the solutions and products available for IoT security. In Sect. 19.5, intrusion detection systems and its types are discussed. Section 19.6 explores the use of Blockchains for the security of IoT systems. Section 19.7 presents the use of lightweight cryptography for IoT security. Finally, the conclusion is presented in Sect. 19.8.

19.2 IoT Architecture

The architecture provides the framework around which the whole system for an IoT application is constructed. It tells an engineer what components need to be included. The architecture draws its structure from the requirements of the application. It means that two different applications who have different requirements will have different architectures. This is the main reason why we see so many different architectures when we examine the literature. But if examined closely it can be observed that architectures also have inherent similarities. An IoT system will have the same set of elements for the same purpose, the only type of elements will differ based upon the requirement of the application. For example, in a Wireless Sensor Based IoT application a mote needs to transmit the data to a gateway at 100 m. It can also utilize Wi-Fi (802.11) as connecting technology but if the same data must be transferred to a sink located 1500 meters connecting technology should be LoRaWAN or NB-IoT [15]. As earlier there was no Standard architecture for IoT systems, but in the past few years, many efforts have been undertaken in this direction by various organizations. IoT-A reference architecture [5] is one such effort. Table 19.1 provides a summary of such reference architectures. It contains the standard its description and the body who has described/finalized the standard.

The standard/reference architecture provides the outline and final architecture can vary in details as per the application requirements. Just like the Vision of IoT, the architecture has also changed over time. The architecture initially was focused on connecting and Identifying things with the help of RFID and EPC global and tracking the items all over and utilizing the information for Various purposes [16–18] then it changed to connecting the Sensors and actuators to Internet with the help of the Gateways for more dynamic and active applications where the information collected by these sensors was utilized to get a work done in optimized way [19–22]. The development then led to next level Web of Things (WoT) [23, 24] where

Table 19.1 Various available IoT architectures

Name of reference architecture	Body involved	Description
IoT-A [5]	European FP7 Research Project	It contains 5 different models as a building block for architectural reference models namely: Domain Security Communication Information Functional
Industrial Internet Reference Architecture (IIRA) [7]	Industrial Internet Consortium	It is based upon four viewpoints: Business Usage Functional Implementational It has included five types of architectural patterns
Reference Architecture Model Industrie 4.0 (RAMI 4.0) [8]		It is a 3-Dimensional layer model. It has 6 layers in the vertical axis to describe the decomposition of machines, 7 levels of functional hierarchy on the right horizontal axis. While the left horizontal axis represents Life Cycles of Facilities and Products
The standard for an Architectural Framework for the Internet of Things (IoT) [9]	P2413-IEEE work Group 27 Members	Active details need to be finalized. Its goal is to provide an extensible integrated architectural network
Arrowhead Framework [10]	Arrowhead Technology	It has defined five different levels of hierarchy from level 0 to level 4 Its core system has 8 systems in it
Web of Things [11]	W3C	It has a four-layer architecture built upon the Networked Things (not formally documented)
IoT RA [12]	ISO	

the participants of the IoT system can connect to Web on their own has this type of architecture has its own different requirements. The decision-making is complex and cumbersome. More resources are required to manage such a number of devices. The first function is to identify the Physical Devices and provide them an address so that these devices can be connected to the Internet. Once the identification and addressing of the devices are completed, the transfer of the information is easily achieved. Next, important work is to manage a large amount of data provided by these devices for decision making it would require data fusion from numerous devices, knowledge abstraction from the data and their semantic representation; this varies from system to system. Once the data has been processed, this refined form needs to be passed to Customers or persons accessing the IoT for various purposes

through various applications. The communicated information can be utilized efficiently if the Physical devices with unique addressing and identification are converted to unique Virtual Entities. Managing Virtual Entities is also important. Finally, when the actuation is performed or the process is completed analytical evaluation needs to be carried out for further.

The Architecture must be able to address all the above-said issues separately and it must also envisage the following essential characteristics:

(a) It must have a comprehensive perception means it should be able to include all type of physical devices whether they are sensors, actuators, smart devices or the smart objects, into the system by uniquely identifying them.
(b) It should be able to provide reliable transmission of the information from the sensors to the Server/Cloud so that information required for the decision making must remain reliable accurate and secure.
(c) The final characteristics of the architecture are its capability to process the acquired data intelligently so that the decision making is robust it must be able to extract information reliably and in the right context from available data.

Heterogeneity of devices and not having a standard architecture does pose a difficult challenge of interoperability for IoT systems. To address the issue of Interoperability issues the architecture can employ the Software Defined Networking (SDN) and NFV (Network Function Virtualization) approach.

Many papers refer to a 3-layered architecture for IoT while many refer to 5 layered IoT as well. A few go for 7 layered IoT architecture like OSiRM [25] depending upon the requirements for the application as well as the security features they have installed. 3-layered architecture mainly refers to the following three layers:

(a) Perception Layer
(b) Network Layer
(c) Application Layer.

These layers have different functionalities as can be understood by their names. Perception layer mainly includes the sensors actuators, Smart objects, Smart thing, etc. While the Network layer addresses the issues from communicating the data to the server and all data processing related activities. Application layer addresses the issues related to decision making and the provision of services. But three-layered architecture is not sufficient to address the issues related to IoT. On the other hand, 5-layered architecture is more suited to the requirements of IoT. Inclusion of these two additional layers, apart from the other three, provides the options to address the issues of cloud computing, big data processing, and middleware. It also helps in addressing the issues of heterogeneity, interoperability. Any other architecture with more layers will add more functionalities to the system. As is the case in the following works. Main factors that will help characterize/differentiate the architecture apart from the number of layers are SoA etc.

In Ren et al. [26] also provides a three-layer architecture for QoS of IoT, here they divide functions of application and perception layers in two sub-layers each. While on application and service layer has two functions provided by service sublayer and on its application sublayer. Perception sublayer has sensors, actuators, etc. on base and they also require gateway functions which is the second part. The network layer is mainly responsible for the transmission of information and its processing.

IoT reference Architecture talks about five layers bottom one sensors/actuators, on top of it devices which are connected through Gateways, from gateway information is passed to the IoT middleware from there it reaches application layer.

Interoperability of various products is one key issue that will act as a major factor in the exponential growth of IoT. IoT-A is one such step towards creating a common architecture of IoT that will make the growth of IoT faster. The main problem with the solutions that are currently available is scalability in terms of communication and device management.

19.3 Security Threats

Mario Frustaci et al. [27] in their work has provided a comprehensive view of the IoT security and related problems. It elaborates the problems in a three-layer IoT architecture. It has assumed that the layers in consideration are perception layer, transportation layer, and the application layer. The attacks that are very prominent on the perception layer are physical attacks, routing attacks, denial of service (DoS) attacks, impersonation attacks, and data transit attacks. In the case of transportation layer the attacks that are important routing, DoS and data transit. At the application layer, data leakage, DoS attacks, and malicious code injection are important attacks.

Based on the analysis of various papers it can be stated that a number of security issues are faced by different layers of IoT. Table 19.1 tabulates the issues pertaining to the respective layer. As can be seen that the issues related to the perception layer are associated with hardware security, physical security, and DDoS attacks. On the transportation layer, the issues are lack of lightweight cryptographic algorithms, lightweight trust management system and lack of secure routing platform, etc. The application layer is suffered by user privacy and application vulnerabilities (Fig. 19.1).

The following key issues require the attention of the researchers.

i. Perception layer is at very high risk. Enormous devices installed in the open and hostile environment creates a big challenge for the physical security of the device. Hardware security is an important issue which can be attributed to the negligence of the manufacturer of the device.

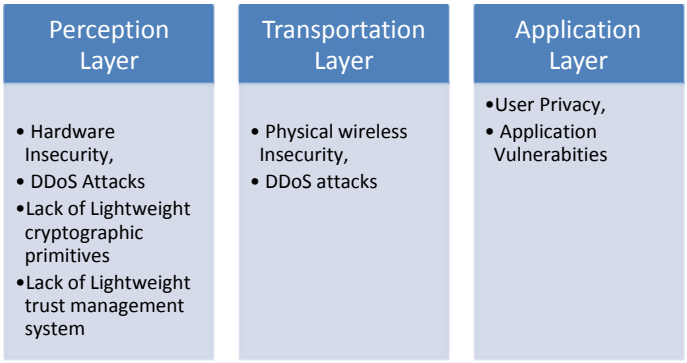


Fig. 19.1 Issues pertaining to different layers

ii. Lack of lightweight cryptographic primitives and effective key management for the integrity and confidentiality of the data in IoT.
iii. Trust management system is quite heavy and its requirement is of utmost importance due to the open deployment of devices. Moreover, the nature of data most of the time is personal in nature which makes it all the more important to find a lightweight trust management system.
iv. Wireless sensor network forms the perception layer and they face strong routing threats. So secure and lightweight routing protocols are another big requirement of the physical layer.
v. The transport layer is comparatively better in terms of security but the most critical issue is the vulnerability of wireless channel which can be an easy target for data transit attacks.
vi. Complexity and heterogeneity of IoT make it vulnerable to DDoS attacks.

Many solutions already exist but a lot of efforts are needed in this direction.

If one looks at the perspective of attacks, these attacks result in two types of results one data disclosure and two, denial of service. Data disclosure relates to the privacy aspect while denial of service relates to the availability aspect of security. Table 19.2 shows the details of attacks that can result in data disclosure and denial of service. The problem of data disclosure can further lead to denial o service or network breach affecting the availability of the services to the customer. Hence it is of the utmost importance for the designer to provide a solution to the network, Wireless channel is a challenging media in which eavesdropping is easier but with the help of cryptography/encryption one can ensure the confidentiality of the information.

Table 19.2 Attacks and related issues in IoT [27]

Issue	Attacks
Data disclosure	• Network sniffing • Device cloning • Side channel attacks • Cryptographic attacks
Denial of service	• Device Jamming • Device cloning • Battery exhaustion • Routing attacks

19.4 Existing Solutions and Products

In this section, solutions and products that exist are discussed layer-wise. Figure 19.2 shows the available solutions and protocols available for the various layers of the IoT.

In this figure, the protocols used by various layers have been shown.

IEEE 802.15.4 is the base for the ZigBee. In this, the security provision is provided at the MAC layer. There is no security available for ACK packets. There are four types of security provided in this standard.

i. No security
ii. Only Encryption using AES-CTR
iii. Only Authentication using AES-CBC-MAC
iv. Authentication with encryption using AES-CCM.

Three types of keys is defined for the key management process namely master key, network key and link key. To avoid node tampering it is must to secure the master key physically.

BLE stands for the Bluetooth Low-Energy and its 4.2 version uses elliptic curve Diffie-Hellman public key cryptography to provide robust and low energy security. It also provides replay protection. At the link layer, it uses AES-CCM to provide confidentiality and integrity. Due to its fix authentication mechanism, BLE is highly vulnerable [28].

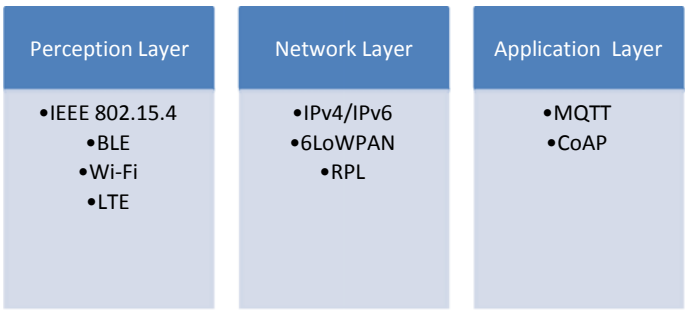


Fig. 19.2 Protocols in different layers

Table 19.3 A brief comparison between WPA and WPA2

	WPA	WPA2
Encryption algorithm	Temporal Key Integrity Protocol	CCMP (AES based)
Authentication mechanism	Same	Same
Algorithm	Michael algorithm	CBC-MAC
Network throughput	Reduced	Comparatively less reduction than WPA

WiFi (IEEE 802.11). For the authentication as well as encryption this standard utilizes WPA/WPA2 protocols with WEP. AES cipher is used to in WPA2. A small comparison is drawn between these two in Table 19.3.

LTE (Long Term Evolution) utilizes two sets of algorithms for integrity and confidentiality. First set is based on SNOW 3G stream cipher and has two algorithms namely 128-EEA1 and 128-EIA1 while the second set is based on AES block cipher with two algorithms, 128-EEA2 and 128-EIA2. Here EEA stands for EPS encryption algorithm and EIA stands for EPS integrity algorithm [27].

IPv6 has been the main invention which has helped the realization of the IoT as it has provided the unique addressing for each thing on earth with the 128-bit address. It utilizes the end to end encryption. IPsec protocol is responsible for the confidentiality, authentication, and integrity at the network layer. It utilizes cryptographically generated address in neighbor discovery messages [29].

6LoWPAN [30] is a protocol that adapts the internet protocol for resource-constrained devices. It does so by compressing the headers and using cross-layer optimization of IPv6. It uses compressed DTLS, compressed IPsec and security features of IEEE 802.15.4 to provide end to end security and link layer security respectively [29, 30].

RPL is the routing protocol for IoT devices and it supports unidirectional and bidirectional traffic by ranking the nodes in the network. It has three modes of operation for security named ‘unsecured’, ‘preinstalled’ and authenticated. The authenticated mode is used by routers and this process uses cryptography. RPL is short form for the routing protocol for low power and lossy networks. It was developed by the IETF and it is based on the IPv6. Its most important feature is link independence. It uses destination oriented directed acyclic graph (DODAG) which stores the information of minimum one parent node or root node. Every node in RPL knows about its previous node but not the next one. To provide faster routing operation RPL has at least one path for the root node. RPL works in two modes. In the first one it utilizes the IP addresses of the nodes and message moves in lower direction in hierarchy. This mode is known as non storing mode. In storing mode, same operation is based on IPv6.

At the application layer, two important protocols are constrained application protocol (CoAP) and message queuing and telemetry transport (MQTT).

CoAP uses the UDP protocol. DTLS and IPsec are used to achieve encryption. AES-CCM is used for different security aspects. No security, pre-shared key, raw public key, and certificates are four security modes in CoAP. There is a number of issues with the CoAP which may be summarized as follows:

i. The heavy cost of computation
ii. Key management
iii. High handshake
iv. Energy consumption.

MQTT provides transport encryption using TLS/SSL. It is the main issue with MQTT as well because it is not adapted for the constrained devices. It is also not a good option due to the heterogeneous nature of IoT devices. Hence the main issues with MQTT are scalability, lightweight and robustness.

TLS, transport layer security, is a protocol based on cryptography to provide data integrity and privacy for the communication services. It uses symmetric cryptography. It also supports authentication. DTLS stands for datagram transport layer security, it is mainly responsible for the confidentiality and integrity of the datagrams. It is based on the TLS protocol. It provides application tolerance against the delays, size and order mismatch by use of UDP.

19.5 Intruder Detection System in IoT

Origin of the Intruder detection systems (IDS) can be traced back to 1980s. Its concept was presented by James Anderson in his paper "Computer Security Threat Monitoring and Surveillance". After this Dorothy Dennig implemented IDS in collaboration with Dept. of Navy in the USA. IDS evolution has gone through the two generations. The first generation was of such Intruder detection systems which were able to identify between insider and outsider; hence it was able to distinguish between misuser and intruder. These were termed as detective systems as they can only alarm about the incident. The second generation was termed as preventive systems as they were able to prevent such an incident apart from detecting it [31–34] (Fig. 19.3).

As can be seen that an intruder detection system can be broadly classified in two types based upon:

(a) Place of detection
(b) Approach of detection.

The first category which is classified on the place of detection is further sub-divided into two types as host based intruder detection system and network based intruder detection system. On the other hand, based on what approach has been used to detect intruder the classification has three categories namely, signature based detection, anomaly based detection, and reputation based detection.

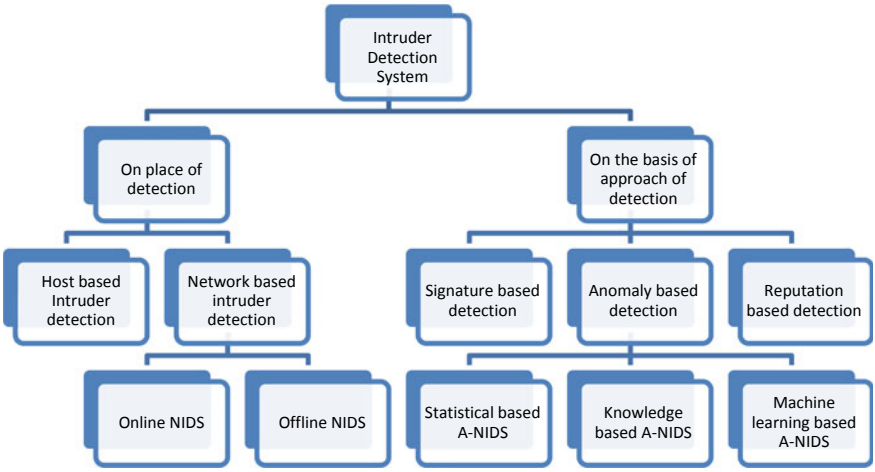


Fig. 19.3 Types of intruder detection systems

The basic process in an IDS can be divided into two types of work first to 'inspect' and second to 'identify activity' in the network.

IDS is of two types

i. Network-based intruder detection system (NIDS)
ii. Host-based Intrusion detection system (HIDS).

Components of IDS are network sensors, central monitoring system, report analysis, database and storage components, and response box.

NIDS is used to examine traffic on the network it does so by keeping the network interface card on promiscuous mode. By doing so NIC accepts all the data. SNORT, CiscoIDS, Symantec Netprowler are a few examples of the NIDS. In NIDS the sensors are placed at strategic locations. So that it can detect maximum activity. Its main aim is to monitor the traffic inside the network. After capturing the traffic it analyses and then match it with the available database of the attacks hence the attack can be identified. On registering the abnormal behavior the alert can be sounded. It can be further subdivided into two types based on the systems' inter-activity into online and offline NIDS. The online mode is also termed as inline mode and provides the real time monitoring. The offline mode is called as tap mode. Processor performance is the most important factor that affect the performance of an IDS. Deep pipelines in processor negatively affects the system performance. NIDS has its advantages and disadvantages as follows:

i. It can support many sensors which improve the monitoring capabilities.
ii. It has blindspots e.g. if the intruder is on host terminal it cannot detect.
iii. It cannot decrypt encrypted data.
iv. It is not able to identify the type of attack and its effectiveness.

HIDS are used to monitor the data on a particular system. Monitoring of inbound and outbound data is its responsibility. It compares the events and searches for problematic events. It looks and verifies the state of the system. It can scan and track the movement of an attacker and alert the administrator. The main disadvantage of using a HIDS is that as compared to NIDS its degree of susceptibility to illegal tampering is higher. It also has a limited view of the network.

On the other hand, it is able to see the local activities in the network. The response of the HIDS is near real time and it is very quick to verify.

Second major classification of the intruder detection system is based on the detection method. It can be divided into three types:

(a) Signature based intruder detection system (SIDS)
(b) Anomaly based intruder detection system (ANIDS)
(c) Reputation based intruder detection system (RIDS).

In signature based method, detection is performed by comparing the current attack with the exiting specific patterns. This approach is mainly inspired by the antivirus. These patterns are called signatures. Normally byte sequences are used as signatures. In Fig. 19.4 the process of the scheme is shown. In this approach, major limitation is that new attacks can not be detected hence time to time updation is required. This weakness of non-detection of new attack was removed by anomaly based IDS. The second type is anomaly based intruder detection system. It can also help detect the unknown attacks. It mainly utilizes machine learning techniques. For this purpose the first step is to create 'a model to define a trustworthy activity'. This is used to compare the inbound behavior. The main advantage lies in its quality of being trained which helps it to perform better and detect unknown attacks. But it also create some limitations for the system as the process become time consuming; false positives increases and performance degrades.

ANIDS has three subtypes. These types are based upon the techniques used for the detection for the deviation in the behavior. The first type utilizes normal statistical techniques to identify the deviation in behavior hence it is called statistical ANIDS. Some ANIDS utilize the prior knowledge for this purpose. These are called knowledge based ANIDS. Expert systems and finite state machine are a few to name. The last type uses machine learning for the same purpose, it can be based on Bayesian networks or fuzzy logic; neural networks or markovian models; clustering and genetic algorithm is also utilized. These techniques are flexible and can be scaled as per requirement. ANIDS is a robust system in comparison to SIDS. But the biggest limitation lies in its high degree of dependency on the assumed model. This model can be univariate or multivariate. Some example are Airdefense guard, NIDES, Next Gen, etc. [35, 36] (Fig. 19.5).

A lot of research has been done in this area, Zarpelão et al. [13] have presented a detailed survey on the intrusion detection for IoT. In this survey authors has categorized the validation strategies for the intruder detection in IoT. Hypothetical, empirical, simulation, theoretical, and none.

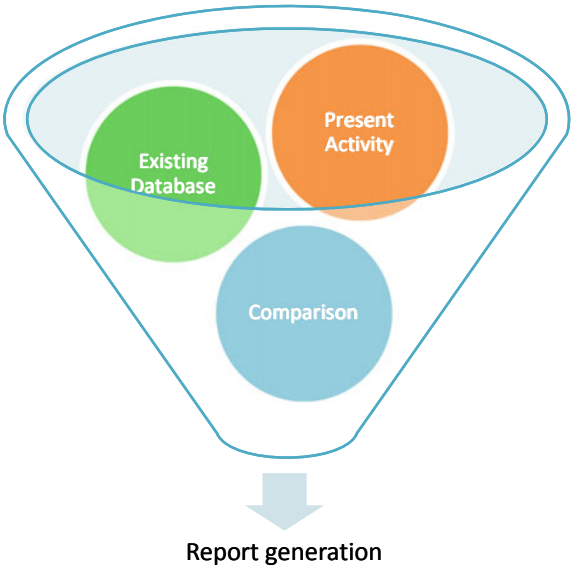


Fig. 19.4 Process for signature based intruder detection system

19.5.1 Intruder Prevention System

The main limitation in the regard of IDS is its inability to prevent the breach. It will only send an alert regarding the breach of security or the attempt of breach. That is not sufficient in the age of IoT where attacker can cause the damage of life and property. Researchers have given next level of security with intruder prevention systems (IPS). These are special type of IDS which not only detect the intruder but also take steps to prevent this intrusion hence called IPS. It is broadly classified into four types as shown in Fig. 19.6.

(a) Network Intruder Prevention System (NIPS)
(b) Wireless Intruder Prevention System (WIPS)
(c) Network Behavior Analysis (NBA)
(d) Host Based Intrusion Prevention System (HIPS).

NIPS is mainly focused on network monitoring. It analyses activity of protocols and then perform the preventive action if needed. WIPS does the same in case of wireless networks and protocols. In network behavior analysis, examination of network is done to identify the threats. Finally, HIPS is concerned with single host's monitoring and analyses. Three type of detection methods come in use in the above said techniques. If the packets are monitored and compared with some known pattern the network then it is known as signature based method. In statistical anomaly based method network and protocols are observed and compared with some predefined baseline. Last method is called stateful protocol analysis in which identification and comparison of events, that are observed in the network, is carried out with profiles that have been established as malicious.

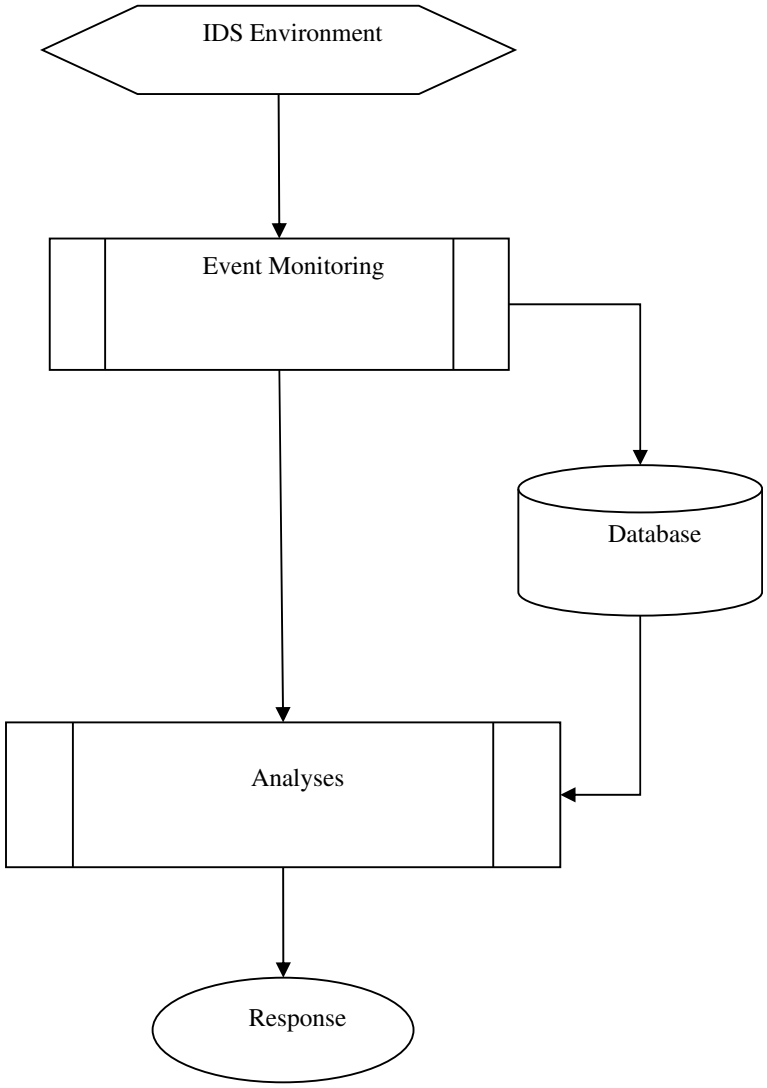


Fig. 19.5 AnIDS

19.6 Blockchains for IoT

Blockchain is a technology that works in peer to peer mode and used for the storing and sharing of information. It utilizes public key cryptography and data structures for keeping records of transactions. Its main role is to provide trust in a transaction and that is why some researchers call it the missing trust layer of the internet (Fig. 19.7; Table 19.4).

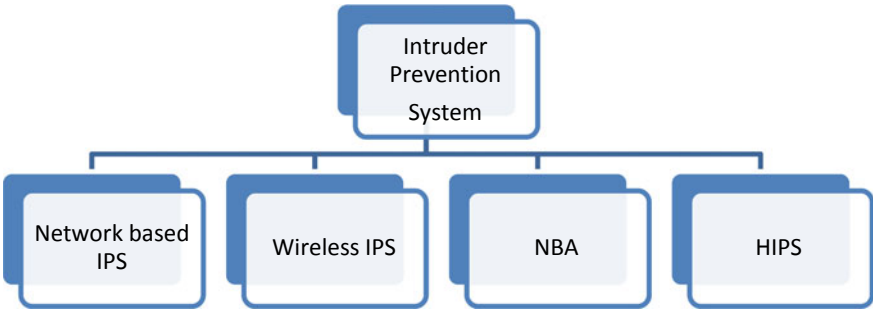


Fig. 19.6 Types of intrusion prevention system

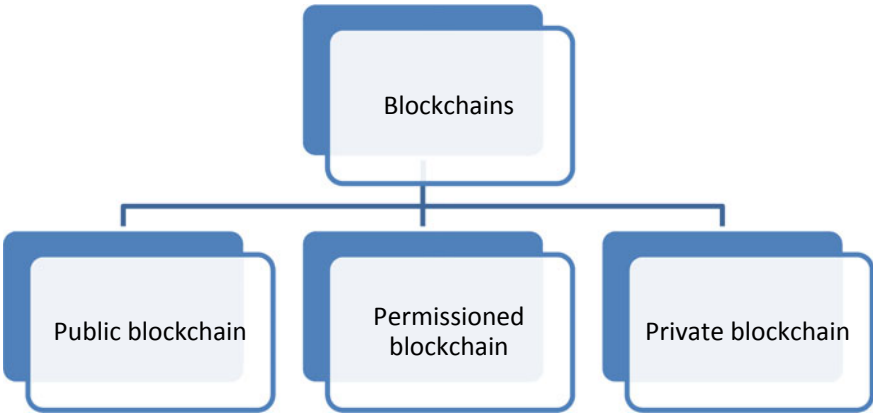


Fig. 19.7 Blockchain and its types

There are three type of block chains namely public blockchain, permissioned blockchains, and private blockchains. One can differentiate these three on the basis of the type of membership, participation, role play, level, the confidentiality of source code, and size of the blockchain, etc. Some other important parameters are security, speed of operation and use of cryptocurrency. Table 19.5 gives a complete comparison of these three types on the basis of the above-said parameters. A blockchain may be categorized into the above three categories even though the blockchains from the same category will vary in working and validation process.

There are three main blocks in the structure of blockchain namely:

(a) Block
(b) Chain
(c) Network.

Blocks are different from each other in different blockchains. They get differentiated from each other on the basis of a list of transaction triggering of events, size

Table 19.4 Process for the blockchain generation [37]

Step	Action
1	Request for transaction/creation of block
2	Request for transmission over the network
3	Broadcast over the network
4	Validation by the node in the network
5	Broadcast of response back from the network
6	Block added to the existed blockchain

Table 19.5 Comparison between different types of blockchains [38–49]

Public blockchain	Permissioned blockchain	Private blockchain
Largely distributed networks	Large and distributed network	Smaller in size
Uses token	Uses token	No token??
Open participation	Controlled role play	Membership is controlled
Open source code	Source code may or may not be open	Trusted members only
More secure and immutable	Easier to scale project and transaction volume	Low cost to run and low time to build
Slower and more expansive to use	Can be fast with low latency	Very fast or no latency
Limited storage capacity	Higher storage capacity	–
Secured with cryptocurrency	Many utilize cryptocurrency	No use of cryptocurrency

and time period, etc. Recording of an event in the block is called a transaction. Values are assigned to a transaction for interpretation purpose.

The chain is a comparatively difficult concept to understand it helps in connecting the blockchains and builds trust among them. Hash is used to connecting or chain blockchains together. It is used to lock the blocks. It can be considered fingerprint of data.

The network consists of computers that run the blockchain protocol called 'software' to secure the network. These computers are called full nodes. So, one can also imagine the network to be an interconnection of these full nodes. The transactions are recorded in these nodes and in lieu of this nodes are rewarded by software [38–49].

Blockchains works on the expectation of threat (EoT). They use proof of work as a consensus model and solves a Byzantine general problem for this. Blockchains have evolved over time. It can be seen in Fig. 19.8 example for the first type of blockchain is Bitcoin which is a globally distributed blockchain with 5000 full nodes. The second type of blockchain is Ethereum, it utilizes traditional blockchain network with a programming language. It has less than 5000 nodes but distribution

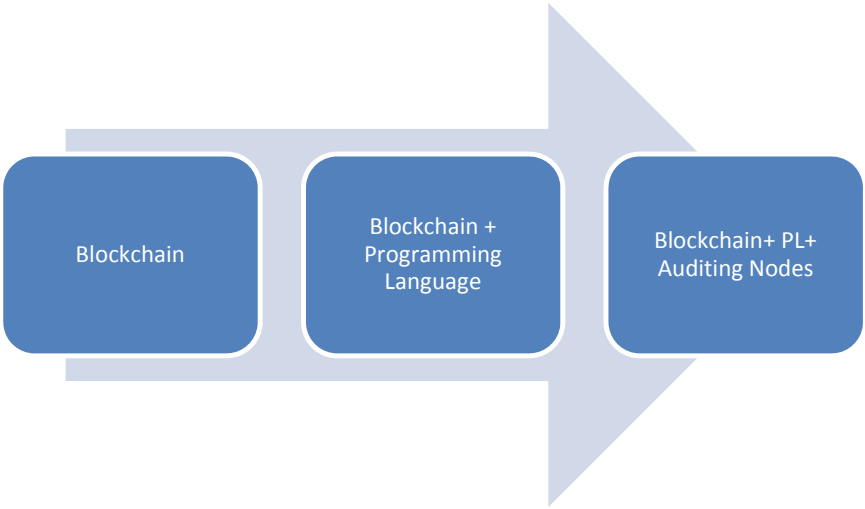


Fig. 19.8 Evolution of blockchains [38–49]

is global. It trades ether and used for creating smart contracts and decentralized autonomous organizations. Example for the final type of blockchain is factum network which makes use of auditing nodes in addition to the second type of blockchain. It helps in small size secure data system.

Application and uses of blockchains are the following:

i. Stock trading
ii. Money transfers
iii. Currency exchange
iv. Part of the software security stack
v. Land record systems
vi. Identity systems
vii. Visa process
viii. Real estate
ix. Insurance etc.

Shared peer to peer technology that actually is a distributed ledger which helps in protecting against alteration and modification. IoT has many problems because of its reliance on centralized cloud services and blockchains may prove to be a solution to all of these.

Every technology has a some advantages and disadvantages which helps in its evaluation. It gives insight to a designer about the scenario where it should or should not be used. One can list the following advantages for the blockchain technology:

i. It helps in building trust in the network i.e. IoT.
ii. It will reduce the overhead costs in the IoT.
iii. It will enable peer to peer communication which will help in the reduction of data exchange as well as processing time.
iv. It will help in the security scalability in IoT.

On the other hand the weaknesses or limitations that blockchain technology faces are:

i. Performance limitation is a big factor for blockchains.
ii. Huge Computational capability is required.
iii. Energy costs associated with it are very high.
iv. Block time corresponds to a long waiting period which is a big concern.
v. Every time a transaction is made it involves a fee which makes it a costly process.

In light of the above factors, it is quite clear that the biggest challenge for adopting blockchains for the IoT is the number of transactions it can process at a time. IoT systems generate a huge number of transactions every second while the processing speed for the Bitcoin is 7 transactions per second which creates a bigger challenge. For time-critical applications also blockchains cannot be utilized in IoT systems. Department of Homeland security is exploring the possibilities and areas of application for blockchains in field of IoT. Romen Beck et al. [37] in their work suggest that blockchains can be used in sharing the IoT datasets which can help in making the predictive security better for IoT. It can also provide for the distributed storage of such huge real-time IoT datasets which are not possible to maintain by a single server.

19.7 Lightweight Cryptography in IoT

Lightweight cryptography is a term coined for cryptographic primitives that consume very small resources in terms of RAM/ ROM memory, code size, power, and energy, etc. These have become so important because the size of devices has become smaller now a day. In the era of IoT, its importance has increased many times as perception layer or the connected devices in IoT are characterized by their small size, limited computational capability, limited memory, etc. which clearly outlines the need of such primitives. Another factor that makes the use of lightweight cryptography so pertinent is the use of wireless communication at the perception layer in IoT. The biggest challenge with wireless communication is maintaining the confidentiality of information. As anybody can eavesdrop it should be ensured that eavesdropper should not be able to comprehend the information. This can be ensured with the use of cryptography. Lightweight cryptography can be utilized at this layer as it is best suited for resource-constrained devices [50, 51].

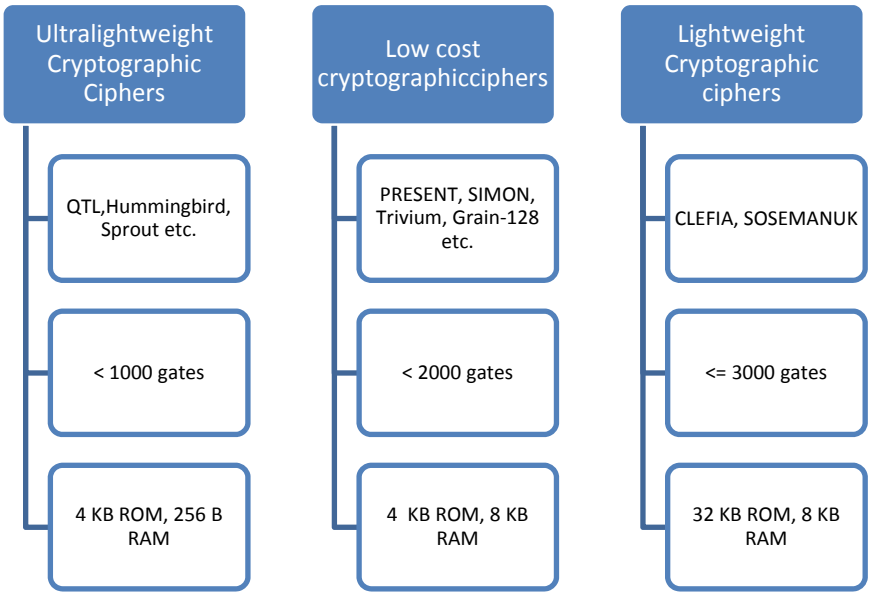


Fig. 19.9 Different categories for lightweight ciphers [52]

Figure 19.9 shows various categories in which a cryptographic primitive can be categorized. As shown, a primitive can be termed as lightweight if the numbers of gates required for the hardware implementation are less than 3000 or memory requirement is 32 KB ROM and 8 KB RAM. For low-cost category, both requirements stand at less than 2000 and 4 KB ROM with 8 KB RAM respectively. In the case of Ultra-lightweight category, gate requirement stands at less than 1000 gate equivalents while memory requirements stand at 4 KB ROM and 256 B of RAM [52, 53].

There are mainly four contenders for the confidentiality and authenticity in IoT namely lightweight stream ciphers, lightweight block ciphers, and lightweight hash functions while in public key cryptography ECC.

Public key cryptography can play a big role in the security of IoT. It can provide confidentiality and authentication. Blockchains utilizes the public key cryptography as well as hash function to generate trust in the transactions. So the role of lightweight cryptographic primitives became more important in this scenario.

There are mainly four options to provide lightweight cryptographic primitives:

i. Lightweight block ciphers
ii. Lightweight stream ciphers
iii. Lightweight hash functions
iv. Elliptic curve cryptography in PKC.

These four primitives have a different role. The biggest advantage with the PKC is that along with confidentiality it also provides authentication. The lightweight hash function ensures the integrity of the data. LBC provides while lightweight stream ciphers can provide low latency on large data. The lifetime of cryptography can be divided into three different generations.

The first generation corresponds to the time period when initial standards for the cryptography were established i.e. the 1980s and 1990s. During this time compact implementations of a cryptographic standard were mean to become lightweight. 2nd generation belongs to the time period from 2005 to 2012. In this period the basic of lightweight cryptography were set and a number of primitives were designed with this in mind. Area reduction was the prime target. The 3rd generation of the cryptography is the present time. It focuses on latency reduction and speed. With the advent of the IoT era, constrained devices have become the main focus and pervasive. The aim of cryptography is now to cater to the requirement of applications and these devices (Fig. 19.10).

The above said four type of primitives are four contenders which are competing for the lightweight option for the IoT security solutions. Most widely used is AES cipher which has been used with different key sizes for different applications. Second type is lightweight stream cipher which has Grain, Trivium, Fruit and Plantlet as it important ciphers. Lightweight hash functions are important for providing integrity of the data. Important lightweight functions are Quark, Photon, Hash-one etc. these belong to symmetric category of the ciphers. Another contender that belongs to asymmetric cipher category is elliptic curve cryptography (ECC). ECC has many variants that are utilized for providing the confidentiality and non

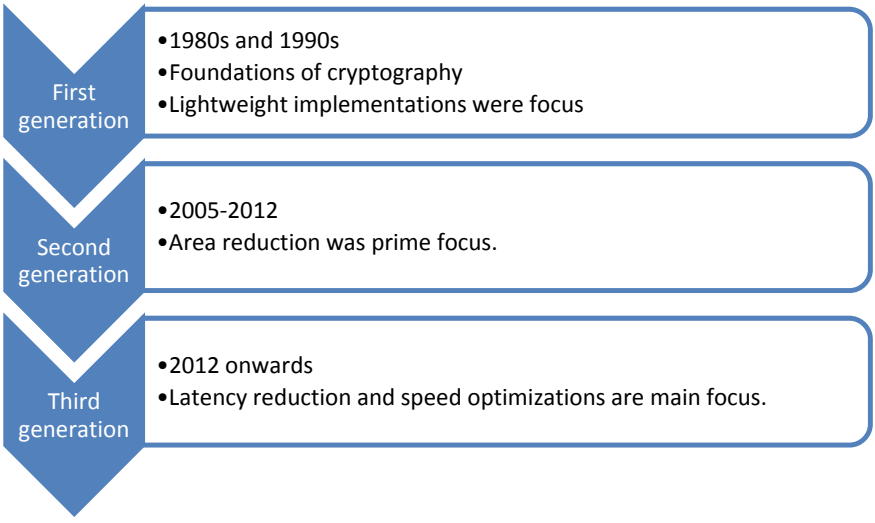


Fig. 19.10 Evolution of lightweight cryptography [51, 52]

Table 19.6 Various lightweight cryptographic primitives and their examples [54–95]

Lightweight stream cipher	Lightweight block ciphers	Lightweight hash functions	Elliptic curve cryptography
Grain; Trivium; Salsa 20/r; Quavium; WG-8; Sprout; Fruit-v2; Plantlet	AES, DESL PRESENT, ITUBEE, SIMON and SPECK; RECTANGLE; Midori; QTL	Quark, Lesamanta-LW, KECCAK, PHOTON, SPONGENT, GLUON, L-Hash, Hash-One, NEEVA	Nano ECC, Micro ECC, Tiny ECC, WM-ECC, Mote-ECC

repudiation. Nano ECC, Micro ECC etc. are a few. Table 19.6 provides the name of important ciphers of these four categories.

The following are the main areas of work for different primitives. As the main area of focus for lightweight block, the cipher is a reduction in block size, key size, simpler rounds, designing simple key schedules. For lightweight stream cipher reduction in chip area, key length, internal state, and reduction in key/IV setup cycles. In case of lightweight hash function reduction in output size, reduction of message size. A strong primitive in public key cryptography is ECC, the main focus of researchers in this is minimizing memory requirements, reducing energy consumption, optimization of pf and group arithmetic/improving speed.

The various factors, as shown in Fig. 19.11, upon which a lightweight cryptographic primitive is evaluated are as follows:

(i) Security is the first and foremost factor that is considered while evaluating a cryptographic primitive. It is the logarithmic of the computational attacks on that cipher. Maximum value for this can be the length of the key.
(ii) Chip area is another metric that decides about the lightweightness of a cipher. It is measured in gate equivalents. It depends upon the technology used for the implementation.
(iii) Throughput which is measured for a particular type of implementation at a fixed frequency should be high for a cipher.
(iv) Latency is a very important metric in the time critical applications where confidentiality is required. It is measured in the number of cycles.
(v) Power and energy consumption is another factor that should be as low as possible. It depends upon the chip area to an extent. A very important metric for the resource constrained devices.
(vi) Efficiencies should be as high as possible for a cipher.

These factors helps in deciding in the selection of an cipher for the particular application. Currently, latency, power and chip area are important metrics that are the focus of the researchers as IoT applications and devices are time critical are resource constrained.

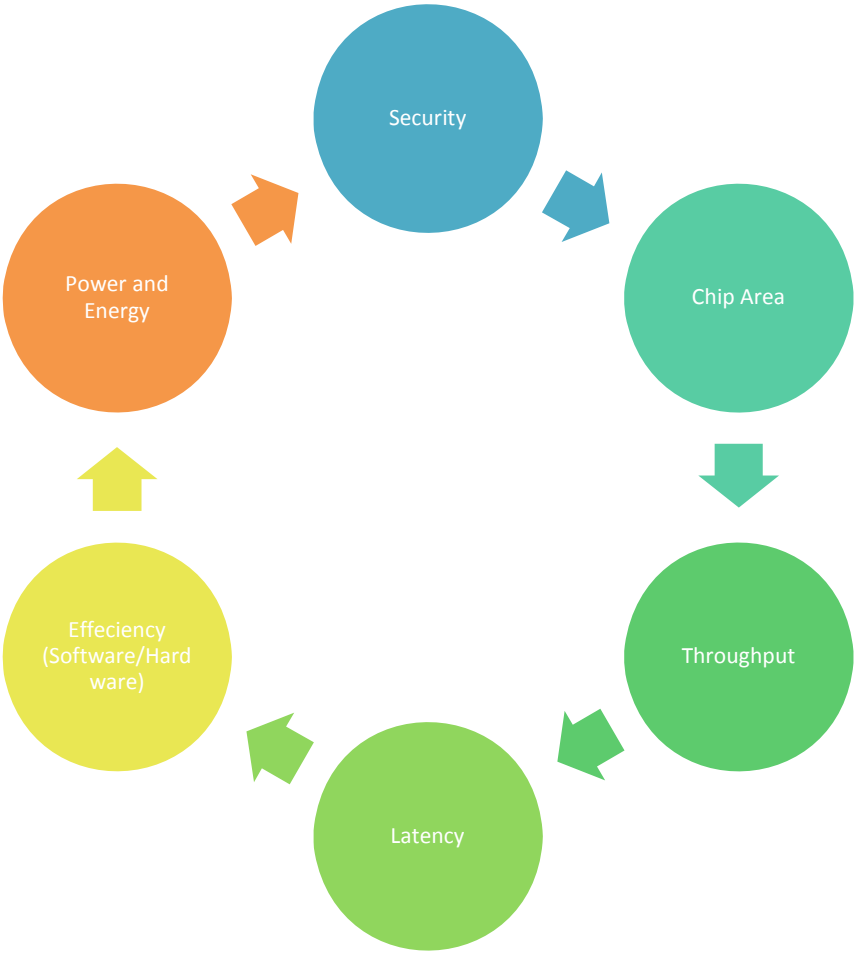


Fig. 19.11 Factors for the evaluation of LWC

19.8 Conclusion

IoT systems are designed with a number of technologies. The architecture of an IoT system may have three to five layers. Most of the literature refers to the three layer architecture. Numerous number of openly deployed connected devices put a lot of challenges on the security aspect of the IoT systems. A large number of challenges face IoT security. Hence a large number of solutions are presented by the researchers. The solutions offered are specific to the layers of architecture of IoT systems. Perception layer is at highest risk. It suffers from hardware insecurity and confidentiality issues. Trust management and denial of service also affects security

at this level. Most of the solution at perception layer has mainly focused on AES-CCM and a few solutions has used ECC as security here is built around the IEEE 802.15.4. It means the lightweight cryptography is key to the security at this level. It became of utmost importance given the resource constrained nature of the devices. At the network layer IPv6 and its compressed version 6LoWPAN along with the RPL are the main choice. These have DTLS and cryptography as the base of the security. At the application layer, CoAP and MQTT are two important protocols utilized in the IoT scenario which again uses DTLS and TLS-SSL for the security purpose. These all existing solutions uses cryptography in them which makes the research in this field.

Another solutions that are used for security are Intruder detection systems and intruder prevention systems these both are an important tool for providing security. Honeypots based IPS are being utilized on a big scale now a days.

Blockchain is another potential technology that can be a a game changer in the field of IoT security. Its potential is explored by the Department of Homeland Security in USA. It can provide an trust based environment. But important thing is that process of blockchain generation is again dependent on the cryptography.

So in a conclusive way one can say the most important area which serves as the base of IoT security is the lightweight cryptography which works on the objectives of reducing the chip area, power consumption and latency reduction. Latency reduction will help in the time reduction in blockchain process. Lightweight cryptography have two type of primitives symmetric and asymmetric. AES is the most widely used cipher in symmetric primitives. In asymmetric cipher, ECC is being used primarily nowadays. These two are contesting for the market. ECC lags behind AES in terms of execution time. Number of ways have been devised by the researchers to speed up the operations. In this way, we can conclude that the lightweight cryptography will be key for securing IoT along with other technologies.

References

1. Atzori, L., et al.: Understanding the Internet of Things: definition, potentials, and societal role of a fast-evolving paradigm. AdHoc Netw. (2017). http://dx.doi.org/10.1016/j.adhoc.2016.12.004
2. Chen, S., et al.: A vision of IoT: applications challenges, and opportunities with China perspective. IEEE Internet Things J. **1**(4) (2014)
3. Evans, D.: The Internet of Things: How the Next Evolution of Internet is Changing Everything. CISCO IBSG (2011)
4. Lopez Research: An Introduction to Internet of Things, Part 1 of IoT Series (2013). Retrieved from: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf
5. Internet-of-Things Architecture (IoT-A), Project Deliverable D1.2—Initial Architectural Reference Model for IoT [Online]. Available at: http://www.IoT-a.eu/public/public-documents/d1.2

6. Introduction to Architectural Reference Model for the Internet of Things. http://www.IoT-a.eu/arm
7. Ind. Internet Consortium, Needham: The industrial Internet reference architecture, version 1.7, MA, USA. Tech. Rep. IIC:PUB:G1:V1.07:PB:20150601, 4 Jun 2015 [Online]. Available at: http://www.iiconsortium.org/IIRA.html
8. Adolphs, P.: RAMI 4.0: An Architectural Model for Industrie 4.0. Plattform Ind. 4.0, Berlin, Germany (2015) [Online]. Available at: www.plattform-i40.de/http://www.omg.org/news/meetings/tc/berlin-15/special-events/mfg-presentations/adolphs.pdf
9. IEEE Standards Association: Standard for an Architectural Framework for the Internet of Things (IoT)—IEEE P2413 (2016)
10. Arrowhead: Automation Systems from IoT Arrowhead Framework: Concepts and Basic Architecture. Information Technology – Internet of Things Reference Architecture (IoT RA) (2017) [Online]. ISO Available at: http://www.arrowhead.eu/material/automation-systems-from-IoT-arrowhead-framework-concepts-and-basic-architecture. Accessed 13 Jan 2017
11. Ragget, D.: Web of Things: enabling exponential growth of IoT services. Sao Paulo (2016). Retrieved from: https://ceweb.br/webbr2016/apresentacoes/Dave-Raggett.pdf
12. ISO: Information Technology – Internet of Things Reference Architecture (IoT RA). International Organization for Standardization, ISO Central Secretariat, Geneva, Switzerland (2015)
13. Zarpelão, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C.: A survey of intrusion detection in Internet of Things. J. Netw. Comput. Appl. **84**, 25–37 (2017)
14. Kshetri, N.: Can blockchain strengthen the Internet of Things? IT Professional, pp. 68–72. IEEE Computer Society (2017)
15. Dhanda, S.S., Singh, B., Jindal, P.: Wireless technologies in IoT: research challenges. In: Ray, K., Sharan, S., Rawat, S., Jain, S., Srivastava, S., Bandyopadhyay, A. (eds.) Engineering Vibration, Communication and Information Processing. Lecture Notes in Electrical Engineering, vol. 478. Springer, Singapore (2019)
16. The EPCglobal Architecture Framework, EPCglobal Final Version 1.3 (2009)
17. Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., Borriello, G.: Building the internet of things using RFID: the RFID ecosystem experience. IEEE Internet Comput. **13**(3), 48–55 (2009)
18. Belpaire, A.: Internet of things: already a reality today, interview in eurescommess@ge. Mag. Telecom Insiders **2** (2009)
19. Weber, R.H.: Internet of things—new security and privacy challenges. Comput. Law Secur. Rev. **26**, 23–30 (2010)
20. Sung, J., Sanchez-Lopez, T., Kim, D.: The Epc sensor network for RFID and WSN integration infrastructure. In: Proceedings of Fifth IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom 2007) (2007)
21. Parks, A.N., Sample, A.P., Zhao, Y., Smith, J.R.: A wireless sensing platform utilizing ambient RF energy. In: Proceedings of IEEE Topical Meeting on Wireless Sensors and Sensor Networks (2013)
22. Lopez, T.S., Ranasinghe, D., Harrison, M., McFarlane, D.: Adding sense to the internet of things: an architecture framework for smart object systems. Pervas. Ubiquitous Comput. **16**(3), 291–308 (2012)
23. Guinard, D., Trifa, V., Wilde, E.: Architecting a mashable open world wide web of things. Technical Report, ETH (2010)
24. Guinard, D., Trifa, V., Mattern, F., Wilde, E., Uckelmann, D., Harrison, M., Michahelles, F.: From the Internet of Things to the Web of Things: Resource Oriented Architecture and Best Practice, Architecting the Internet of Things (2011)
25. Minoli, D., Sohraby, K., Occhiogrosso, B.: IoT considerations, requirements, and architectures for smart buildings—energy optimization and next-generation building management systems. IEEE Internet Things J. **4**(1), 269–283 (2017)
26. Duan, R., Chen, X., Xing, T.: A QoS architecture for IoT. IEEE International conference on Internet of Things, Cyber Physical and Social computing. (2011)

27. Frustaci, M., Pace, P., Aloi, G., Fortino, G.: Evaluating critical security issues of IoT world: present and future challenges. IEEE Internet Things J. **5**(4), 2483–2495 (2018). https://doi.org/10.1109/JIOT.2017.2767291
28. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: IoT: survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. **17**(4), 2347–2376 (2015)
29. Kushalnagar, N., Montenegro, G., Schumacher, C.: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): overview, assumptions, problem statement, and Goals. Internet Eng. Task Force (IETF), Fremont, CA, USA, RFC 4919, vol. 10 (2007)
30. Montenegro, G., Kushalnagar, N., Hui, J., Culler, D.: Transmission of IPv6 packets over IEEE 802.15. 4 networks. Internet Eng. Task Force (IETF), Fremont, CA, USA, Internet Proposed Std. RFC 4944 (2007)
31. Debar, H.: An introduction to intrusion-detection systems. In: Proceedings of Connect '2000, pp. 1–18 (2000)
32. Patel, A., Qassim, Q., Wills, C.: A survey of intrusion detection and prevention systems. Inf. Manag. Comput. Secur. **18**(4), 277–290 (2010)
33. Pongle, P., Chavan, G.: Real time intrusion and wormhole attack detection in Internet of Things. Int. J. Comput. Appl. **121**(9), 1–9 (2015)
34. Raza, S., Wallgren, L., Voigt, T.: SVELTE: real-time intrusion detection in the Internet of Things. Ad Hoc Netw. **11**(8), 2661–2674 (2013)
35. Thanigaivelan, N.K., Nigussie, E., Kanth, R.K., Virtanen, S., Isoaho, J.: Distributed internal anomaly detection system for Internet-of-Things. In: Proceedings of the 13th IEEE Annual Consumer Communications Networking Conference (CCNC), pp. 319–320 (2016)
36. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E.: Anomaly-based network intrusion detection: techniques, systems and challenges. Comput. Secur. **28**, 18–28 (2009)
37. Roman, B., Jacob, S.C., Nikolaj, L., Simon, M.: Blockchain - The gateway to trust-free cryptographic transactions. Twenty-Fourth European Conference on Information Systems, Istanbul Turkey. Research paper, vol. 153 (2016)
38. Christidis, K., Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things, pp. 2292–2303. IEEE Access (2016)
39. Nordrum, A.: Wall Street firms to move trillions to blockchain in 2018. IEEE Spectrum (2017). Retrieved from: https://spectrum.ieee.org/telecom/internet/wall-street-firms-to-movetrillions-to-blockchains-in-2018
40. Lewis, K.: Blockchain: four use cases transforming business. IBM Internet of Things blog (2017). https://www.ibm.com/blogs/internetof-things/iot-blockchain-use-cases/
41. Lotay, K., DeCusatis, C.: Using blockchain technology to digitize supply chain systems. In: Proceedings of the National Conference on Undergraduate Research, Atlanta, GA, 3–5 Nov 2017 (2017)
42. Peck, M.: Blockchains: how they work. IEEE Spectrum (2017). https://spectrum.ieee.org/computing/networks/blockchains-how-theywork-and-why-theyll-change-the-world
43. Peck, M., Wagman, D.: Blockchains allow rooftop solar energytrading. IEEE Spectrum (2017). https://spectrum.ieee.org/computing/networks/blockchains-will-allowrooftop-solar-energy-trading-for-fun-and-profit
44. Flores, A., Gannon, K.: BlockChain on AWS: Disrupting the Norm. Paper GPSD301, AWS Re:Invent 2016 (2016). https://www.slideshare.net/AmazonWebServices/aws-reinvent-2016-blockchain-on-aws-disrupting-the-norm-gpst301
45. Cisco Institution: Cisco 2017 annual cybersecurity report. Cisco, Tech. Rep. (2017)
46. Hypponen, M., Tuominen, T.: F-Secure 2017 State of Cybersecurity report. F-Secure, Tech. Rep. (2017)
47. Nakamoto, S.: Bitcoin: a peer to peer electronic cash system (2008). http://nakamotoinstitute.org/bitcoin/, http://bitcoin.org/bitcoin.pdf, https://github.com/saivann/bitcoinwhitepaper
48. Miller, R.: IBM unveils HyperLedger project (2017). https://techcrunch.com/2017/03/19/ibm-unveils-blockchain-as-a-servicebased-on-open-source-hyperledger-fabric-technology/

49. DeCusatis, C., Zimmermann, M., Sager, A.: Identity-based Network Security for Commercial Blockchain Services (2018)
50. Singh, S., Sharma, P.K., Moon, S.Y., Park, J.H.: Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J. Ambient Intell. Hum. Comput. (2017). https://doi.org/10.1007/s12652-017-0494-4
51. Schneier, B.: IoT security: what's plan B? IEEE Secur. Priv. **15**(5), 96 (2017)
52. Hatzivallis, G., Fysarakis, K., Papaefstathiou, I., Manifavas, C.: A review of lightweight block ciphers. J. Cryptogr. Eng. **8**, 141–184 (2018)
53. Schinianakis, D.: Alternative security options in the 5G and IoT era. IEEE Circuits Syst. Mag. 6–28 (2017)
54. Kong, J.H., Ang, L.-M., Seng, K.P.: A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments. J. Netw. Comput. Appl. **49**, 15–50 (2015)
55. Leander, G., Paar, C., Poschmann, A., Schramm, K.: New lightweight DES variants. In: Biryukov, A. (ed.) The 14th Annual Fast Software Encryption Workshop—FSE 2007. LNCS, vol. 4593, pp. 196–210. Springer, Berlin, Germany (2007)
56. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Proceeding of Cryptographic Hardware and Embedded Systems—CHES 2007, pp. 450–466. Springer (2007)
57. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (extended abstract). In: Fast Software Encryption (FSE 2007). LNCS, vol. 4593, pp. 181–195. Springer (2007)
58. De Canniere, C., Dunkelman, O., Knežević, M.: KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers. In: International Workshop on Cryptographic Hardware and Embedded Systems, pp. 272–288. Springer (2009)
59. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE: a lightweight, versatile block cipher. In: Proceeding of ECRYPT Workshop on Lightweight Cryptography 2011, pp. 146–169 (2011)
60. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., Yalçın, T.: PRINCE—a low-latency block cipher for pervasive computing applications. In: Proceeding of ASIACRYPT 2012, pp. 208–225. Springer (2012)
61. Karakoç, F., Demirci, H., Harmancı, A.E.: ITUbee: a software oriented lightweight block cipher. In: Proceeding of Lightweight Cryptography for Security and Privacy—LightSec2013, pp. 16–27. Springer (2013)
62. Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J., Wingers, L.: The SIMON and SPECK lightweight block ciphers. In: Proceeding of 52nd ACM/EDAC/IEEE, Design Automation Conference (DAC), pp. 1–6. IEEE (2013)
63. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, I.: RECTANGLE: a bit-slice ultra-lightweight block cipher suitable for multiple platform. Sci. China Inf. Sci. **58** (12), 1–15 (2014)
64. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., Regazzoni, F.: Midori: A Block Cipher for Low Energy, pp. 411–436. Springer, Berlin, Germany (2015)
65. Li, L., Liu, B., Wang, H.: QTL: a new ultra-lightweight block cipher. Microprocess. Microsyst. **45**, 45–55 (2016)
66. Sadeghi, S., Bagheri, N., Abdelraheem, M.A.: Cryptanalysis of QTL cipher. Microprocess. Microsyst. **52**, 34–48 (2017)
67. Boesgaard, M., Vesterager, M., Pedersen, T., Christiansenm, J., Scavenius, O.: Rabbit: a new high-performance stream cipher. FSE 2003, LNCS, vol. 2887, pp. 307–329. Springer, Lund, Sweden (2003)
68. Hell, M., Johansson, T., Meier, W.: Grain—a stream cipher for constrained environments. In: Workshop on RFID and Light-Weight Crypto: Workshop Record, Graz, Austria, Jul 2005

69. De Cannière, C., Preneel, B.: Trivium—A Stream Cipher Construction Inspired by Block Cipher Design Principles. ECRYPT Stream Cipher (2006). Available at: http://www.ecrypt.eu.org/stream/papersdir/2006/021.pdf
70. Bernstein, D.J.: The Salsa20 stream cipher, slides of talk. In: ECRYPT STVL Workshop on Symmetric Key Encryption (2005). http://cr.yp.to/talks.html#2005.05.26
71. Hell, M., Johansson, T., Maximov, A.: A stream cipher proposal, Grain-128. In: IEEE International Symposium on Information Theory, Seattle, WA, pp. 1614–1618 (2006)
72. Babbage, S., Dodd, M.: The MICKEY stream ciphers. Proceeding of New Stream Cipher Designs, pp. 191–209. Springer, Berlin (2008)
73. Bernstein, D.J.: ChaCha, a variant of Salsa20 (2008). http://cr.yp.to/papers.html#chacha. Accessed 28 Jan 2008. Supersedes: (PDF)2008.01.20
74. Orhanou, Ghizlane, Hajji, Said E.L., Bentalab, Youssef: SNOW 3G stream cipher operation and complexity study. Contemp. Eng. Sci. **3**(3), 97–111 (2010)
75. Tian, Yun, Chen, Gongliang, Li, Jianhua: Quavium—a new stream cipher inspired by trivium. J. Comput. **7**(5), 1278–1284 (2012)
76. Fan, X., Mandal, K., Gong, G.: Wg-8: a lightweight stream cipher for resource-constrained smart devices. In: International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, pp 617–632. Springer, Berlin, Heidelberg (2013)
77. Armknecht, F., Mikhalev, V.: On lightweight stream ciphers with shorter internal states. In: Leander, G. (ed.) Fast Software Encryption: 22nd International Workshop, FSE 2015, Istanbul, Turkey, Revised Selected Papers, pp. 451–470. Springer, Berlin (2015). https://doi.org/10.1007/978-3-662-48116-522
78. Ghafari, V.A., Hu, H., Xie, C.: Fruit V2: ultra-lightweight stream cipher with shorter internal state. Cryptology ePrint Archive Report 2016/355 (2016). http://eprint.iacr.org/2016/355
79. Hamann, M., Krause, M., Meier, W.: LIZARD—a lightweight stream cipher for power-constrained devices. IACR Trans. Symmetric Cryptol. **2017**(1), 45–79 (2017). https://doi.org/10.13154/tosc.v2017.i1.45-79
80. Aumasson, J.-P., Henzen, L., Meier, W., Naya-Plasencia, M.: Quark: a lightweight hash. In: International Workshop on Cryptographic Hardware and Embedded Systems, pp. 1–15. Springer (2010)
81. Hirose, S., Ideguchi, K., Kuwakado, H., Owada, T., Preneel, B., Yoshida, H.: A lightweight 256-bit hash function for hardware and low-end devices: lesamnta-LW. In: Proceeding of International Conference on Information Security and Cryptology, pp. 151–168. Springer, Berlin (2010)
82. Kavun, E.B., Yalcin, T.: A lightweight implementation of Keccak hash function for radio-frequency identification applications. In: International Workshop on Radio Frequency Identification: Security and Privacy Issues, pp. 258–269. Springer (2010)
83. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON family of lightweight hash functions. In: CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. International Association for Cryptologic Research (2011)
84. Bogdanov, A., Knežević, M., Leander, G., Toz1, D., Varıcı, K., Verbauwhede, I.: SPONGENT: a lightweight hash function. In: CHES 2011, LNCS, vol. 6917, pp. 312–325. International Association for Cryptologic Research (2011)
85. Berger, T.P., D'Hayer, J., Marquet, K., Minier, M., Thomas, G.: The GLUON family: a lightweight hash function family based on FCSRs. In: Mitrokotsa, A., Vaudenay, S. (eds.) Progress in Cryptology—AFRICACRYPT 2012. Lecture Notes in Computer Science, vol. 7374. Springer, Berlin, Heidelberg (2012)
86. Wu, W., Wu, S., Zhang, L., Zou, J., Dong, L.: LHash: A Lightweight Hash Function (Full Version) (2013). https://eprint.iacr.org/2013/867
87. Mukundan, P.M., Manayankath, S., Srinivasan, C., Sethumadhavan, M.: Hash-One: a lightweight cryptographic hash function. IET Inf. Secur. **10**(5), 225–231 (2016)
88. Bussi, K., Dey, D., Kumar, M., Dass, B.K.: Neeva: A Lightweight Hash Function. IACR Cryptology ePrint Archive (042) (2016). Available at: https://eprint.iacr.org/2016/042

89. Szczechowiak, P., Oliveira, L.B., Scott, M., Collier, M., Dahab, R.: NanoECC: testing the limits of elliptic curve cryptography in sensor networks. In: Wireless Sensor Networks—EWSN 2008. Lecture Notes in Computer Science, vol. 4913, pp. 305–320. Springer (2008)
90. Varchola, M., Guneysu, T., Mischke, O.: MicroECC: a lightweight reconfigurable elliptic curve crypto-processor. In: Proceedings of International Conference on Reconfigurable Computing and FPGAs, Cancun, Mexico, 30 Nov–2 Dec 2011. https://doi.org/10.1109/reconfig.2011.61
91. Liu, A., Ning, P.: TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks. In: Proceedings of the 7th International Conference on Information Processing in Sensor Networks (IPSN 2008), pp. 245–256. IEEE Computer Society Press (2008)
92. Wang, H., Li, Q.: Efficient implementation of public key cryptosystems on mote sensors. In: Information and Communications Security—ICICS 2006. Lecture Notes in Computer Science, vol. 4307, pp. 519–528 (2006)
93. Liu, Z., Wenger, E., Großschädl, J.: MoTE-ECC: energy-scalable elliptic curve cryptography for wireless sensor networks. In: Boureanu, I., Owesarski, P., Vaudenay, S. (eds.) Applied Cryptography and Network Security. ACNS 2014. Lecture Notes in Computer Science, vol. 8479. Springer, Cham (2014)
94. He, D., Wang, H., Khan, M.K., Wang, L.: Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. IET Commun. **10**(14), 1795–1802 (2016)
95. Liu, Z., Huang, X., Zhi, H., Khan, M.K., Seo, H., Zhou, L.: On emerging family of elliptic curves to secure Internet of Things: ECC comes of age. IEEE Trans. Depend. Secure Comput. **14**(3), 237–248 (2017)

Chapter 20
Security Threats for Time Synchronization Protocols in the Internet of Things

Suresh Kumar Jha, Niranjan Panigrahi and Anil Gupta

Abstract The Internet of Things (IoT) is an emerging field of application includes several technologies such as the Internet, Wireless Sensor Networks (WSN), Radio Frequency Identification (RFID), and communication technology which build a system that connects real and digital worlds. For the consistent working of the IoT ecosystem, the backbone WSN needs time synchronization. In the IoT ecosystem, the sensors are generally located in an unattended environment where may be a high chance of the existence of malicious nodes. In such a scenario, the time synchronization protocols will behave incorrectly which in turn will hamper the normal working of other dependent protocols. This chapter contributes a thorough insight into the possible threats to time synchronization in backbone WSN of IoT, existing security measures with qualitative and quantitative analysis, and their scope and limitations. This will further help the research community to develop light-weight and efficient secured time synchronization protocols for IoT.

Keywords IoT · WSN · Time synchronization · Security threats

20.1 Introduction

In a short time ago, the Internet of Things (IoT) emerged as a new era of application in almost all fields of society and engineering problems. In all applications of IoT, sensors are deployed to form a network to observe the physical or natural condition

S. K. Jha (✉) · A. Gupta (✉)
Computer Science Department, MBM Engineering College JNVU, Jodhpur, Rajasthan, India
e-mail: suresh.jha84@gmail.com

A. Gupta
e-mail: anilgupta@jnvu.edu.in

N. Panigrahi (✉)
Computer Science Department, PMEC, Berhampur, Odisha, India
e-mail: niranjan.cse@pmec.ac.in

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_20

and can collaborate with other components of the system to keep a record of the status of things such as movements, temperature, heat, pressure, humidity, etc. It would be not surprising to say that WSN acts as the backbone of IoT. For the consistent working of the IoT ecosystem, the backbone WSN needs time synchronization. It is the process by which sensor nodes in IoT adjust their clock value to coordinate with the other devices in the network. It is crucial for many applications like real-time control, power management, sleep schedule, and speed calculation in IoT. Moreover, if one node's clock is not synchronized from other neighbor's nodes in the network, it may lead to message collision, network congestion, energy depletion for resynchronization and incorrect results from other time-dependent protocols like TDMA, localization, etc. [1].

A lot of protocols using for time synchronization have been shown in research for WSN in the last decades with the least concern for security threats. In the IoT ecosystem, sensor nodes are generally located in an unattended environment where it may be a high chance of the existence of malicious nodes. In such a scenario, the time synchronization protocols will behave incorrectly which in turn will hamper the normal working of other dependent protocols. Some recent works of literature have reported security threats to time synchronization protocols like message manipulation attack, Sybil attack and proposed some traditional cryptographic and complex mechanism as countermeasures. But, due to the built-in limitations of sensor networks like limited hardware, limited energy, and processing power, restricted bandwidth, unattended environment, etc., it makes it difficult to apply traditional security mechanisms due to large computational overhead. Hence, it is necessary to have a comprehensive survey on vulnerabilities issues in time synchronization for sensor networks and their countermeasures [2].

The proposed chapter will contribute a thorough insight into the fundamentals of time synchronization, an exhaustive survey of state-of-the-art time synchronization protocols, possible threats to time synchronization in backbone WSN of IoT, existing security measures with qualitative and quantitative analysis, and their scope and limitations. This will further help the research community to understand the security aspect of time synchronization and to develop light-weight and efficient secured time synchronization protocols for IoT.

The remaining chapters are arranged in following ways. Section 20.2 explores a brief overview of the IoT ecosystem, time synchronization fundamentals, and different threat models. Section 20.3 describes some state-of-art time synchronization protocols. Section 20.4 discusses possible threats to time synchronization protocols and their existing countermeasures. Section 20.5 presents a qualitative and quantitative analysis of the existing time synchronization approaches with security aspects and Sect. 20.6 concludes the chapter.

20.2 Preliminaries

This part of the chapter explores a brief overview of the IoT, time synchronization and security threat models.

20.2.1 IoT Overview

Internet of Things means a combination of two terms: first is the Internet, the Internet means a network where billions of computing devices connected and communicate by some common rules is called protocols. The second is the Things, which means these devices and objects converted into intelligent objects where each device can communicate, compute and converted into meaningful information as to their requirement. In other words, IoT is the interconnection of physical worlds (sensors and actuators) and digital worlds. The future IoT network can be visualized as shown in Fig. 20.1.

The IoT is turning into a promising worldview with the broad market selection of the improvement of related innovations, for example, distributed computing, cloud computing, wireless mobile network and so on.

This will reveal the future direction of the worldwide communication technology. Continuous integration of monitoring and preparing the usefulness of IoT apps

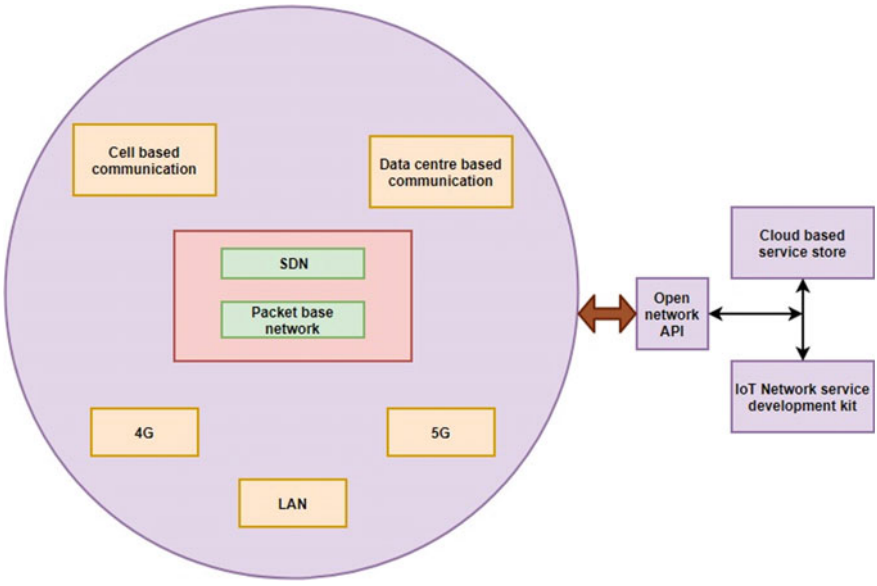


Fig. 20.1 Future IoT network

is enabled by Wireless Sensor Networks together with present communication techniques. Since sensor nodes are usually used to obtain sensitive data from unattended or antagonistic circumstances, they are discovered for safety assaults that strongly affect user privacy and network performance.

In IoT, the service layer, platform layer, network layer, and computer layer are four layers. The basic layer is the IoT service layer, which established communication with users. The platform layer whose main task is the execution of different applications like data analysis platform. The network layer responsible for the transmission of the data among each device and manages network traffic also. The fourth layer is the device layer that senses the environment by using the sensing devices, convert the information by applying a smart algorithm and deliver to the sink node. The security aspect might be considered as an important issue in all layers of IoT as shown in Fig. 20.2 to protect the overall ecosystem from threats [3].

There are different security threats mechanisms and their solutions for WSN protocols have been explored in the literature [2]. Being the backbone of IoT, it is necessary to consider its relevance and related security challenges from the IoT point of view. The thought process of this chapter is to examine and demonstrate the impact of security challenges in time synchronization protocols of backbone WSN for IoT.

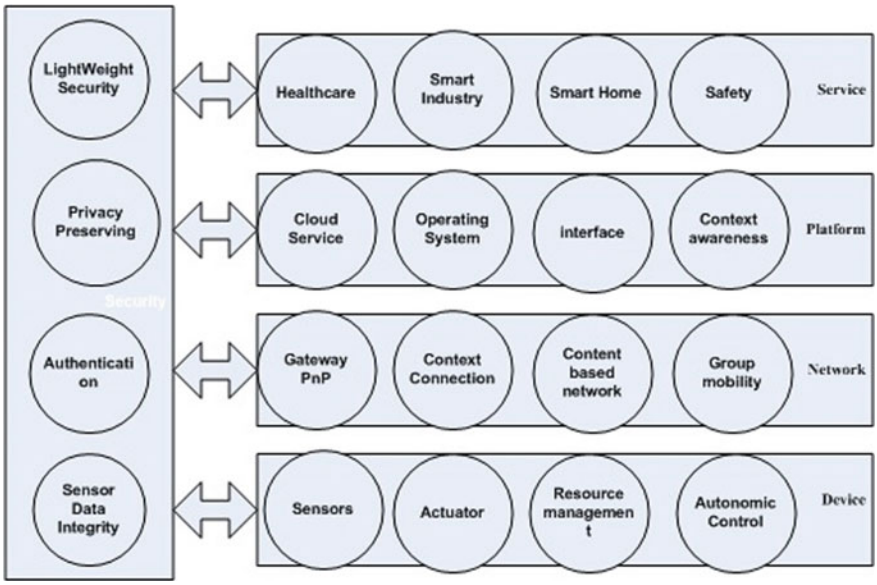


Fig. 20.2 IoT ecosystem

20.2.2 Time Synchronization Overview

Synchronization word is very important in the computer science field like process synchronization, thread synchronization, and data synchronization. The requirement for synchronization arose not only in the single processor but also in concurrent processes to multiprocessor and distributed computing. Parallel programming also requires synchronization to all processes waits for other processes to completion. In the era of the 17th century, Galileo and Christian have developed an accurate scientific clock, based on the pendulum motion. After that atomic clocks were used in different applications like the GPS system, digital communication network. Furthermore, it has been seen that all nodes should be agreed on a unique time in the network. Therefore, time agreement is the essential requirement in the network, which helps to smoothly work of other protocols and applications [4].

The technique to provide the unique time notation among different nodes in the wireless network is known as time synchronization. For accomplish the time synchronization it is required that, every node of the network must communicate with one another through the communication link. These links may be wired or wireless. Time synchronization is an exciting subject in WSN as being a backbone of IoT. The following sections present the fundamentals and terminologies of time synchronization.

20.2.2.1 Hardware Clock

The clock is a main part of a sensor node built by an oscillator and a counter register. There are many types by which oscillators can be embedded in micro-controllers like crystal oscillators, RC oscillators one more is silicon oscillators. But crystal has more accuracy and lower cost, for this reason mostly sensors uses crystal oscillators in the time circuit. Two types of hardware clock available in sensor motes like internal hardware clock and another is external which is on-board.

The hardware clock is fixing inside the micro-controller. The crystal oscillators used in the clocks have lower frequency stability and the internal clock is switched off while the CPU is in sleeping mode. So, the internal clock is not useful for many applications.

Therefore, to deliver continuous timing service for continue interval, an external onboard hardware clock must be used. Furthermore, the external clocks work actively while the CPU resides in a sleep mode. Each hardware clock is equipped with a counter register to read the real-time of the hardware clock. The counter register is decreased at each oscillation of the crystal, while it reaches zero. It is reset and an interrupt occur. The interrupt generated is called a clock tick, which increased the software clock as other counter considers this value as the clock time of the sensor node.

A software clock therefore indicates sensor node's local time, where C(t) at some real time t indicates the clock reading. The time resolution of the software clock can be described as the distance between two ticks [5]. The clock offset can be define as the differences among the local times of each nodes and the clock rate is the frequency on which the clock is being progressed.

The clock skew can be characterized as the deviation in frequencies of two clocks. The clock rate dc/dt depends on the age of crystal, temperature, humidity, voltage, etc., the drift rate can expresses as η the rate by which two clocks can drift apart, that is, dc/dt − 1 [5].

$$1 - \eta \leq \frac{dc}{dt} \leq 1 + \eta \tag{20.1}$$

20.2.2.2 Software Clock

The software clock is an external hardware clock that indicates the local time as C(t) which is the clock real-time t. It can be represented by expressed mathematically as:

$$C(t) = K \int_0^t \omega(t)dt + C(t_0) \tag{20.2}$$

Here ω(t) is considered as the oscillator's frequency.

K is a proportionate coefficient and $C(t_0)$ can be considered as clock's initial value.

For an ideal clock, dc/dt = 1. But due to the ambient nature of sensor nodes such as vibration, circuit voltage, the temperature of the area, the quartz oscillator's age, oscillator frequency varies accordingly, and the clock drifts.

As shown in Fig. 20.3, if dc/dt < 1, the clock is considered as slower clock and if dc/dt > 1, clock is treated as a faster clock. When the angular frequency could be a fixed value, the clock of node 'i' can be explored.

$$C_i(t) = a_i(t) + b_i \tag{20.3}$$

where a_i = clock skew and b_i = clock offset.

The frequency rate of the clock and offset is known as the variation from the actual time is known as the skew rate. The comparison of the local clock of one node 'i' with another relative node 'j', Eq. 20.3 can be again written as

$$C_i(t) = a_{ij}(t) + b_{ij} \tag{20.4}$$

where a_{ij} = relative skew and b_{ij} = relative offset. When both nodes would synchronized, then $a_{ij} = 1$ and $b_{ij} = 0$ [4].

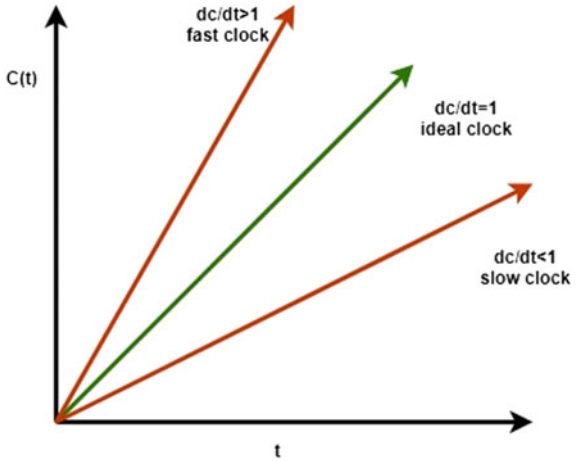


Fig. 20.3 Clock behaviors

20.2.2.3 Sources of Synchronization Error

These are the following classification of delays by which the synchronization error occurred in WSN.

1. **Send time**: It is known as taken time by the sending node to preparing the packets on the application layer, sending it to the MAC layer. It is done on the operating system level.
2. **Access time**: It is known as the MAC layer waiting to get the transmission channel. This delay plays the most vital role in the systems.
3. **Transmission time**: The message requires time for the wireless connection to be transmitted. It is also a determinist delay and the duration of the packet size and the channel data rate can be estimated.
4. **Propagation time**: The time spends on the wireless link, between network interfaces of the sender and receiver once packet moves from the sender. It is negligible in WSN.
5. **Reception time**: When the receiver receives the packet and passed it to the MAC layer, it is called reception time.
6. **Receive time**: Processing the incoming packet and sending it to the host requires time for the receiver side.

20.2.2.4 Performance Metrics

The wireless sensor network's performance is based on some quantitative parameters known as performance metrics. Different applications have requires different demands on the clock synchronization scheme. Some of the applications required high accuracy like TDMA, while some needs energy efficiency in WSN. There exist

many performance metrics discussed in the literature. All requirements cannot be satisfied by an algorithm, yet tries to optimize it. These are the following performance metrics for WSN, which can be considered in designing a synchronization algorithm [4].

1. **Energy Efficiency**: As the sensor node's power source is the battery, which has limited energy. During the message exchange between nodes more energy consumed. While designing a synchronization algorithm it should be the main issue.
2. **Scalability**: while network size grows or shrink the accuracy of the synchronization algorithm must stable.
3. **Ease of Deployment**: The sensor networks made by of millions of sensor nodes, so each node should be achieved communication by others in the absence of infrastructure of the network.
4. **Precision**: Synchronization precision or accuracy varies according to applications. Some applications required simple ordering of events e.g., some monitoring applications. Whereas, some required high precision in the microseconds in time-critical applications e.g., body area sensor networks for surgical purposes.
5. **Hop Count**: The number of hop in the network determines the cost of the path and the energy consumed in the process.
6. **Robustness**: Robustness related to fault tolerance. Sensor nodes are spread in the unattended area, due to node failure or link failure for any reason, the operation should continue with the required accuracy.

Apart from the above-mentioned metrics, there are some other factors such as production cost, operating environment, topology, constraints of hardware, and transmission media have to be considered. More or less, many works of literature have made attempts to evaluate the above performance metrics, but the security issue is still the least explored area in time synchronization protocols. Considering security as the scope of this chapter, the following section introduces the attack models in time synchronization protocols.

20.2.3 Network Model, Attack Model, and Clock Model

20.2.3.1 Sybil Attack Model

To represent the attack, a sensor network is considered with x normal node and y malicious node where $x > y$. The attacker node may be outside or inside which is convinced by the attacker. The graph-based approach is used to explore the attack

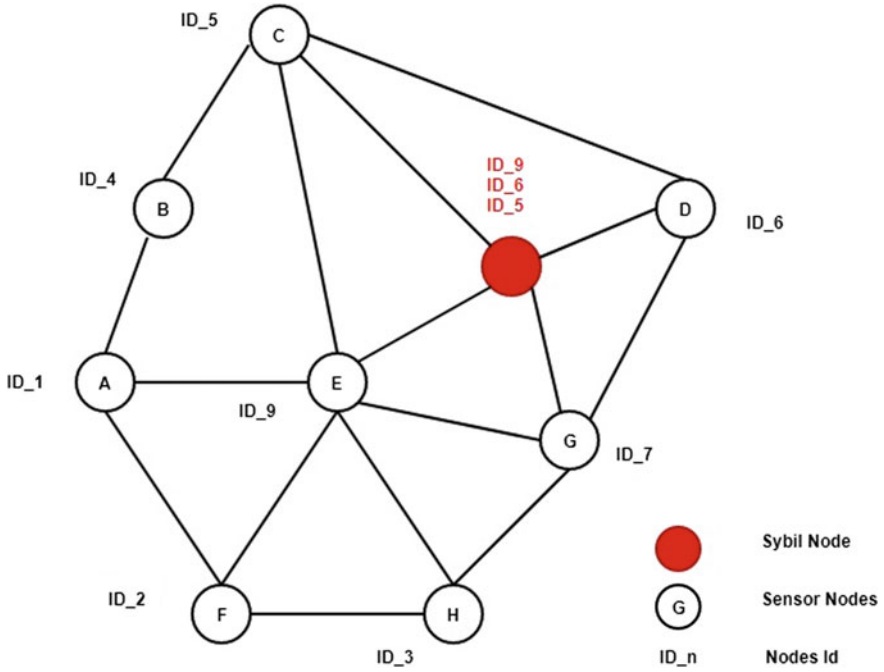


Fig. 20.4 Sybil attack model representation using graph

model. Let G(t) = (v, e(t)) represent the Graph of a network where V represents the all vertices or nodes while e(t) are the transmission links. We assume that the graph is fully connected and undirected.

Figure 20.4 shows a graph containing 9 number of vertices which are connected as shown. The node in red color is represented as an attacker node or Sybil node which keeps the identity of nodes 5, 6, 9. At the synchronization phase, a Sybil node sends multiple identities and convinces other nodes to communicate and finally desynchronize the network.

20.2.3.2 Message Manipulation Attack Model

In Fig. 20.5 Node B sends packets with a header to node G. But Intruder I decapsulates packets, change the header and node G has no direct route with H, thus the packet dropped.

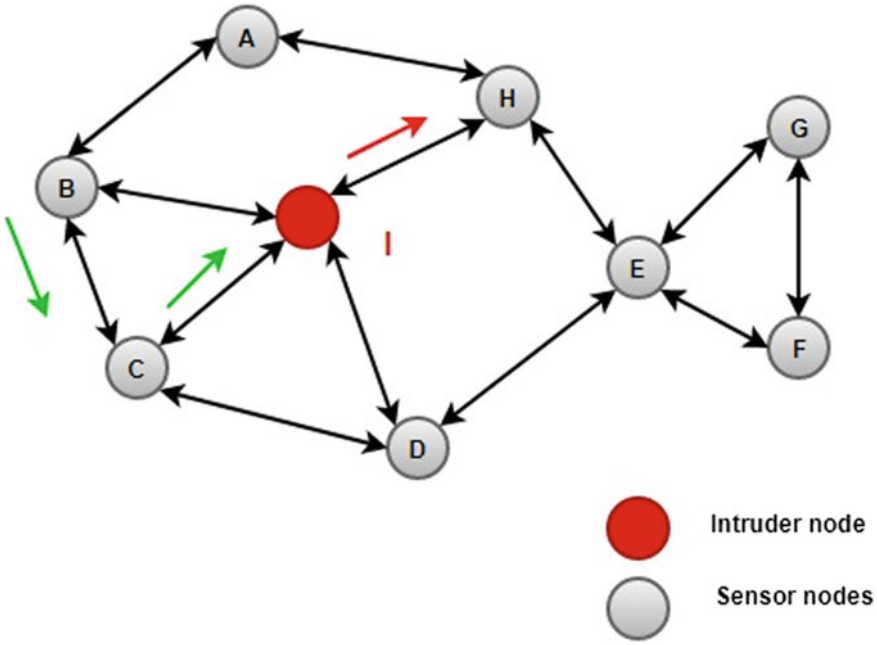


Fig. 20.5 Message manipulation model

20.2.4 Clock Model

In literature [6], clock model of time synchronization is adopted as the hardware clock $P_i(T)$ of a node $i \in v$ at time T can be represented as a linear function.

$$P_i(T) = q_i T + r_{i,} \quad i \in v, \tag{20.5}$$

where q_i may be considered as hardware clock skew represent the clock speed and r_i hardware clock offset. In the ideal case, $q_i = 1$ and $r_i = 0$.

Here q_i and r_i cannot be determined. Moreover, the hardware clock of the node can also be explores as

$$P_i(T) = \frac{q_i}{q_j}\tau_j(T) + \left(r - \frac{q_i}{q_j} r_j\right) = q_{ji}\tau_j(T) + r_{ji,} \tag{20.6}$$

where $q_{ji} = \frac{q_i}{q_j}$ is the relative hardware clock skew $r_{ji} = r_i - q_{ji} r_j$ and is the relative hardware clock offset.

The relative skew q_{ij} is defined as $q_{ij} = \frac{q_j}{q_i}$, which is estimated by

$$q_{ij}(T) = \frac{P_i(T_1) - P_j(T_0)}{P_i(T_1) - P_i(T_0)}, \quad i,j \in v, \tag{20.7}$$

Since it is almost impossible to adjust the hardware clock skew or offset manually. To replace the hardware clock, we can identify a logical clock $K_i(t)$ as follows:

$$K_i(T) = \hat{q}_i(T)P_i(T) + \hat{r}_i(T) = \hat{q}_i(T)q_i t + \hat{q}_i(T)r_i + \hat{q}_i(T), \tag{20.8}$$

where $q_i(T)$ and $r_i(T)$ are two adjusting parameters.

20.3 Backgrounds

The WSNs have distributed networks that consist of a huge collection of sensors with limited power, small transmission range, limited processing, low bandwidth, and fix storage capacity. In recent years, WSNs in IoT have witnessed many applications such as in medical, agriculture to monitor the environment, weather

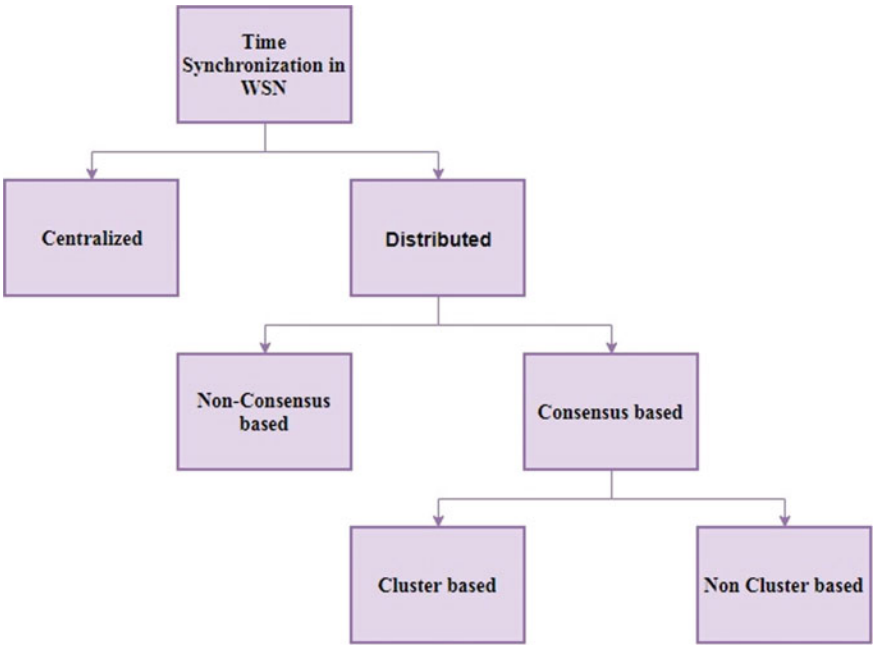


Fig. 20.6 Classification of time synchronization in WSN

forecast, target tracking, event detection, security, and target localization. For all these applications, time synchronization is an essential feature. Due to the lack of a global physical clock, time synchronization has one of the basic issues that remained in the traditional distributed scheme due to the absence of a worldwide physical clock. It was a well-studied issue in a wired network. The Network Time Protocol (NTP), for example, was used on the Internet as a synchronization protocol. NTP needs an atomic clock server. The client is synchronized with the server by UDP packet exchange. NTP is used to synchronize nodes on the Internet. It is not suited for sensor networks for its complexity and sensor node's limitation in terms of the energy issue, cost and size [7] (Fig. 20.6).

In this section, we have explored the standard protocols used for time synchronization and briefly present the journey from a centralized approach to a traditional distributed approach in WSNs. Then, based on the existing methods a survey tree is shown, which helps the research community to distinguish the different time synchronization methods available for WSNs. The current protocols for time synchronization can be widely split into the following kinds [8].

1. Centralized approach
2. Distributed approach

20.3.1 Centralized Approach

Centralized time synchronization protocols are fully dependent on the unique source node and have less scalability and robustness in their topology. Some examples in the centralized approach are RBS, TPSN, and FTSP [9–11]. In RBS, An intermediate node is used to synchronize two node clocks. To synchronize two node clocks, an intermediate node is used. Different nodes in TPSN protocol [12] involve pair synchronization to find their offset and drifts, assuming both are linear. One node declared as the leader node in FTSP [11] and the other nodes synchronize with the leader node. Many times synchronization protocol uses sender to receiver synchronization while RBS uses R-R synchronization approach. The RBS protocol broadcast reference messages to set of receivers for synchronization with other nodes, when the broadcast message arrives at all receivers, each receiver records its local time, then exchange local time with each other to calculate the offset.

TPSN follows the sender-receiver approach and tree-like topology to synchronization with other nodes. The concept is divided into two phases, one is the phase of level discovery and the other is the phase of synchronization. The level discovery stage constructs the network's hierarchical structure and assigns each node a level. One node operates as a tier zero root node. All n-level nodes synchronized with $n - 1$ level nodes up to the root node in the synchronization stage. The level discovery stage is executed during the network deployment. The root node is fixed at level 0 and broadcast the level discovery packets to initiate the synchronization with its neighboring nodes. This packet keeps the identity of nodes and the sender's

node levels. The next neighbors of the root took this packet and assigned them a level for themselves, more than one from the previous level that is 1. When setting the level they send new packets also known as discovery packet including its own level. The process continued until every node assigned a level in the network. The phase performs pairwise synchronization among the hierarchical structure done in the previous stage. This protocol uses a sender-receiver message approach to handshake among nodes [10].

There are many advantages of FTSP over TPSN. The TPSN supports a multi-hop network, but not able to handle the network at the changes on topology. The disadvantage is that when a topology change occurs, it repeats the level discovery phase from the root node. This required more overhead and increase network traffic. FTSP is more reliable that transmit the flooding of synchronization messages at node failure or changes of dynamic topology. At a regular interval, the root node is elected on the dynamic topology changes. FTSP also supports MAC layer time stamping by increasing accuracy and reducing jitter to eliminate the time mistake of propagation. To estimate clock drift and offset, it utilizes the linear regression method and multi-time stamping. The FTSP advantages are that it supports dynamic topology and achieve robustness at node failure by continuous sending flooding packet. FTSP uses MAC-layer time stamping to achieve high precision performance by clock skew estimation.

20.3.2 Distributed Approach

This chapter focuses on a distributed approach in wireless sensor networks to enhance time synchronization. The concept behind the distributed approach is that

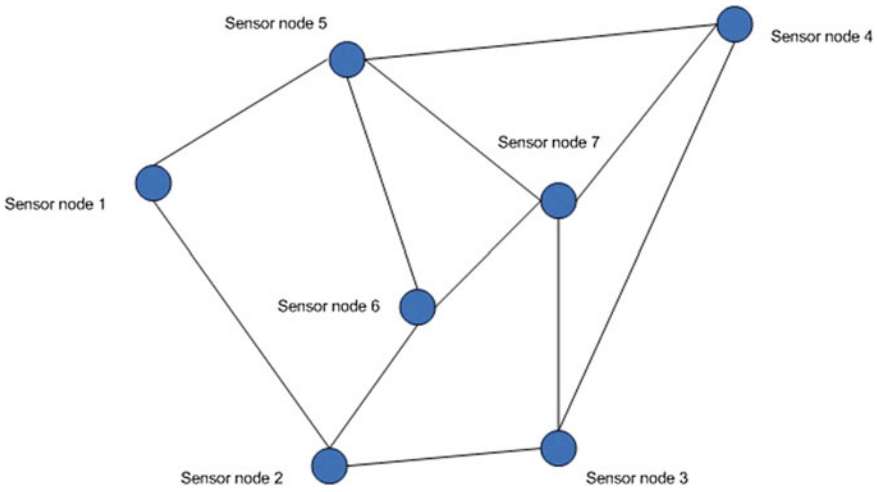


Fig. 20.7 Distributed synchronization

at a common moment in a network, all nodes in a network should be satisfied without reference to a root node. The distributed approach further categorized in two types, i.e., consensus and non-consensus based. Consensus-based protocols are RFA, ATS, MTS [6, 13, 14] (Fig. 20.7).

The Reachback firefly (RFA) algorithm is more robust to the failure of links and nodes. In RFA all node produce a pulse signal and receives pulses by neighbors nodes and according to this set their firing phase. To calculate the delay among nodes MAC-layer time-stamping has been used. To deal with delay the term Reachback response has been discussed. By this method when a node listening to its neighbor fire, it doesn't react rapidly, but store the messages in a queue and then report to all nodes in the next cycle [14].

The Gradient Time Synchronization Protocol [15] (GTSP) operates on local data and does not use tree topology or a reference node which build it robust in link or node failure. Each node periodically sends their neighbors a message of synchronization called beacon. The theoretical analysis demonstrates that the logical clock is measured by the synchronization signals received from the neighbors.

Schenato and Fiorentin [13] explored a consensus-based protocol, known as Average TimeSync (ATS) which agreed on a common message, ATS is an average consensus-based time synchronization protocol. The idea behind ATS is to let update each node according to the message exchange from its neighboring node for synchronizing a wireless sensor network. The common concept is to average local data and reach a common agreement on a particular amount of interest. It is fully distributed, involving both skewed and computational lite compensation. It also needs an enormous quantity of information exchange and gives slow converging speed, when network size increases and can be quite slow owing to this converging speed.

An improvement has been shown over ATS in the maximum consensus-based time synchronization protocol (MTS) protocol [16]. The main concept of MTS protocol is a maximum value consensus approach. The logic behind MTS is to maximize the local information for global synchronization. It provides faster convergence speed, means synchronization can be finished in a finite time and also compensates clock skew as well as offset. Moreover, the MTS protocol is fully distributed, and more robust on packet dropping, nodes failure and including any new nodes [15].

20.4 Time Synchronization Threats and Their Countermeasures

Wireless sensor networks are usually implemented on the IoT platform to collect delicate data from hostile settings. They are exposed to security attacks that can affect user privacy and efficiency of the IoT network. The numerous articles addressed multiple safety mechanisms and solutions for WSNs [11, 17].

But, it requires more awareness for its application and feasibility standard regarding security challenges in the IoT perspectives. This section explores the influence of traditional Wireless Sensor Networks security challenges in clock synchronization with the IoT perspective. There are two approaches of time synchronization in WSN, i.e., centralized and distributed approach which is already discussed in Sect. 20.3. The protocols which come under a centralized approach are RBS, TPSN, and FTSP.

RBS [9] protocol supports receiver to receiver message passing technique, on which attack can be done easily. In RBS both nodes receive the reference beacon and after that compute the offset with each other. An attack can be executed by convincing anyone node by an incorrect time. The other node which is not convinced will compute the wrong offset during the message exchange time.

TPSN [10]. The tree like structure follows the sender to receiver message passing method. First, the level discovery stage and the synchronization phase are two stages, both initialized by the root node. In the first phase the level number and the time both to be sent through by the route. An attack can be executed by simply convinced a non-root node with the incorrect time. It will propagate in the whole tree and all the nodes will be desynchronized. The nodes can also give wrong information about their level. Which may be the reason for other nodes that, when a request to synchronization information it could give wrong information? That node maybe refuses to take part in the level discovery phase and the cause may be eliminating its child node from the network. In FTSP there is a facility to select a node as a root node after a certain time frame not received synchronization message. An intruder node can announce itself as the root node and remaining nodes will respond to their timing information to intruder root node instead of the correct root node and result would be incorrectly calculated skew and offset.

Since RBS is a single-hop protocol, so anyhow prevent a sending node to do not convince by the intruder to send out erroneous timing information. An authentication process or use of private key strategy between the sender and receiver nodes can prevent to convince of any node by the attacker. The TPSN and FTSP both are multi-hop network and use tree-like structure so the root node could follow the authentication process or use the private key to propagate in the network. These approaches are a distributed approach in which all nodes take participation in synchronization.

The security aspects of time synchronization in a distributed approach was firstly discussed by Ganeriwal et al. [18] which discussed three types of attack, that is internal attack and external attack and pulse delay attack. The most difficult attack is a pulse delay attack in which an intruder in the moment of propagation of the packet arbitrarily produces delays that directly affect the synchronization accomplished.

The authors proposed the solution as the concept of secure pairwise synchronization. The integrity and authenticity of messages is assured in this protocol by using Message Authentication Codes (MAC) and a main Kxy shared between node x and y. By using this method, in the synchronization pulse or in the acknowledgment packet, attackers cannot alter any values. In addition, the attacker cannot suppose a node y identity because the Kxy secret key is not accessible.

An intruder can hear the packet across the wireless channel and produce authenticated packets in the future using the MAC. In this protocol, the attacks are identified by a compare the calculated message end-to-end delay D, and expected message delay D*. It can be observed that end delay calculation, D, becomes the protocol's auxiliary advantage. If the calculated delay exceeds the expected delay, discontinue the offset calculation [16].

It was also seen that an ARP poisoning attack and a selective delay attack can stop the clock synchronization. An attacker's by using the ARP poisoning attack changes the MAC address and targeting on Ethernet LAN by changing the ARP cache of the target node with a forged ARP request and response packets. ARP protocol used for the established relationship among the network layer and Data link-layer addresses, i.e., it setup the connection among the IP addresses and MAC addresses. By using the ARP poisoning attack, man-in-the-middle attack on the network is possible due to lack of authentication. The sender and receiver nodes believe they exchange data with each other in the ARP attack, but in reality they interact through the intruders.

The author has suggested two approaches to security alternatives, one against ARP poisoning and the other against delay imposing. Both kinds of solutions can be used for security against clock synchronization. The nodes encrypted all ARP messages in the first strategy, but it needed more computation in the nodes and also required additional delay to messages sending. In order to safeguard the ARP poisoning attack, the second strategy needed a control element validation server that could monitor and analyze it. The server can check the request and authenticate all the sensor node's ARP tables. Because managing all ARP tables in a big network can become difficult and failure of a single node server may stop the protection.

The average time synchronization protocol (ATS) is a distributed protocol based on fully consensus. It's not depend on any reference node or network topology that build it reliable for various types of attacks, such as DoS attack and node destruction, etc. The authors suggested that ATS is susceptible to attacks of message manipulation [13].

The ATS protocol requires a huge amount of data exchanges so when the network size increases due to this reason the converging speed heavily impacted may be slow down. The authors identified the effect of message manipulation attacks on ATS and suggested a required constrain for ATS to converge on secure ATS (SATS) protocol. Traditional ATS is extremely susceptible to attacks of manipulation of messages. The SATS provides an exponentially converging speed. The authors suggested the hardware clock checking method to avoid the hardware clock reading attacker corruption and the logical checking process to dynamically restrict the logical clock corruption of the attacker [19].

Douceur initially proposed the Sybil attack in peer-to peer networks [20]. He suggested it could affect distributed storage system's redundancy processes. After that systematically addressed the attack on Sybil and suggested how to protect Sybil's attack in sensor networks [9].

The Sybil attack is a problematic attack in which an intruder node acts by imitating other nodes or claiming fake identities because it has many nodes. An

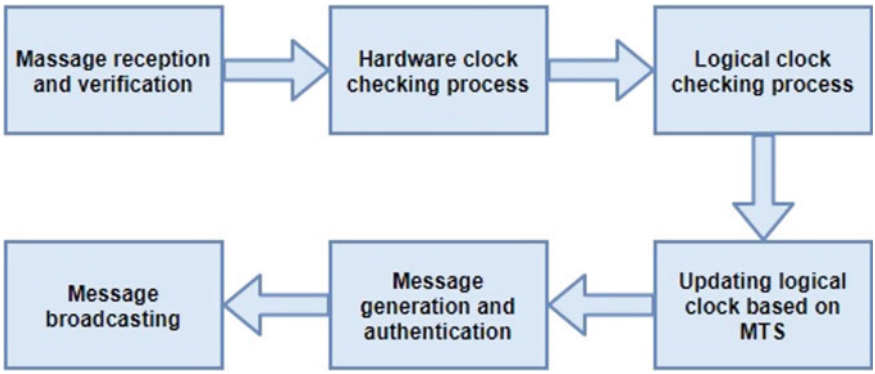


Fig. 20.8 SMTS architecture [6]

attacker can use one physical device to create an arbitrary amount of illegitimately numerous identities of an extra node. They suggested various defenses from the Sybil attack, such as radio resource testing, main pre-distribution validation for random key, position verification, and registration. The radio resource testing method has been shown to be more efficient by quantitative analysis since a malicious node can not spread concurrently on various channels.

Under message manipulation attack, the (MTS) protocol is not suitable. The protocol Secured maximum consensus time synchronization (SMTS) on the maximum consensus approach is introduced to identify and invalidate message manipulation attacks (Fig. 20.8).

Moreover, the SMTS guaranteed to converge at once of both clock skew and offset. The mainly two steps have been proposed that is hardware clock and logical clock checking processes, so it can identify and negate the possibility of message manipulation attacks. In message manipulation attack the attacker tampering the synchronization information and transmits fake synchronization messages by pretend itself as a safe node. By this method, the attacker node misleads the neighbor nodes and corrupts the synchronization [6].

These attacks also can be included as message manipulation attacks like replay attacks, fault data injection attacks, and delay the attack. The replay attack may be considered to add the negative time to the message; it is feasible to model delay attack as include a delay to the real message. Hardware clock's safeguard technique is suggested to check hardware clock procedures. Using the linear clock model, the Relative skew estimation algorithm checks the successive adjacent hardware measurements at each step, so that if the attacker exists, they can not readily alter the hardware reading for broadcast [6].

Rahman and El-Khatib [21] proposed a pairing and identity-based cryptography approach to secure time synchronization and decrease the transmission and storage capacity of each node. The suggested protocol is fully reliable against a replay attack, selective forward attack, wormhole attack, masquerade attack, message

manipulation attack, and delay the attack. The main concept behind this protocol is that each node in the network collects only the secret points from the base station over an elliptic curve at the time of deployment, allowing important space to be reduced by the suggested protocols. Any other intruder node cannot pass the authentication phase, so it is not permitted to enter the communication network. Nodes never store private or public keys from this protocol, the nodes produce their own secret on the fly key by exchanging their identity with adjacent nodes that are used with their communication neighbor for authentication reasons.

The authors proposed a Receiver only synchronization approach focus on PBS used PKC-based authentication scheme. Moreover, a PKC-based approach is resilient to compromise nodes, compared with the symmetric key based approach. The Elliptic Curve Cryptography is a type of PKC approach that shows the fast computation and more efficient for compact signatures and small key size. The idea behind the PBS is that while two nodes synchronized with each other, the nearby node overwhelming the other two and also synchronized with them by receiver only synchronization. Different types of an attack like Sybil attack, replay attack message manipulation attack, delay and wormhole attack, the misleading attack has been analyzed on pairwise broadcast synchronization [2] (Fig. 20.9).

A secure pairwise broadcast synchronization protocol (SPBS) has been proposed to address in PBS attack. These are the technique to analyze address attacks on

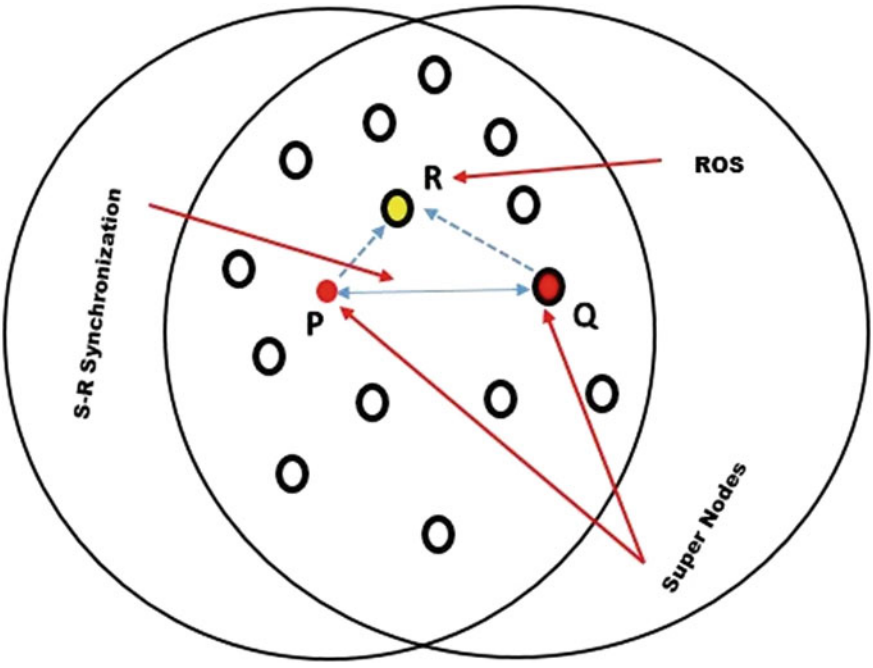


Fig. 20.9 Secure pairwise broadcast synchronization [3]

PBS. The SPBS depends on the PKC-based authentication scheme and Nonce techniques. If end-to-end calculated delay crosses a threshold value, then synchronization is strictly aborted. This paper focused on the defending technique from the Sybil attack in the distributed time synchronization. In Sybil attacks, the attacker node makes the various identities including actual identities, which provide the actual nodes a false neighbor information and impact on distributed storage, data aggregation and routing [22].

Many authors proposed different countermeasures on Sybil attacks as key management and neighboring time information. But these methods are not appropriate for WSN because they required complex computation, high storage and extra hardware resources. The Sybil attack on time synchronization disrupted the whole network and loses synchronization. Novel node-identification-based secure time synchronization (NiSTS) protocol has been explored to protect against Sybil attacks. The comparative skew checking mechanism is used in the design of NiSTS to identify forge messages. The proposed NiSTS protocol works separately into two parts: the detection process and clock update process upgrade the logical clock parameters build on a present clock synchronization algorithm to obtain time synchronization. Because its quick convergence and simultaneous compensation of the clock skew and offset, the MTS protocol is used as base paper. They conclude that both message manipulation attacks and Sybil attacks are being defended by NiSTS [23].

The RTSP, a Robust and secure Time Synchronization Protocol has been proposed to protect against Sybil attacks. It is based on ATS and MTS [16] to achieve synchronization since MTS achieves faster convergence. It adopts MAC-layer time stamp to remove source and sink side uncertainties. RTSP is a distributed synchronization protocol that is far better than centralized protocols in terms of security because the reference node failure doesn't break the synchronization service. It uses the graph-based strategy of fine grained detection system to attack detection not only at the message level but also at the node level. This makes it more reliable against Sybil attacks and message manipulation attacks.

RTSP protocol distinguishes between the legal timestamps and illegal timestamps in the network. RTSP uses a graph approach to identify legal or illegal timestamps from valid timestamps. This protocol not only detects intruder node under message manipulation attacks but also detects illegal timestamp. The RTSP consists of four main steps, i.e., message reception, anomaly detection, clock update, and message broadcast. The main approach is to conformation between valid or invalid timestamp to one another. For this novel graph technique, the maximum clique approach is adopted. If there will be an error like invalid node confirmation, the graph not able to build a max clique. All valid nodes form the max clique but if there will be any invalid node, the error occurs and clique will not build. That vertex which is not in the max clique may be considered as anomalies. Since the maximum clique finding in the graph is an NP-complete problem, yet authors also proposed many properties to make the maximum clique [8].

Table 20.1 Qualitative and quantitative analysis of time synchronization protocols for WSN

Qualitative metrics					Quantitative metrics		
Protocol	Approach	Message passing	Security aspects	Converging speed	Precision	Network size	Message complexity
RBS [9]	Centralized	Receiver to receiver	Node-based attack	High	29.1 ms per hop	20 nodes	$O(n)^2$
TPSN [10]	Centralized	Sender to receiver	Node-based attack	High	16.9 ms per hop	150–300	$O(n)^2$
FTSP [11]	Centralized	Tree-based	Root based attack	High	1.5 ms	60	–
ATSP [12]	Distributed	Consensus	Delay attack	Converge in a non-finite time	0.5 ms	10–20 nodes, 1–5 malicious nodes	O(2n)
ATS [13]	Distributed	Consensus	Message manipulation attack	Exponential	600 ms	9–35	–
SATS [19]	Distributed	Consensus	Message manipulation attack	Fast convergence	–	–	–
WMTS [16]	Distributed	Consensus	None	Converge in a non-finite time	–	–	–
RFA [14]	Distributed	All node-based	None	–	131 ms	2–20 nodes	–
PBS [22]	Distributed	Multi-hop	None	–	100 ms	200–400	$O(n)^2$
SMTS [6]	Distributed	Consensus	Message manipulation attack	Fast convergence	–	100 safe nodes, 5 attack nodes	–
RTSP [8]	Distributed	Consensus	Sybil attack	Exponential	–	100 nodes, 3 attack nodes	$O(n)^2$
NiSTS [23]	Distributed	Consensus	Sybil attack, message manipulation attack	Slow	–	30 nodes, 3 Sybil node	–

20.5 Key Observations and Analysis

The chapter shows the following observations regarding security threats in time synchronization for wireless sensor networks, which acts as the backbone network for IoT.

1. Wireless sensor network being a distributed system, it has no centralized physical clock, so synchronization is the main issue.
2. Sensor nodes being a backbone of IoT are deployed in a hostile environment to collect sensible data. This increases security threats to different protocols for IoT and so also for time synchronization.
3. Sensor nodes have restricted energy and storage capacity. So, the normal cryptography approach is not suitable, because it required more computation overhead. Simple and light-weight approaches should be developed to countermeasure security threats.
4. Synchronization protocols are more vulnerable to Sybil attack and message manipulation attacks.
5. The ATS protocol is vulnerable to the message manipulation attack, but SATS shows the exponential convergence and compensate both skew and offset.
6. The MTS protocol is also vulnerable to message manipulation attacks.
7. The SMTS demonstrates that the potential message manipulation attacks are to be defended and invalidated.
8. The RTSP protocol trying to identify Sybil attack using dynamic programming by finding max clique in Graph, but its time complexity is high, O (n^2) and max clique identification in the graph is an NP-complete problem.
9. NiSTS protocol defends against Sybil attack and message manipulation attacks.

Table 20.1 gives a brief overview of state-of-the-art time synchronization protocols for WSN with security as a major point of consideration along with other performance metrics.

20.6 Conclusions

The chapter focuses on security threats and their countermeasures for time synchronization protocols in traditional wireless sensor network which acts as a major backbone for IoT. Different types of time synchronization protocols under centralized and distributed approaches have been thoroughly studied with qualitative and quantitative analysis, emphasizing more on security aspects. In fact, time synchronization is a crucial issue for any distributed system, so also in IoT. Though a plethora of work has been carried out on time synchronization protocols in the last few decades, the security aspect is not considered in many of the state-of-the-art

protocols. Hence, this chapter will give a very useful insight into the research community to comprehend the importance of security issues in time synchronization problem in IoT which is an emerging paradigm of technology.

References

1. Lee, S.K., Bae, M., Kim, H.: Future of IoT networks: a survey. Appl. Sci. (2017)
2. Burhanuddin, M.A., Abdul-Jabbar Mohammed, A.: A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective. J. Telecommun. Electron. Comput. Eng. (open journal system) (2013)
3. Ahmad, B., Shiwei, M., Lin, L., Yang, S.: A cognitive global clock synchronization method in wireless sensor networks. J. Wireless Netw. Commun. 29–39 (2016)
4. Panigrahi, N.: Consensus-based time synchronization algorithms for wireless sensor networks with topological optimization strategies for performance improvement. PhD thesis
5. Dargie, W., Poellabauer, C.: Fundamentals of Wireless Sensor Networks: Theory and Practice. Wiley (2010)
6. He, J., Chen, J., Cheng, P., Cao, X.: Secure time synchronization in wireless sensor networks: a maximum consensus-based approach. IEEE Trans. Parallel Distrib. Comput. (2014)
7. Mills, D.L.: Internet time synchronization: the network time protocol. IEEE Trans. Commun. **39**(10), 1482–1493 (1991)
8. Dong, W., Liu, X.: Robust and secure time synchronization against Sybil attacks for sensor networks. IEEE Trans. Ind. Inform. (2015). https://doi.org/10.1109/tii.2015.2495147
9. Elson, J., Girod, L., Estrin, D.: Fine-grained network time synchronization using reference broadcasts. In: ACM SIGOPS Operating Systems Review – OSDI '02: Proceedings of the 5th Symposium on Operating Systems Design and Implementation, vol. 36 (SI), winter 2002 (2002)
10. Ganeriwal, S., Kumar, R., Srivastava, M.B.: Timing-sync protocol for sensor networks. In: SenSys '03 Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, pp. 138–149 (2003)
11. Maróti, M., Kusy, B., Simon, G., Lédeczi, A.: The flooding time synchronization protocol. In: Proceedings of 2nd International Conference on Embedded Networked Sensor Systems, pp. 39–49 (2014)
12. Hu, X., Park, T., Shin, K.G.: Attack-tolerant time-synchronization in wireless sensor networks. In: IEEE INFOCOM 2008 (2008)
13. Schenato, L., Fiorentin, F.: Average TimeSynch: a consensus-based protocol for clock synchronization in wireless sensor networks. Automatica **47**(9), 1878–1886 (2011)
14. Werner-Allen, G., Tewari, G., Patel, A., Welsh, M., Nagpal, R.: Firefly inspired sensor network synchronicity with realistic radio effects. In: Proceedings of ACM SenSys, pp. 142–153 (2005)
15. Sommer, P., Wattenhofer, R.: Gradient clock synchronization in wireless sensor networks. In: Proceedings of ACM/IEEE IPSN, pp. 37–48 (2009)
16. He, J., Cheng, P., Shi, L., Chen, J., Sun, Y.: Time synchronization in WSNs: a maximum-value-based consensus approach. IEEE Trans. Autom. Control **59**(3), 660–675 (2014)
17. Elson, J., Girod, L., Estrin, D.: Fine-grained network time synchronization using reference broadcasts. In: Proceedings of 5th USENIX Symposium on Operating System Design and Implementation (OSDI'02), pp. 147–163 (2002)
18. Ganeriwal, S., Capkun, S., Han, C.-C., Srivastava, M.B.: Secure Time Synchronization Service for Sensor Networks (2005)

19. He, J., Cheng, P., Shi, L., Chen, J.: SATS: secure average-consensus-based time synchronization in wireless sensor networks. IEEE Trans. Signal Process. **61**(24) (2013)
20. Douceur, J.R.: The Sybil attack. In: First International Workshop on Peer-to-Peer Systems (IPTPS '02) (2002)
21. Rahman, M., El-Khatib, K.: Secure time synchronization for wireless sensor networks based on bilinear pairing functions. IEEE Trans. Parallel Distrib. Syst. (2010)
22. Benzaid, C., Saiah, A., Badache, N.: Secure pairwise broadcast time synchronization in wireless sensor networks. In: Distributed Computing in Sensor Systems, 7th IEEE International Conference and Workshops, DCOSS 2011, Barcelona, Spain, 27–29 June, 2011 (2011)
23. Wang, Z., Zeng, P., Kong, L., Li, D., Jin, X.: Node-Identification-Based Secure Time Synchronization in Industrial Wireless Sensor Networks. MDPI (2018)

Chapter 21
Security Vulnerabilities and Issues of Traditional Wireless Sensors Networks in IoT

Bhanu chander and Kumaravelan Gopalakrishnan

Abstract From the past decade, Wireless sensor networks (WSNs) spread out significantly with the result of technological progress in hardware, software, and micro electro mechanical systems. With the enlargement of WSNs, great advances have been shaped in Internet-of-Things (IoT) by an ample variety of applications. IoT applications practiced in myriad phases include human life, ecological supervise, public wellbeing and medical behavior, smart shipping, traffic monitoring, smart cities, smart home applications, smart grid, and others. Mostly Internet of Things maintained with various sensing devices and technologies such as Sensors, GPS (Global positioning system), laser sensor, gas inductor, RFID (Radio-frequency identification devices), infrared sensor and many more, which collects large range features from the real world and send abstract feature objects which need to be monitored. Most of the devices are linked and interacted with more than one. The main idea behind IoT is to connect device-to-device, device-to-human, human-to-human. Development of IoT can make people live in a convenient way; however, it does not make sure the security of secret confidential information of its user. With a great collection of distribution, responsiveness and somewhat high processing capacity of IoT objects formed them as an optimal objective for cyber-attacks. So here some probabilities, secret confidential information may be a leak or stolen some point in time. Just once a sign of IoT device is captured or suspended it intention straightforwardly perturbs the security about whole information of IoT. Moreover, enormous IoT nodes accumulate a large amount of extensive prosperous, private information and process it, so its like lottery for cyber attackers to steal entire important data. Security obstacles like privacy, secure communication, access control, safe storage of data are becoming important tackles in the IoT domain. Hence, each solitary node that we positioned, each solitary device that we discover, each solitary byte that generated within the sphere of an IoT domain, at some point of time comes under inspection in the

Bhanu chander (✉) · Kumaravelan Gopalakrishnan
Computer Science and Engineering, Pondicherry University, Pondicherry 609605, India
e-mail: gujurothubhanu@gmail.com

Kumaravelan Gopalakrishnan
e-mail: gkumaravelanpu@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_21

course of the investigation. An IoT not including proper premeditated solutions for security issues it will principally limit its improvement. So securities, in particular, the ability to detect malicious nodes with preserving support of malicious activities appear as a priority in the successful employment of IoT networks. IoT has three dissimilar layers, each layers security approaches along with defensive methods are briefly described. Blockchain technology will progress the integrity in the real world shared data sets. Primarily blockchain applied in support of recording fiscal transactions where connections encoded (pre-arranged) and kept back with participants, on one occasion transaction confirmed by blockchain it cannot be modeled or else wipe out; if any modification is applied it is easy to map out and recognize. Blockchain technology position in IoT security, challenges, and Research problems in brief discussed.

Keywords Internet of Things · WSN · Security · Black chain · Integrity · Key management · Security measures

21.1 Introduction

The Internet of Things (IoT), one of the topmost modern technical knowledge that has drawn attention of industrial, scientific and academic fields. IoT continuously interconnects the physical and digital world into one heterogeneous system through the Internet. IoT heterogeneous system consists of a huge number of objects/Things, each object/things collect data from its surrounding environment and transfer them to other connected Things or central database storage through a communication channel. In this present Era internet of things revolutionize the life we exist—revolutionized means the way we work, how we make decisions, the way of transportation we doing, the way we live, the way of our healthcare management and the way how we obtain our energy, etc. [1–3]. IoT holds dissimilar objects refined sensor nodes, actuators, chips implanted into our surrounded physical things for making them smarter than ahead of. Moreover with the constant improvement in network technology, micro-electro-mechanical systems, wireless communications emerging modern world appliances demands slowly but surely enforced scope of internet of things applications from complex operations to intelligent transportation, traditional management tracking to intelligent control, smart home, weather forecasting, smart city, precision agriculture with supply water management and other domains. On the other hand, being as a new innovative technology IoT facing problems from numerous security issues. Compared with other standard technologies IoT security issues such as keeping transformed data and its way of transmissions are more challenging because of its complicated system surroundings and resource-constrained IoT devices. A lot of researchers presently working to make available efficient security solutions in IoT, most importantly on resource

constraints and scalability issues. In addition technologies like crypto-currency areas as Software-defined networking; Blockchain modernizes the mean of IoT regarding their scalability and effectiveness [3–5].

In the late 1950s the development of internet service has started after the innovations of electronic computer systems. In 1960s ARPANET a packet exchanged network introduced. In 1980s the concept of internet is introduced to all over the world through Transmission Control Protocol/ Internet Protocol (TCP/IP) standardization. In 1999 concept of the Internet of Things (IoT) was established because of tremendous development in wireless communication technology, sensor nodes, and Radio frequency identification (RFID) technologies. The main concepts of IoT are inter-connecting or integrate things/objects any-time, any-place and any-situation which entail things/objects like RFID tags, sensors, and actuators permit to interaction among the physical and virtual worlds. IoT is an expansion to prior traditional technologies and internet framework so former security forms should not be applicable to IoT in order to assurance for fundamental security services include integrity, authentication, non-reputation, availability, confidentiality and access control. Nonetheless, the Internet of things controlled through countless new characteristics such as IoT special operation environments, limited computational power, numerous things interacts together in a complex manner. Mostly IoT applications consist of numerous amounts of sensor nodes which leads to serious security problems [1–6].

21.1.1 Wireless Sensor Network

In view of the fact of rigorous development in the fields of micro-electro-mechanical systems, chip manufacture technologies, information and communication technologies, computer networks, wireless communications at the present minute we have an innovative communication as well as computation structural design acknowledged as wireless sensor network (WSN). WSN is a company of miniature nodes, the amount of sensor node may raise from hundreds to thousands depends on specific applications. Each sensor node individually collects its surrounding information and transform to one or more base/sink station through a communication link which was defined at the time of network deployment. Generally, sensor networks are application specific. The focal purpose of sensor networks design is real-time data compilation, scrutiny for low-level statistics in military surveillance and it was developed by US military research society in the 1950s [7–9]. By considering this as a reason WSN are well-matched for ample varieties of screening and supervision appliances like Traffic monitoring, smart home, machinery performances, forest fire monitoring, sea water levels, industrial quality control, patient health monitoring, observation of critical infrastructure, chemical laboratories, robotic works, agriculture, electronic grid monitoring, automobiles etc. But mostly sensor nodes deployed in unfriendly environments with dynamic intelligent opposition. Whereas sensor node employment in

unfriendly or inhospitable surroundings makes the sensor nodes vulnerable to various promising attacks, moreover limited resource constraints of sensor nodes easy for vulnerable attacks furthermore the conventional security solutions unworkable. For one specific application huge amount of sensor nodes are utilized out of them some sensor nodes may contain insufficient power and memory resources which are easy targets for attackers to attack and steal sensitive information apart from that sometimes attackers can gain the power to control the entire network. Nevertheless, the sensing technology with sufficient processing energy along with suitable wireless communication makes WSNs and IoTs profitable in great quantity on the coming future [4–11].

21.1.2 Explanation for WSNs to Be Attacked

There are some unique reasons for WSNs to be attacked by various eavesdroppers [2–6, 10, 11].

Large-scale deployment—Generally sensor network contains a huge amount of sensors, depending upon the application this number will raise hundreds to thousands in order to complete the assigned task. Means information transformed through many nodes in order to reach a suitable receiver, where classical security protocols may not work successfully in WSN. Furthermore, one particular sensor node may leak valuable sensitive information in relation to the complete network. **Wireless communication channel**—Wireless sensor node communicates through wireless communication channels such as Bluetooth, Radio frequencies, the attacker simply wishes to alter the frequencies to eavesdrop that being switch over among sensor nodes. **Resource limitations**—Sensor node is a tiny microelectronic device which incorporates of limited power, small storage database, insufficient communication bandwidth, and limited processing capabilities. Generally, computer network security mechanisms hang on some form of cryptography. Both symmetric and asymmetric keys are successful to provide security assurance but among them asymmetric key more multitalented security scheme comparative to symmetric key cartography. But in the view of a limited resource-constrained sensor node, above-mentioned procedures must be utilized on precise optimization algorithms on both designs as well as execution stage.

21.1.3 Security Goals for Traditional Sensor Networks

Sensor nodes mostly employed at complicated regions to collect sensitive information regarding particular regions where humans not able to construct a normal network. Sensor networks can also work ad hoc mode and defense goals cover mutually conventional networks along with goals suitable to the exclusive constraints of ad hoc sensor system [1–5, 7–11].

Data Confidentiality: Confidentiality presents that sensor node messages or information's approached by only those nodes make-believe to accept. So any message or information broadcast over the network is supposed to remain confidential. This part of the mechanism is a very key concern in sensor network protection; sensor node should not expose or exchange information with its surrounding neighbor's nodes without checking proper secure functionalities. In a sensor network, confidentiality provided by cryptographic techniques where sender node encrypts message or packets being sent and receiver nodes decrypt it. Depending on the purpose, encryption might be applied on the data part of a packet or full packet, here encryption of full packet help-out to confuse the sensor node recognition that can help to lessen the probability of an eavesdropper toward node identification being spoofed.

Data Authentication: Authentication ensures node toward making sure that the uniqueness of a new node with whom it wants to communicate as claimed. Means data authentication confirms both sender and receiver identity earlier than they send a message to communicate. Authentication guarantees the trustworthiness of message or packets as a result of validating source who broadcast to it. Moreover, it also supervises probabilities that packets or messages dishonestly introduced into the wireless testimonial tube which might be misguided for legitimate packets. Data authentication can be accomplished through applying symmetric and asymmetric key procedures but due to wireless network nature and broadcast media, it is exceptionally not easy to make sure authentication.

Data Integrity: Integrity in sensor network guarantees the truthfulness of message along with intelligence to confirm that the message has not distorted or tainted while in the transmission channel. For example, packets are interchanged while routing or data aggregation, if such nodes adapted or altered by any malevolent unit, the whole network will go into halt position. Present designed sensor network has fine secrecy measures; still, there is an opportunity that the information integrity has been negotiation by modifications such as malicious node presented in the network injects false data, wireless channel break or failure, etc. With the help of Message authentication code (MAC) technique, message alteration or modifications can find out.

Secure Localization: Effectiveness of sensor network depends on theirs capability to accurately, mechanically discover every node in that set-up. An invader with ease alters in-secured region information by means of exposure to fake strengths, replaying signals.

Data Availability: Availability in WSN indicates that WSN network provided resources must be available for the sensor node to communicate a message when it needed. Frankly WSN network must be positive at all the scenarios and produce services whenever required. Nevertheless, failures of sink/base/cluster node earlier or later threaten the whole sensor network. Make sure trustworthiness on node and network stage is the one solution for achieving something availability but implementing network is not in favor to dissimilar types of Denial of service (DOS) attack which is very crucial in order to get definite availability of the WSN.

Self-organization: Senor Node in WSN cannot be monitored or maintained after employment. Sensor network characteristically like an unplanned network, it need each sensor node must flexible, self-governing, self-healing as reported to dissimilar state of affairs. Till now there is no predetermined infrastructure existed, this inherent characteristic makes a huge dispute to WSN safety. If self-governing is not available in sensor network the harm resulting from molests or else uncertain atmosphere might be divested.

Data Freshness: Data freshness makes sure that data or information that came is a recent one and make sure that no previous messages have been repeated. Generally, the WSN network, depending on the appliances continuously or periodically sense or forward data from the surrounding atmosphere or advances information in reaction toward the definite event. In these above-mentioned scenarios, sensor sensed data reach base/sink node as soon as possible. Data freshness archived through reliable transport and routing schemes, a Nonce value and time-related counters.

Time-synchronization: Mostly sensor network appliances have some kind of time synchronization at the time of network deployment. Moreover, some sensor nodes could estimate source-to-source detain of a packet as it transit among paired sensor nodes in order to confirm the security measurements. High collaborate sensor network may possibly need a collective association with tracking appliances.

21.2 Attacks on Traditional Wireless Sensor Network

Wireless sensor network employed in harsh environments collects real-world valuable raw sensed information in the form of sensed data according to the required appliance. Because of its wide range of characteristics WSN used in many appliances from indoor to outdoor. Although transmitting information in a WSN is essential to endow with security. Providing appropriate security is one of the major difficult tasks in WSN at the same time it is also not an easy task to keep watch on a sensor node or sensor network continuously. However, it must design an appropriate security mechanism while data in the transmission medium to avoid intruder/attacker. Ultimately, because of sensor nodes limited resource constraints encryption, decryption techniques not so useful which need good quality power and processing resources. WSNs defenseless against many attacks such as invaders can attack radio transmission, add their own data, reply old message packets or simply drop them before reach destination. The invader can also deploy some malicious nodes in the sensor network with the same capabilities of a normally deployed node and try to overwrite them. A first-rate secure network must be ought to support all security properties [1–5, 7–11].

Based on the status of damage or on which state or else status of attackers access the network, attacks separated as passive attacks and active attacks. In a passive attack, an attacker/invader collects sensitive information through silent monitoring or access the data without modifying it without any interrupt of actual

communication procedure. Coming to active attacks, attacker intentionally disturbs the actual communication by adding faulty data, sometimes entirely spoils the network working process. Furthermore, an attacker who does not have any access with deployed sensor network but still wants to damage the network called as external attacks or outcast attacks. These malicious nodes take part and participate in this kind of attack are not part of the network. The node which is positioned inside the network and tries to steal information is called an insider attack. These kinds of nodes are truly a part of the employed sensor network. Compared to outsider attacks, insider attacks are more dangerous moreover they know crucial information and have all categories of access rights.

Some hearts of security attacks on WSN and sensor node are displayed below (See Fig 21.1) [7–11]:

Denial of service attack: Denial of service (DoS) attacks which disturb, destroy, diminishes and try to shrink network power to complete estimated functions. Attackers continuously send false requests to network systems so that network is not available to communicate with legitimated users in that network. For the reason sensor node limited resource constraints which make easy for attackers attack with DoS, most of the sensor nodes largely affected with this kind attack system. In literature numerous standard procedures are available to deal with some or more complicated DoS attacks; most of the designed procedures need high computational problem, power sources which not appropriate on behalf of resource constrained WSNs. Moreover, some DoS attacks particularly in WSNs proven expensive; the research community needs to spend great attempt toward classify various nature DoS attacks and formulate stratagem to secure against attacks. However, for a good judgment development of generic security method in opposition to DoS attacks is still be an open research dispute.

Sybil Attack: In this attack, the attacker presents one single sensor node with multiple identifications to other sensor nodes in that sensor network. Simply attacker generates a situation like a sensor node can be more than one place at a time. Sybil attack applied to attack various kinds of protocol standards. Location-based protocols, voting, routing algorithms, misbehaviors detection, fair resources allocation, and data aggregations are some of them, each and every one of the mentioned techniques employed with multiple identities. For instance attack on routing– Sybil attack depends on malevolent node captivating on the personality of numerous nodes, hence routing various multiple pathways throughout a solitary malevolent node.

Hello flood attack: Generally in WSN, protocols make use of the HELLO packet or messages in order to convey the receiving node that sender node of the packet within its broadcast range. In clear words, dispatcher of that packet is surrounded by the recipient. In HELLO flood attack, an attacker generates packets with high-power transmission and throw them to idiotic outsized amount of nodes and formulates them to think that they surrounded by its territory region. The malevolent node who receives these packets sends the sensed data packets to the attacker. Consequently, attacker node misleadingly transmits a simple shot route toward the base station and every node those receive HELLO packets attempt to

transmit toward the malevolent node. An attacker can change, modify or simply drops the packets. This type of attack is one of the difficult attacks on WSNs, which causes lots of energy to lose any chance to network jamming occurrence.

Wormhole attack: In wormhole attack, attacker records information on solitary locality in the network, transform to a new locality through low latency tunnel. Wormhole attack is very hard to detect and defend in WSNs. The link or tunnel could be fixed by the use of solitary node broadcasts packets among two adjoining non-neighbor nodes, or else by two same nodes placed in dissimilar locations of the network and communicate mutually. Whenever sender node forwards information, one of the malicious/compromised node tunnels information to another compromised node. After getting information, received compromised node broadcasts information to its adjacent nodes which positioned at a distance of one/two hops but actual distance among these two is multiple hops.

Selective forwarding attack: Accumulated information of a sensor node broadcasts to the sink/base node by the multi-hop process. If all the connected nodes broadcast the sensed data in a correct way then network communication is good. But an attacker can disturb communication by compromise one of the node in such a way that selectively promotes a small amount of messages and deliver messages with long routing process sometimes simply drops them. In such scenarios, adjacent nodes assume as failed communication and search for the new route.

Sinkhole attack: In Sinkhole attack, an invader generates a conceded node which eye-catching to adjacent nodes and advertises fake routing information to invite almost every ones traffic of selective region transform via it. As an end result, adjacent nodes choose that conceded eye-catching node as their next step to route their data in that network.

Spoofed routing information: In this, assailant straightforwardly attacks routing protocol working procedure where each compromised sensor node stated as a router. The attacker is able to create, later change routing loops, create false as well as error messages and enlarge end-to-end latency.

Black hole attack: In this attack, an attacker creates malevolent nodes at some stage in the path-finding a procedure or in routing table updating which announce the shortest path or better suitable pathway to reach the target node. The main intention of the attacker is to stop all sensed packets to reach the destination node. Sometimes hold the path-finding process to make packets to reach late.

Camouflage Adversaries: In camouflage adversaries, an assailant may possibly introduce their malicious node or compromise a sensor node to conceal in the network. Later than these nodes can replicate as regular nodes and advertises fake routing information, in addition, invite packets starting adjacent nodes in support of additional forward where secrecy investigation on packets might be carried out systematically.

Byzantine attack: A Byzantine attack in WSN is very difficult to recognize for the reason that these attacks do not show signs of any uncharacteristic activities. Single malicious node or collection of malicious nodes work in collusion way and obtain attacks like forwarding packets to long-range destinations route, creating routing loops, selectively tumbling packets, etc.

Acknowledgment spoofing: Sensor nodes sensed information broadcast to concede destination by appropriate routing procedures. Some routing protocols applied in WSNs need acknowledgment of transmitted packets. Some malicious node performs false acknowledgment to the nodes. The most important purpose of this attack is to make the sender satisfy that dead or lifeless node is still alive. After that sender continuously transmits information to the dead node which causes information loses.

Information disclosure: In this, a malicious node may possibly disclose private or momentous information to illegitimate nodes. Localization of nodes, routing technology that applied, the topology of network and type of information created, etc. are some of them in information disclosure attack.

Tampering: Employment of sensor network mostly placed in unattended or dangerous environments where they can easily vulnerable to physical attacks because of distributed nature. In tampering attack, an attacker pullout cryptographic key from captured sensor node moreover changes made on program codes, altered or replace it with a compromised node.

Traffic analysis attack: The major aim of attack, to continuously monitor the traffic stream among two entities for assembling specific knowledge about message strength, message encryption techniques, message frequency, the pattern of message and communication frequency. By implementing a traffic analysis attack, the attacker can know some specific sensor nodes with exceptional activities as well as events in the sensor network. For instance, if there is a rapid boost message exchanging between two nodes, indicates that nodes contain a few special actions to check or keep an eye on.

Node replication attack: As the name suggested an attacker generates one cloned node by doubling the ID of an already connected node with the network. This cloned node act exactly as original nodes and build severe damage to the sensor network. Sensed data packets despoiled or misrouted which shows the end result as fake sensor reading moreover disconnect network setup. There is a massive probability if an invader can achieve physical access of complete network, can replicate cryptographic keys of sensor nodes after that invader can straightforwardly influence a specified segment of the set-up or disconnects it in total.

Flooding: In this, an attacker continuously forwards a fresh connection establishment appeals until the resources those essential for each connection drained or reaches maximum edging state. After that, those request sent by the legitimated sensor will be ignored.

Node Malfunction: In this type of attack, the attacker generated malfunctioning node produce erroneous packets that could expose the truthfulness of the sensor network. This type of attack mostly applied to data aggregator nodes like a cluster head or base station.

Reply attack: In this, an invader interrupts the transformation process of a message and retransmits the same message in the future. By doing this attacker can reduce the bandwidth of the network. Nonce values or timestamps with suitable encryption algorithms are implemented to avoid these types of attacks.

Jamming Attack: In jamming attack, attacker obstructs with radio communication consumed in the network. Jamming source is powerful to perturbs the complete network even an attacker can able to perturb the entire network with low jamming power resources by intentionally influencing jamming resources. Moreover, jamming can proficiently use excessive power at each node by establishing bad-mannered packets; here receipts nodes will also consume power by getting those packets.

False Node: In this, a false node injected by an attacker involves in adding malicious data packets moreover it can able to prevent true data from the network. Adding wicked node to the existed network is one of the worst and most dangerous attacks that can stretch all over the network and potentially destroy entire network set-up moreover sometimes taking over the network on behalf of an attacker.

Resource-depletion attack: Malicious node make an effort to reduce the resources constraints of remaining nodes in that network. Computational power, bandwidth, and battery power are some of the listed resources under attack by this attack.

Monitor and Eavesdropping: This type of attack is nearly regular in WSNs which effects on data privacy directly. Particularly in WSNs those packets which enclose control information expresses more information than reached or gathered via location server, by eavesdrop or snooping on these messages confirms more helpful and easily determine the message contents for an enemy. If the messages encrypted with talented cryptographic methods can only solve this problem.

De-synchronization: De-synchronization indicates to disturb accessible connection as a result of repetitively sending spoof messages to a destination for retransmission of misplaced frames.

21.3 Secure Architecture and Security Challenges in IoT

21.3.1 Security Architecture of IoT

Internet of Things (IoT) has different applications; each application has dissimilar industrial standards and interconnected network standards. As noted in the above introduction, natural IoT service system contains heterogeneous devices with implanted sensor nodes, things, devices interconnected through an internet network. Each implanted thing in IoT uniquely identifiable moreover most of them characterized by limited memory, limited processing capability and small available memory. These IoT devices through employed gateways connect with the external world for isolated data as well as services to IoT abusers. Till now there is no standard, unified structure for IoT was shaped. Nonetheless, in the view of IoT security standards, several individual institutes have issued minimum standards like ETSI, IEEE, etc. Many of the existing IoT solutions have self-governing small networks where reasonably few mechanisms can be attacked. But for the reason of

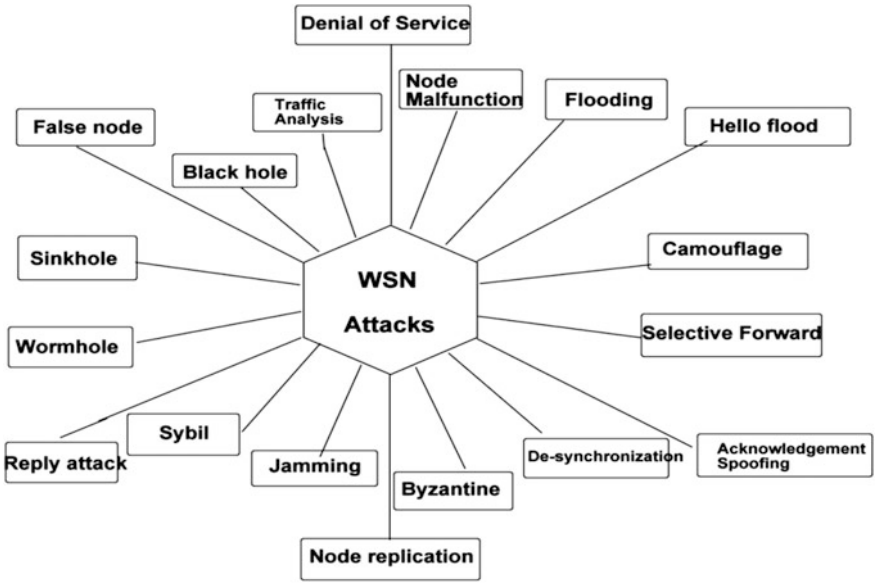


Fig. 21.1 Pictorial strategy of various attacks on traditional WSN

continuous enlargement of IoT, these tiny networks will unite into an outsized network. As a result of this, it might be more and more complicated to guarantee the security. Resolving these security troubles would be the key reason to make a decision on the potential development of the Internet of Things. Compared security issues of mobile communication networks, sensor networks, and internet networks, IoT has the equivalent issues furthermore it has additional security mechanisms such as information storage, different authentication processes, privacy issues and access control and network management so on. Among these list data security and privacy protection are major challenges in modern IoT system moreover these mechanisms decide the future growth of IoT appliances [12–14].

In IoT, both Radio Frequency Identification Devices (RFID) and Wireless Sensor Networks (WSNs) assure integrity and confidentiality of information through cryptographic password technology. Determined access control, as well as authentication, completes the communication within two entities moreover confirm each other's genuine identification and validity of the transmitted information. IoT system is a combination of multiple heterogeneous networks where it must be dealt against competitiveness concerns among connected network systems that prone to security problems. Most of the IoT devices/things continuously displaced from one place to another place where building trust among them is a very difficult task. However, this will be solved by implementing standard routing and key management protocols. In view of uninterrupted data transmission, there are easy chances for network congestion. Hence while employment of IoT system formulates

consideration on connectivity and capacity issues like as address spaces. Ipv6, WLAN technologies affect IoT transport security. IoT applications straightforwardly associate with human's daily life, hence need for stronger human-security consciousness and types of individual activities at the similar time [13–16].

The security structural design of IoT separated into three layers namely perception layer, transportation layer and application layer. Designed IoT must make sure the safety measures of all the three mentioned layers. RFID security, Wireless network security, a combination of both RSN securities comes under perception layer. Coming to transport layer security LAN security, 2G/3G/4G access network security and Wi-Fi security, etc. Middleware technology security, Service support platform security, Cloud computing security moreover some new information platform security placed under the application layer. More interestingly IoT appliances in special manufacturer companies have different appliance necessities. Hence, overall networking security turns to be huge multiple layered security structure. Finally, IoT security system takes a description of overall system crossing from perception layer, transport layer as well as application layer [12–16].

21.3.2 Security Challenges in IoT

Efficient solutions for massive heterogeneous data: An IoT service creates continuous gigantic heterogeneous information. So it is taken as one of the most important research problems and needs to find a proficient approach to deal with this gigantic information so that we can accomplish a more ample security solution for the complete appliance linked to IoT scheme. **The overall security architecture of entire IoT system**: Internet of Things is an application specific. Based on dissimilar application frameworks and respective security requirements, necessitate designing appropriate security architecture. It indicates that security architectures for IoT system are specially made for an individual problem which is not intelligent to handle all security issues. However, there is a chance to build top-phase security architecture for IoT with the help of ideas from software engineering. Try to build a security design that affords security adapters with dissimilar appliances, explicit algorithms to swap information via the existing top-phase safety algorithm. **Lightweight security solutions**: Most of IoT devices/things have limited resources constraints, so designing lightweight security solution is always useful thought moreover that will direct towards future innovations. Hence, try to propose trivial solutions for IoT arrangement like key managing; exact confirmation and access control moreover ensure that designed solution congregate the definite necessities of specific applications [12–16].

21.4 Layer-Wise Security Issues Analysis of IoT

Internet of Things still now not has a standard architecture design. But the planned architecture must have the three characteristics namely *Comprehensive perception*—Employed sensor nodes in the perception layer achieve entity information any-time/any-where/any-situation. *Reliable transmission*—accumulated information of entities transferred to the respective data center through wireless communication channel completely and safely. *Intelligent processing*—middleware analysis procedure which deal with the composed information earlier than submitting to the appliance terminal [3].

21.4.1 Perception Layer Security Concerns

As discussed above perception layer essentially work on the subject of information collection, objects/things control. The composed data of perception layer transformed to network layer through gateway or controller. RFID, WSNs, RSN, etc. some technologies applicable in perception layer. Below each techniques security issues and defenses are discussed [3, 7, 10, 11, 17–20].

Radio Frequency Identifier (RFID) security issues: Radio frequency identifier (RFID) is an automated identification skill which mechanically recognizes the target tag signal with appropriate data. With this specification RFID technology widely used in a various harsh, insensitive atmosphere. However, RFID exposes to lots of issues because when the sensor data is composed, the way of data transmit is wireless technology. Most of the IoT devices employed in complicated monitoring areas, where the transmitted signals effortlessly monitored, disturbed and intercepted moreover gain access to the equipment control or damage. RFID, as well as WSNs both, are important constraints for information transmission so here we mentioned each techniques security problems and defensive mechanisms separately [3, 21].

Uniform coding—Till now there is no uniform coding standard for RFID tag, this problem will cause issues like the receiver cannot able to read tag information, the possibility for error occurrences. The universal identifier is one of the RFID technology which was mostly used in nowadays. Presently there are two RFID collisions namely *Tags collision*—readers have a huge amount of label but unable to access the data transmission in the right manner or sufficiently well. Various readers supportive work important in IoT but in some circumstances, effective capacity of readers may overlaps, which will results in an increase the load of the transmission on the network which describe as readers. *Conflict collision*—with the help of multiple RFID tags additional data transmitted to the receiver at a time, but this may reason for the reader not capable to read or access the information appropriately [22, 23].

RFID Defensive methods: An RFID tag has limited resource constraints such as limited storage facility, weak processing, and computational potentialities. So the designed system needs trivial explanations for privacy safeguard. Data privacy in RFID security separated into *physical based schemes*—antenna energy analysis, block tags, pseudonyms tags and clip tags, etc. *password-based schemes*—cryptographic techniques, hash locks, etc. Location privacy in RFID security is very important because RFID tags does not store any intelligence although attackers are able to find tag knowledge used to track product/object location. Trust management is the main functionality in IoT, it exists between reader and tags, and it has more importance when it comes between reader and base station. Digital signature based cryptographic techniques significantly used in trust management but the issue is traditional cryptographic techniques require high computation, storage capacity. So while designing security, privacy and trust management of RFID, researchers must consider storage and computation capacity which have limited resource constraints [17–20].

Wireless sensor networks security issues and defenses: As discussed above, the role of perception layer is to collect information, so while collecting information through sensor node, information may be subjected to attacks such as message tampering, miss routing, message drops, injecting false data which affect the security of IoT [2, 3].

Cryptographic techniques in WSNs: Wireless sensor network exposes in many application areas, where network requirements like data security, confidentiality and privacy issues solved with cryptography. Asymmetric key encryption algorithms difficult to apply in WSNs which need more computational and storage capacity those are not available. However, symmetric key encryption procedures have some problems—key exchange protocol, complexity on key confidentiality, problematic message authentication and digital signature. These above-mentioned issues turn people to choose asymmetric or public key encryption algorithms for WSNs security and privacy. Compared to symmetric algorithms it has good scalability, with no, necessitates of complex key management procedure, notably, it is very well-situated for node validation. Symmetric, as well as asymmetric encryption techniques, have their own advantages—symmetric key algorithm reasonably excellent but security strength is no so high, asymmetric key algorithm provide superior high security but problems in hardware, well-made algorithms, and suitable parameters trim down the quantity of power expenditure [2, 24–27].

Key management in WSN—The most important objective of key management is security in key generation and updating algorithm, distribution and storage, forward and backward privacy against the source authentication, freshness and collision attacks. Among this key distribution is very important, it consists handling of a public key and secret key, toward guarantee key transportation plus circulated steadily directed toward genuine abusers. There are four key-distributions available in WSNs namely ***key pre-distribution agreement***—Before node employment master key shared among the node and base/sink station in the shape of pre-distribution. ***Key broadcast distribution***—This set-up is mainly applicable in asymmetric key distribution where the key for station security, broadcast

information to all the nodes. ***Distribution of key between two nodes***—The key which was shared among nodes is referred to as key shared among two nodes. It is mainly utilized to resolve security crisis connections among bordering nodes. ***Group key distribution***—Group-key which exploited to protect exchanges among several nodes in a similar group. Depending on application sensor node network creates an inner network which consists of several nodes. What are the instructions to propose a trivial secret key sharing method on the source of the sensor nodes through restricted distribution scheme and sensor nodes with partial resources? On the way to sustain every level of protocols, appliances and services safety is most important trouble. Combining asymmetric and symmetric key methods provides make use of both compensations to accomplish key distribution design which is also in progress [2, 28–32].

Routing security issues and defenses: Routing plays huge responsibility while data transmission in WSNs. Attacks on general routing protocols may straightforwardly lead to the diversion of the entire network. In general, the well-organized secure routing protocol follows multiple hops routing, key mechanism, clustering mechanism, etc. Secure routing protocols provide authenticated routing information which is most important for authentication in information transmission. Sensor protocol for information via negotiation (SPINS) security structure for WSNs secure routing technology, Secure Network Encryption Protocol (SNEP) protocol for ensuring secrecy, integrity, and freshness. Micro Timed Efficient Streaming Loss-tolerant Authentication Protocol (μTESLA) is resourceful stream authentication protocol that base on time are some popular WSNs routing technologies [2, 33–35].

Robust Security Network (RSN) or Heterogeneous network integration: IoT is a heterogeneous network of various devices where a huge amount of distributed data is collected continuously. Data which was collected from dissimilar network standards in dissimilar ways constantly in different formats. Analysis of this data is omnipotent work moreover data may lose, destroyed and compromise; nodes collected data may be captured or stolen if there is no appropriate integration technique finally that results into a security, privacy issue. Integration of RFID and WSN networks is named as Robust Security Network (RSN) which utilized to resolve the crisis caused by heterogeneous data. Because both RFID and WSN has their own protocols and standards which advances to harmonious controversies in data formats and communication protocols. Moreover, RFID and ESNs have dissimilar data storage formats, dissimilar security supervise mechanisms, dissimilar data access formats and dissimilar applications furthermore both technologies have dissimilar data preprocessing methods such as aggregation, filtering, and clustering, etc. In IoT environment RFID features to large number nodes where dissimilar nodes have dissimilar radio capabilities, processing procedures, and power utilization. Subsequently, WSNs nodes employ in harsh environments, extra nodes may add or delete after network deployment and nodes will not stand for a long epoch of time. So researchers need to concentrate on data access formats, data storage formats and data processing procedures in the view of security control [2, 3, 36, 37].

21.4.2 Transportation Layer Security Concerns

Wi-Fi security issues: It is also known as IEEE 802.11 or Wireless Fidelity, which is wireless network access arrangement where intermediate, allied to each other's through wireless. In IoT, devices utilize Wi-Fi mechanisms in applications like accessing the internet via Wi-Fi web, accessing emails, downloads, online gaming and watching videos, etc. Network security is a major dispute in Wi-Fi, whenever a user tries to access internet web-page; it is likely to compromise and store user profile and passwords. Access control plus network encryption are the two key procedures to resolve the protection problems of Wi-Fi. Only legitimate abusers can approach the Wi-Fi network is termed as access control. Only the beneficiary who can decrypt in the approved manner can recognize the data substance is termed as Network encryption [2, 3, 38, 39].

Ad Hoc security: Wireless Ad hoc set-up was a collection of independent sensors or stations shaped as self-organizing, self-management and independent predetermined communications which utilize distributed network administration. In IoT, ad hoc network eliminates heterogeneous among perception layer through Ad hoc network routing protocol. Security threats for Ad hoc set-up are radio channel (easily vulnerable to eavesdropping) and network interferences. Moreover, each node should capable to confirm the identity of other adjacent nodes; certification technology can provide the identity of node whether it is legitimate or illegitimate. Authentication and key management also resolve this concern [2, 3, 29, 40, 41].

3G Networks: The 3G network has similar issues as WSN and Ad hoc networks, additionally it has the following security problems those are information incompleteness, information leakage, and illegitimate attacks, etc. Data encryption, key management techniques, data source authentication and confidential information maintenance by the user could save from above-mentioned security issues [2, 3, 42].

Local area network (LAN): Wireless LAN has a responsibility regarding information leakage and servers independent protection. Security problems of Wireless local area network like an injection of malicious code, unnecessary OS services can protect with help of secure password mechanisms [2, 3, 43].

21.4.3 Application Layer

In the application layer, according to dissimilar industrials and applicable environments, its security issues are also different. The application layer in IoT supports all the business services moreover understands intelligent resources computation, screening, choosing, fabricating and handing-out data. Application support layer able to detect legitimate data, malicious data and spam data moreover filter the system in real-time. The application layer in IoT can be organized as Machine-Machine mode of IoT (M2M-IoT), cloud computing and middleware [2, 3].

Machine-Machine is popular IoT application module but still faces issues in security because the information transfer performed base on electric chain, mobile and wireless network. Information collected and transmitted in IoT services was huge and energetic, hence middleware must have massive capacity moreover it must be linearly scalable in order to store ever-increasing data. Both application backend and middleware need to gratify high protection necessities. Furthermore, confidentiality and consistency are the other two essential worrying concerns in IoT. Cloud computing platform has numerous security issues such as the possibility of data isolation, risk of management agencies, the threat of data recovery, the hazard of long-term development and the threat of priority process. Cloud computing stage encrypts data as well as backing user's data which will not erase until a definite amount of instant [44, 45].

Intelligent transportation system (ITS): Intelligent transportation in IoT is broadly exploited in logistic industry. It represents the next generation shipping with the target of associate people, roads along with intellectual vehicles and communication technologies. Here the implementation of ITS consist sorting, sending, receiving and transfer with other interlinked systems. Through linking, dispensing intellectual creative processors in the interior of vehicles from all the way through transportation communications, it is possible to build the transportation invulnerable greener and well-situated. RFID technologies on objects transport utilize GPS; through GSM/CDMA provides objects positions headed to the data center. However, RFID systems equivalent as internet and the ultimate severe data security hazard of RFID scheme is data/information loss. The electronic tag could enclose interior or individual information like production bunch number, individual characteristics plus shopping habits. There are many security challenges on transportation system vehicular networks stripped to every type of attacks, changes in topology made frequently which makes security solutions highly challengeable. **Smart home issues**: the development of innovative intelligent home-based system consists of sensors, internet and intellectual control it can offer a proficient, comfortable, protected, suitable, ecologically friendly living surroundings. For instance, when a guest approaches the sensors on door unlock mechanically and turn off after guests go away. The principally useful technologies of intelligent home scheme consist of communication, mobile technology, and network control. **Mobile terminal technology**: mobile intellectual devices such as Personal computers, Smartphone's and their major security issues is eavesdropping and DDOS attacks which occurs during transmission of 3G/4G. There is numerous security issues on this layer such as security threats, investigate audit issues and attack issues. **Communication technology**: in communication technology we have both wired and wireless machinery the majority of them full-fledged like Bluetooth base wireless communication skill for patient health and smart-home services. Because of miniature power and further area coverage features in intelligent home systems will turn out to be another emphasize [46–48].

Present digital world, IoT is growing faster and faster as well as there are numerous security concerns also needed to be explained. Security concerns for IoT cannot be complete by just deposit solutions for all sub-layers mutually. IoT has

dissimilar applications base on that it has dissimilar security requirements. In order to present the most excellent safety measures must be set special weights from special appliances. Researchers not simply deal with single layer mixed concerns but also necessitate dealing with cross-layer mixed concerns. Need to find a new-fangled technique to meet the system amalgamation representation that has the capability to congregate the cross-layer constraint, as a result, it provides identical data across different special layers [2, 3].

21.5 Blockchain Technology in IoT

IoT expansion expeditiously rising in distinctive fields outset from smart devices to smart cities, smart society and internet of Everything (IoET), Battlefield-based IoT (IoBT), Internet of medical things (IoMT), improvement smart grids, etc. Because of their respective commonness, frequency and popularities of such devices and services security and privacy are the two foremost essential concerns in IoT. Moreover, fields like IoMT and IoBT which consists of data-flexibility appliances ensure the security of devices, systems moreover data computing is decisive [49–52]. Internet of Things positioned us at the digital world with numerous advantages than prior. Conversely, incomplete security as well as trust management of IoT limits its adoption in modern appliances. Traditional cryptography technologies not sufficient to address security along with privacy disputes in IoT because of devices or sensors utilized in IoT are limited resource constraints. Internet-based IoT intrinsically insecure, data security was a postscript while designing, security is noticeable from frequent links and physical handlings. More importantly, IoT service system has considerably dissimilar architectures starting from the internet; enlarge network connections as well as computations obstacle to objects with restricted computation powers like electrical devices, sensor nodes with minimal human interventions. In most of the scenarios collected data exchanged by mentioned IoT devices, stored at dissimilar servers transversely in a cloud and process, access in a dispersed manner. Nonetheless, cloud services insecurity from internet moreover prone to cyber molests such as SQL injection, vulnerable to single node failure, data tampering, data integrity, confidentiality, and availability, etc.

The contemporary IoT solutions result in security risks, easy vulnerabilities and cyber attacks which should be explored appropriately. Moreover, IoT nodes typically have little power which not suitable computation qualifications. For the reasons, conventional protection procedures lavish for little-powered IoT gadgets. More importantly existing work on cyber-attacks formed on centralized networks, which might not fit for absolutely centralized IoT systems. Hence in order to get out from cyber attacks, IoT needs scalable, lightweight and distributed solutions. Blockchain expertise is capable to protect the security, privacy of IoT abusers with the extremely decentralized background. Moreover, blockchain also identifies and implement a dissimilar level of access rules to limit unofficial functions on data

produce through IoT devices. Present two important functions in working of blockchain, first one—transactions generated by the user in the system. Second—transaction records in blocks must be in sequence order and not changed [53–65].

21.5.1 Blockchain Basic Word List

The hurried development of blockchain technology and blockchain involved appliances have begun to revolutionize digital worlds financial services. At present, the appliances of blockchain raise from a financial transaction or insurance claim to issues in share trades and corporate bonds. In presumption, any-person any-place can utilize blockchain technology to broadcast information/data steadfastly. Compared to other traditional transactional techniques like batch-oriented and linear, blockchain has compound transaction confirmation specifications where multiple parties engage in that. This involvement process efficiently removes single point failure of convolution data interchange systems. All parties have discern-ability toward what kind of function is going on, what is simulated, synchronized and replicated across the multiple geographic locations. More interestingly information or data is not able to be forfeited, which means data cannot be modified or deleted that makes it a well-dressed contract [53, 54].

Blockchain technology is kind of distributed ledger knowledge that efficiently removes the central data point rather than most commonly used supply chains data structures. Here, distributed ledger knowledge/technology is the heart of blockchain mechanism, which offers validation method via a network of computers that make possible peer-to-peer connections devoid-of the requirement for mediator/centralized supremacy to inform and manage the information engender by the transactions. The entire and every transaction in blockchain technology authenticate through a group of authorized transaction operations, which were involved as a fresh block to a previously existed chain of transaction operations, because of this reason it named as Block-chain. Just the once a transaction fixed, joined to chain transaction it cannot be modified, distorted or deleted. Notably, there are two most successful blockchain networks available—public or permission-less blockchain networks—Each user can individually access and perform much like open source network, permission blockchain networks—specific individuals or organizations use to conduct transaction operations [53–56].

Blockchain: Blockchain defined as a peer-to-peer intelligence ledger of dealings which might be in publicly or privately dispersed to the entire customers or participants in a decentralized form. It uses cryptography mechanism and an agreement to authenticate transactions/dealings which guarantees the authority of transactions avoid double-spending and permit for high-value transaction dealings in a suspected atmosphere. Moreover, it suggests precision as well as abolishes the need for intermediaries/third-parties administrators.

Virtual currency: Virtual currency is not like as fiat currency, it is a digital illustration of assessment that could digitally operate, also serviced as a component

entity of store-value. Digital coins or digital tokens are some examples of virtual currency.

Distributed ledger technology: Distributed ledger technology (DLT) typically known as distributed, decentralized ledger characteristic of blockchain. Not like centralized authority, in the company of DLT, a ledger can able to maintain secured, authenticated as a result of relying on a decentralized network of computers.

Virtual currency conversion: A personality or a thing that converts virtual currency on behalf of fiat currency or farther forms of funds.

Crypto-currency: A virtual-currency that secured through cryptography procedures is named as crypto-currency. Bitcoin, Litecoin, Ripple, and Ethereum are examples for crypto-currencies as a piece of price used to carry-out on the primary blockchain.

Proof-of-Work and Stake: Proof-of-work and Stake are the two familiar authorization methods for justify blockchain dealings/transactions. In proof-of-work authorization process, in a competition fighting by solving cryptographic puzzle participants add the next transaction block to the existing blockchain. Coming to proof-of-stake process, network contestants devote digital coins in the blockchain arrangement that represents theirs stake in a particular block.

Mining: Mining progression present by the abusers to legalize transaction records on blockchain that utilize the proof-of-work method for justification procedure.

Token: Crypto-currency that work or fabricate on a blockchain to have a series of utilizes, in-addition serving as currency dissimilar platforms. All these virtual currencies, as well as tokens, have principal gains potentially if there is intensifying demand for the appliances, functionalities related to virtual-currency otherwise token.

Utility token: Tokens whichever intended mainly to confer the vendor access as well as privileges to make use of a scheme. Utility tokens characteristically suggest connection and functionality feature, given that vendor with connection to blockchain arrangement and functionalities contained by that arrangement.

21.5.2 Existing Literature Work on IoT Related Security Issues

Cryptography is a frequent procedure to make available data confidential, incorruption [66]. Introduced the superior technique of VPN validation via GPS. VPN client as a substitute of raw data broadcast hash assessment for GPS message in order to shield Geo-confidentiality of the user. As endow with solitary GPS coordinates region can be offered for index through verification server for every user. With the help of Google maps test the hit velocity of user GPS coordinates of the target section [67]. Designed a DDOS termination scheme via IDS, firewall base on data digging methods that compromises model selection and evaluation, data

selection and data preprocessing transformation. Disparate security mechanisms have been presented for dissimilar WSNs, Wi-Fi, honey-pots, MANETs, local area networks, and sensor nodes. In [68] produced a MANETs security model support on service from firewall, Public key infrastructure (PKI), and IPS. In this model almost every node has an identical defense replica, as a result, provide professionally protected map-reading, data transportation moreover monitor molests. Both data and routing are signed encrypted so they can accept only authorize nodes only. IPS utilized to organize the network situations prepared in PKI and firewall. Obtainable IPS allocate for early exposure, removal hateful packets, and delays for packets delivery [69]. Projected an Intrusion Filtration System (IFS) that endow with heavy protection to conclude implementation and disturbing of dishonored files. In this, all files which are available in the system are scan plus information regarding the entire appliance and software inaugurated inside the method store in IFS database [70]. Invented IDS for WSNs using pattern harmonizing system. Here specified signatures to express objectionable actions, and when the pattern counterparts an event, a specified achievement perform and define by a set of signature rules. Constant divergence among recent and earlier patterns will generate an attentive sign [71]. Addressed Wi-Fi based WSN works on Linux OS, utilizing Snort, Kismet in place of IDS and IPS, diffusion analysis perform through 5 R3 make use of the integration of Fern Craker along with Ettercap enhance the arrangement production via rising the exposure speed on higher layers regarding Wi-Fi WSNs [72]. Offered a method to facilitate apply IDPS and ZigBee base locale set-up. Without much information about the attackers, the offered method provides prevention technique by employing dynamic machine learning. In the proposed method, stated protective trials like malicious packets, spoofing anticipation is there to stop molests. The Q-learning technique employed to conclude most excellent policy, not in favor of an attack [73]. Introduced multi-level behavior outlier identifier in favor of Android campaign, the identifier recognizes or obstructs assumed intimidation through detect explicit activities prototype for a group of famous intimidations, as a result of the inspection the demanded consent and character metadata, every time the innovative app is fixed [74]. Presents three securities manage procedures to prevent, detect and correct procedures, headed for guarantee safety, seclusion of electronic health record (HER) structures. Prevent an attack can achieve through password and defect can achieve through IDS/IPS finally the corrective control done by control the damage done by attackers [75]. Using TCP simulated attacks and with the help of UDP evaluated the results to learn a dissimilar variety of DDOS molests on the firewall. Besides, it utilized to identify abnormal packet amalgamation and activities of the attacker [76]. Introduced a crossbreed encryption system with RSA in the company of Digital signature algorithm toward tremendous security as well as high throughput in MANETs. The performance of projected protocol estimated via NS-2 [77]. Presented IDS for MANETs that make use of the digital autograph method for remove accidents plus limit broadcast function to decrease false alarm velocity [78]. Employed a disseminated structure Collaborative boundary Gateway procedure for the monitor as well as defense from edge-based molests. It applied on application

level services which organize allotment of network motion via routers [49]. Proposed malware and threat distribution proposal to accumulate, share significant indicators of attacker targets. In this, both private, public groups able to allocate info moreover compromise indicators on top of existed attacks of loyalty background [50]. Described self-distributed robust firewall design pedestal on the collaboration of dissimilar workings of that system transportation [51]. Employed scattered host base shared recognition procedure to diminish False Data Injection (FDI) assaults in smart-grid CPS. An imperative base mass selection system was projected toward notice an irregularity in negotiated phasor dimension entity. Here anticipated methods calculate by real-time dimension statistics from power simulator [52]. Designed a mobile base health system based on IoT transportation to decrease healthcare management costs and needless hospitalization. An embedded smart sensor node monitor patient sugar level, asthma, blood pressure, etc. and communicates through devices which are mostly wirelessly connected to IoT servers [79]. Made Mutual cyber-physical security (M-CPS) supervision model in favor of dangerous infrastructure [80]. Introduced extension of existed right to use methods through protection hazard procedures scheduled professional social networks (PSN). Collision, risk, and susceptibility describe the risk for the incoming request. The risk threshold value is fixed based on that organizations refuse an access request [81]. Proposed a collaborative security approach by combining adaptive and collaboration adaptive. Adaptive identify security control requirements based on environmental changes, coming to collaborative adaption targets on method necessary for manifold mechanism collaboration [82]. Observe both collaborative, as well as wormhole, molests in MANETs, by what method to identify mentioned molest utilizing AODV routing algorithm. Evolution took in NS-2 simulator [82]. Employed an SDN-base honey-pot-nature frame in order to facilitate dissimilar parties to work together energetically as well as decouple gate-ways as well as honey-pots.

21.5.3 Limitations of IoT Security

As discussed earlier IoT structural-design include perception layer, networking contracts, services, and interface layer. Perception layer contains sensors, actuators for assembling and preprocessing surrounding environmental information such as motions, temperature, and acceleration and location functionalities. Network layer responsible to connect other system devices plus servers. Service layer handle particular services to congregate the IoT appliances requirement. Finally interface layer relations with objects [53–56].

The topology for IoT varies with respect to application scenarios, smart home applications have stable topology and transportation applications have mobility applications. It is difficult to make network connectivity, things management and to reach security and privacy issues. IoT is a collection of dissimilar objects which have dissimilar hardware abilities. For example sensor nodes which have very

limited resource constraints, those are extensively deployed in dangerous environments for gathering valuable raw sensible data. However, there some technologies developed to increase the lifetime of the network but still; sensors are limited in processing and storage perspective. Furthermore most of IoT devices, sensors deployed in unattended fields where humans can not able to monitor all those devices. This kind of scenarios makes sensors and devices vulnerable to multi-dimensional harms. Classical security systems as cryptographic techniques computationally not applicable for the reason of IoT devices limited abilities. Furthermore erratic, insecure wireless channels with spread-out nature bring other hazards to data safety. There are some general attacks on IoT starting from lower level to upper level, those are described shortly below.

Adversaries can capture control nodes via node capture attacks to steal important secure information. If broadcasting signals are not encrypted well adversaries may possibly overhear something on transmitting channels. Adversaries can able to explore the vulnerabilities of network protocols and initiate selective flood attack, reply attack, man-in-the-middle attack, block hole attack, Sybil attack, and wormhole attacks, etc. this kind of attacks compromise the good effectiveness and accuracy of selection methods and multi-path routing protocols. Generally sensed data transmitted through hop-by-hop paths till reaching their respective destinations. It affords the attackers an opportunity to inject or tamper false data. Attackers develop Denial of service kind of attacks which degrades the limited resources of the sensor nodes. Attackers may be creating a software attack which uses backdoors of software to alter software functions and control operations.

21.5.4 Blockchain in Data Sharing

Blockchain proposed in 2008 by Satoshi Nakamoto and practically implemented in 2009 using cryptography technique as reproduced crypto-currency bitcoin. The main functionality of the proposed block chain is to store transaction data in a secure and distributed manner. Every time a fresh transaction is initiated and transmits throughout blockchain setup. Users or nodes who received the transaction can verify by validating the signature on transaction those are called as block miners. To produce a block, block miners need to solve harmony puzzle problem and transmit their newly generated blocks throughout the network setup. After getting a new block, block miners must able to solve the harmony crisis in order to append the newly generated block to individual chains of blocks which was sectionally sustained at the miners. New block encloses a link to the prior block in chains with taking advantage of cryptographic principles. A specific terminology definite to promise the constant ledger shared across the dispersed set-up. Cryptography based private keys is apply to sign mark on a transaction, resulted in signature embedded as an primary element of the transaction and mathematical indication as testimony that the transaction arrive from the specified vendor of

private key. The miners who verify the validation of the transaction has corresponding public to that private key. This could be done through preload the public key at each and every-one miners or attach public key of the digital credential or signature for transmission [53, 54, 59–63].

Every minor block records backward-associated register of blocks as a local evidence of dealings. As a ledger, each block summarizes a set of verified transactions. Furthermore, each block contains parent blocks links in its header along with the answer for the harmony problem. Depending on other specified demands block header may also contain a timestamp, nonce value, etc. cryptographic hash algorithm is applied on bock header for unique identification based on the generated hash value. Based on each hash function sequences initiates the each blocks links with its parent block, it may be useful to overturn all the way to locate the first ever formed block. It indicates blocks are succession mutually acts as ledger at every solitary node. The link of the parent block is within the block-header and that distress the existing blocks hash-value. In order to change any-one available block in the chain, the subsequent child, and grandchild blocks need to be re-designed to meet appropriate harmony problems. But such kind of functioning redesigning is high priced moreover obligate difficult transactions in bitcoin operation. On longest blockchain is widely acknowledged as the ledger to the complete system and all locally sustain chains are modernized consequently. Remember the nodes whichever propagate transactions/dealings in the foremost place are accountable for dissemination of transactions and re-dissemination the dealings at any time it needed. The miners that resolve the harmony crisis and engender new blocks take the task of distribution the blocks across the set-up. Byzantine agreement problem is the primary objective that exploits Blackchain functionality. The byzantine problem describes the situation where the peers efforts to accomplish a consensus at the same time traitors with peers might deceive the others and avert them from getting the harmony. Forging messages, ignore messages, deploying fake messages of other peers are some of the possible strategies of the betrayers [54–58].

The key role of blockchain is consensus protocols that make distributed and consistent ledger with no need for centralized coordination furthermore produce respective solutions to byzantine problems. Blockchain creation and generation defined by the law of consensus protocols. Blockchain miners solve the consensus or harmony problems that defend any kind of potential attackers or from compromised miners from being hijack or modify the blockchain generation process. Consent protocols in open access system agree to unproven as well as unreliable miners to extract blocks with no need to verifying their identities these was called as a public blockchain. In another kind of blockchain only permission, authentic participate miners advice apiece in a peer-to-peer manner of their annotations of dealings these were names as private blockchain [56–64].

21.5.5 Existing Literature Work on IoT Related Security Issues

In [83] Explained HTTPS protocol to generate secure HTTPS channel for IoT devices in order to eradicate in-between devices. Here authors utilized Password based key derivation function—2 which presents session keys moreover IoT transactions stored among several devices those preserve Blockchain. In [84] authors presented enlightenment for allocation data among IoT devices. In presented system Blockchain maintains data control and storage principles. Mainly focused on separation, supervision of data and flexible messages based on query request. In [85] explore a platform namely Autonomous decentralized peer to peer Telemetry base on Ethereum procedure where devices contract and do transactions in an adaptable way. As a result, IoT devices can able to identify, situate independently their own roles, farm-duties and dealings among themselves in the entire IoT eco-system. In [86] described resolution for SSH public keys support on blockchain, generally paying attention on key organization difficulty across IoT devices. In [87] proposed health management base blockchain formation. In order to provide privacy for patient personal information (Electronic Medical Record—ERH) authors come up with three layers architecture. ERH encrypted signed to make guarantee for confidentiality, truthfulness and confirmation. Based on report from authors [88] to make sure privacy in IoT arrangements, suggested to go with per-to-peer structural design. In recent times authors [89] explained multi-layer protection structural design for smart cities that incorporate with Blockchain technology as disseminated ledger toward store, share mixed data like as cities humidity, traffic, temperature etc. [90]. Designed privacy preserving method for IoT devices in a cloud environment. Authors also developed a method where devices to improve manufacturing attribution without any authentication from third-party

21.5.6 Challenges Blockchain Applying to IoT Applications

The applications of Blockchain on the Internet of things face following challenges that are described below [53–65]:

1. Internet of things is a collection of heterogeneous networks where sensor nodes and smart devices collect valuable raw sensed data. Some Blockchain activities are unoffered for the limited resources of IoT devices. Cryptographic techniques, secure routing protocols with authentication, attribute base encryptions and access control protocols which are applied on Blockchain for privacy are too much excessive on IoT devices. A complete node of Blockchain has to search, verify each transaction deal which is very difficult for resource-constrained IoT sensor nodes. Typically in bitcoin operation entire network can produce or perform nearly 10 power 9 hash values for a second which was difficult to perform by IoT devices.

2. Blockchain requires huge storage spaces, one bitcoin blockchain nearly need 156 gigabytes which is prohibitive in IoT devices. Exclusive of these gigantic records, IoT systems are incapable to prove the transaction deals produced by others. In addition, transaction dispatcher wants historical stored data for steadiness and transaction indicator to create innovative transactions. However, storage demand can reduce by the deployment of IoT devices with uncomplicated nodes in the blockchain systems.
3. Blockchain involves continuous transmissions and exchange data in order to sustain constant records for new blocks and records. IoT devices use wireless communications technologies (Bluetooth, Zigbee, WiFi) suffer from collision and interference problems. IoT Nodes consume more energy in the communication process than computational.
4. A few IoT devices specially planned to manage for a extensive time period with limited battery supply by employing energy-saving strategies, high communication technologies, and sleep mode. But blockchain operations computation and communication typically energy hungry.
5. Wireless sensor network provides two kinds of transportation one is a standard version where sensor nodes forward by fixed base stations and another one where sensor nodes move one place to another place and transform packets to other nodes. The mobility function in IoT devices weakens the blockchain performance.
6. High latency of blockchain is exploited to promise stability in the decentralized blockchain set-ups. But coming to IoT it is not acceptable. For one block conformation in bitcoin is 10 min which is excessively long for delay-sensitive appliances like target tracking, healthcare management, and vehicle networks.

21.5.7 Research Problems

In the future the Internet of things will make an even more important role in our modern society in both civilian as well as military frameworks [53–65].

1. Depend on applications some IoT devices employed in publicly available areas, under some circumstances an IoT device physically under the supervision of an attacker, in what way a blockchain can provide security and privacy for data generated in those type devices.
2. Consider limited resource constraints of IoT devices, how to implement best cost effective blockchain based security solution.
3. Researches may focus on optimization based blockchain data sharing and security frameworks that will diminish energy expenditure at the same time as performing most proficient and effectual services.
4. The storage-space of IoT devices is dreadfully imperfect which stops the emergent power of blockchain ledger. Conversely, some information in IoT devices is not more useful or not meaningful in future after it used. Such

information deletion without breaking the trust of storage data may increase the storage capacity of blockchain. Modification and deletions possible only when editable blockchain guarantee or reach some specific circumstances and reports for any edit procedures. Present time editable blockchain design got the attention of researchers as an interesting research area.

5. Nowadays blockchain sharding mechanism growing at a high-speed rate which enables the parallel transaction. IoT assembles a huge amount of data across the network region and IoT data shows strong locality and heterogeneity useful for local regions this gives strong backup for development for sharding blockchain in IoT environments.
6. In some applications, IoT devices may move far away or travel large distances from home networks. The integrity of data generated by these mobility nodes equals important as static nodes. Data generated by these nodes mined in blocks and embedded in dissimilar blockchains because of their distance from home networks. Migration or integration of these blocks may provide consist of records.
7. Specially developed consensus protocols are vital to promote IoT-Blockchain appliances. Which plays a momentous role in authorize transaction data as a replacement for of further specifications?
8. The operations such as block mining and amount of blockchain data too heavy to implement on IoT services. There is a need for simple verification technologies that can able to verify transaction without block mining and stores all the transaction records in blocks.

References

1. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Future Gen. Comput. Syst. **82**, 395–411 (2015)
2. Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D.: Security of the Internet of Things: perspectives and challenges. Wireless Netw. **20**, 2481–2501 (2014)
3. Kouicem, D.E., Bouabdallah, A., Lakhlef, H.: Internet of things security: a top-down survey. Comput. Netw. 1–24 (2018)
4. Sfar, A.R., Natalizio, E., Challal, Y., Chtourou, Z.: A roadmap for security challenges in Internet of Things. Digit. Commun. Netw. (2017). https://doi.org/10.1016/j.dcan.2017.04.003
5. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. **76**, 146 (2015)
6. Zhao, K., Ge, L.: A survey on the Internet of Things security. In: 2013 Ninth International Conference on Computational Intelligence and Security (2013)
7. Bhanu chander, Kumaravelan: Simple and secure authentication in wireless sensor network using digital certification. Int. J. Pure Appl. Math. **119**(16), 137–143 (2018)
8. Bhanu chander, Kumaravelan: Introduction to WSN. Soft Computing in WSN. CRC Press/ Taylor and Francis Publications (2018)
9. Sen, J.: Security in wireless sensor networks. Int. J. Comput. Sci. Inf. Secur. **4**(1 & 2) (2014)
10. Alam, S., De, D.: Analysis of security threats in wireless sensor network. Int. J. Wireless Mob. Netw. (IJWMN) **6**(2) (2014)

11. Padmavathi, G., Shanmugapriya, D.: A survey of attacks, security mechanisms and challenges in wireless sensor networks. Int. J. Comput. Sci. Inf. Secur. (IJCSIS) **4**(1 & 2) (2009)
12. Akyildiz, I.F., Su, W., Sanakarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
13. Hamad, F., Smalov, L., James, A.: Energy-aware security in M-Commerce and the internet of things. IETE Tech. Rev. **26**(5), 357–362 (2009)
14. Tsudik, G.: YA-TRAP: yet another trivial RFID authentication protocol. In: Proceedings of Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 196–200 (2006)
15. Mathur, S., Trappe, W., Mandayam, N., Ye, C., Reznik, A.: Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In: Proceedings of Mobile Communications, pp. 128–139 (2008)
16. Montenegro, G., Castelluccia, C.: Crypto-based identifiers (CBIDs): concepts and applications. ACM Trans. Inf. Syst. Secur. **7**(1), 97–127 (2004)
17. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and privacy aspects of low-cost radio frequency identification systems. Secur. Pervas. Comput. 201–212 (2004)
18. Juels, A., Rivest, R.L., Szydlo, M.: The blocker tag: selective blocking of RFID tags for consumer privacy. In: Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS 2003), pp. 103–111 (2003)
19. Ohkubo, M., Suzuki, K., Kinoshita, S.: Cryptographic approach to privacy-friendly tags. In: RFID Privacy Workshop, p. 82. MIT, Cambridge, MA (2003)
20. Lakafosis, V., Traille, A., Lee, H.: RFID-CoA: the RFID tags as certificates of authenticity. In: Proceedings of the IEEE International Conference on RFID, pp. 207–214 (2011)
21. Hu, F., Wang, F.: Study of recent development about privacy and security of the internet of things. In: Proceedings of the International Conference on Web Information Systems and Mining, pp. 91–95 (2010)
22. Lv, B.Y., Pan, J.X., Ma, Q., Xiao, Z.H.: Research progress and application of RFID anti-collision algorithm. In: Proceedings of the International Conference on Telecommunication Engineering, vol. 48, no. 7, pp. 124–128 (2008)
23. Finkenzeller, K.: RFID Handbook Fundamentals and Applications in Contactless Smart Cards and Identification, 2nd edn. Wiley, West Sussex (2003)
24. Karlof, C., Sastry, N., Wagner, D.: TinySec: a link layer security architecture for wireless sensor networks. In: Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems, pp. 162–175 (2004)
25. Chen, M., Lai, C., Wang, H.: Mobile multimedia sensor networks: architecture and routing. EURASIP J. Wireless Commun. Netw. 1–9 (2011)
26. Han, K., Luo, J., Liu, Y., Vasilakos, V.: Algorithm design for data communications in duty-cycled wireless sensor networks: a survey. IEEE Commun. Mag. **51**(7), 107–113 (2013)
27. Malan, D.J., Welsh, M., Smith, M.D.: A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. In: Proceedings of the IEEE International Conference on Sensor and Ad Hoc Communications and Networks SECON04, pp. 71–80 (2004)
28. Hu, Y.C., Johnson, D.B., Perrig, A.: SEAD: secure efficient distance vector routing for mobile wireless Ad Hoc networks. Ad Hoc Netw. **1**(1), 175–192 (2003)
29. Huang, C.H., Du, D.Z.: New constructions on broadcast encryption and key pre-distribution schemes. In: IEEE INFOCOM, pp. 515–523 (2005)
30. Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: Proceeding of the IEEE Symposium on Security and Privacy, pp. 197–213 (2003)
31. Ren, F.Y., Huang, H.N., Lin, C.: Wireless sensor networks. J. Softw. 1282–1290 (2003)
32. Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., Culler, D.E.: SPINS: security protocols for sensor networks. Wireless Netw. **8**(5), 521–534 (2002)
33. Cao, Z., Hu, J.B., Chen, Z., Xu, M.X., Zhou, X.: Feedback: towards dynamic behavior and secure routing in wireless sensor networks. In: Proceedings of the IEEE Workshop on Pervasive Computing and Ad-hoc Communication (PCAC'06), vol. 2, pp. 160–164 (2006)

34. Wood, A.D., Stankovic, J.A.: Denial of service in sensor networks. IEEE Comput. **35**(10), 54–62 (2002)
35. Douceur, J.R.: The Sybil attack. In: Proceeding of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), pp. 251–260 (2002)
36. KSW Microtec AG: KSW—TempSens (2013). http://www.ksw-microtec.de/www/doc/overviewtempsens1124436343en.pdf. Accessed 12 Oct
37. Wang, K., Bao, J., Wu, M., Lu, W.: Research on security management for internet of things. In: Proceeding of the IEEE International Conference on Computer Application and System Modeling (ICCASM), vol. 15, pp. 133–137 (2010)
38. Zhang, L., Wang, Z.: Integration of RFID into wireless sensor networks: architectures, opportunities and challenging problems. In: Proceeding of the IEEE Fifth International Conference on Grid and Cooperative Computing Workshops GCCW '06 (58), pp. 463–469 (2006)
39. Li, C., Chen, C.L.: A multi-stage control method application in the fight against phishing attacks. In: Proceeding of the 26th Computer Security Academic Communication Across the Country, pp. 145–153 (2011)
40. Liu, Z.Y., Yang, Z.C.: Ad hoc network and security analysis. Comput. Technol. Dev. **16**(1) (2006)
41. Avudainayagam, A., Lou, W., Fang, Y.: DEAR: a device and energy aware routing protocol for heterogeneous ad hoc networks. Parallel Distrib. Comput. **63**(2), 228–236 (2003)
42. Yang, Z.W.: Look the internet of things from the internet and 3G. Radio frequency (rf) in the world, (01) (2010)
43. Zhang, B., Zou, Z., Liu, M.: Evaluation on security system of internet of things based on fuzzy-AHP method. In: Proceeding of the IEEE International Conference on E-Business and E-Government (ICEE), pp. 1–5 (2011)
44. Sweeney, L.: K-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 557–570 (2002)
45. de Saint-Exupery, A.: Internet of things [EB/OL]. http://www.sintef.no/upload/IKT/9022/CERP-IoT%20SRA_IoT_vll_pdf.pf. Accessed 12 Oct 2013
46. Zhang, D., Zhou, J., Guo, M., Cao, J., Li, T.: TASA: tag-free activity sensing using RFID tag arrays. IEEE Trans. Parallel Distrib. Syst. **22**(4), 558–570 (2011)
47. Zai, L., Liu, S.D., Hu, X.B.: ZigBee Technology and Application. Beijing University of Aeronautics and Astronautics Press, Beijing (2007)
48. Shao, P.F., Wang, Z., Zhang, B.R.: Smart home system research for the mobile internet. Comput. Meas. Control **20**(2), 474–476 (2012)
49. Da Costa Júnior, E.P.: An Architecture for Self-adaptive Distributed Firewall
50. Li, B., Lu, R., Wang, W., Choo, K.-K.R.: Distributed host-based collaborative detection for false data injection attacks in smart grid cyberphysical system. J. Parallel Distrib. Comput. **103**, 32–41 (2017)
51. Almotiri, S.H., Khan, M.A., Alghamdi, M.A.: Mobile health (m-Health) system in the context of IoT. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, pp. 39–42 (2016)
52. Papastergiou, S., Polemi, N., Karantjias, A.: CYSM: an innovative physical/cyber security management system for ports. In: International Conference on Human Aspects of Information Security, Privacy, and Trust, pp. 219–230 (2015)
53. Wang, X., Zha, X., Ni, W.: Survey on block chain for Internet of Things. Comput. Commun. (2019). https://doi.org/10.1016/j.comcom.2019.01.006
54. Ejaz, W., Anpalagan, A.: Internet of Things for Smart Cities. Springer Briefs in Electrical and Computer Engineering (2017). https://doi.org/10.1007/978-3-319-95037-2_5
55. Efanov, D., Roschin, P.: The all-pervasiveness of Blockchain Technology. In: 8th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2017. Procedia Computer Science, pp. 116–121 (2018)
56. Gordon, W.J., Catalini, C.: Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput. Struct. Biotechnol. J. **16**, 224–230 (2018)

57. Banerjee, M., Lee, J., Choo, K.-K.R.: A blockchain future for internet of things security: a position paper. Digit. Commun. Netw. 149–160 (2018)
58. Rennock, M.J.W., Cohn, A., Butcher, J.R.: Blockchain Technology and Regulatory Investigation, February/March 2018 | Practical Law© 2018 Thomson Reuters (2018)
59. Nuce, M.: Blockchain and Data Sharing. CSCMP Hot Topics, April 6 (2018)
60. Banerjee, M., Lee, J., Choo, K.-K.R.: A blockchain future to Internet of Things security: a position paper. Digit. Commun. Netw. (2017). https://doi.org/10.1016/j.dcan.2017.10.006
61. Zhang, P., White, J., Schmidt, D.C., Lenz, G., Trent Rosenbloom, S.: FHIRChain: applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J. **16**, 267–278 (2018)
62. Greenspan, G.: Blockchains vs centralized databases (2018). Available at https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases. Accessed 16 Jul 2018
63. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F.: Secure and trustable electronic medical records sharing using blockchain. arXiv preprint arXiv:1709.06528 (2017)
64. Guo, Y., Liang, C.: Blockchain application and outlook in the banking industry. Financ. Innov. **2**(1), 24 (2016)
65. Zhang, Y., Wen, J.: The IoT electric business model: using blockchain technology for the internet of things. Peer-to-Peer Netw. Appl. 1–12 (2016)
66. Jin, Y., Tomoishi, M., Matsuura, S.: Enhancement of VPN authentication using GPS information with geo-privacy protection. In: 2016 25th International Conference on Computer Communication and Networks (ICCCN), pp. 1–6 (2016)
67. Keshri, A., Singh, S., Agarwal, M., Nandiy, S.K.: DoS attacks prevention using IDS and data mining. In: 2016 International Conference on Accessibility to Digital World (ICADW), Guwahati, pp. 87–92 (2016)
68. Filipek, J., Hudec, L.: Securing mobile ad hoc networks using distributed firewall with PKI. In: 2016 IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMI), Herlany, pp. 321–325 (2016)
69. Dewanjee, R.: Intrusion Filtration System (IFS)-mapping network security in new way. In: 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), pp. 527–531 (2016)
70. Kalnoor, G., Agarkhed, J.: Pattern matching intrusion detection technique for Wireless Sensor Networks. In: 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-informatics (AEEICB), Chennai, pp. 724–728 (2016)
71. Yacchirena, A., Alulema, D., Aguilar, D., Morocho, D., Encalada, F., Granizo, E.: Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system. In: 2016 IEEE International Conference on Automatica (ICA-ACCA), Curico, pp. 1–7 (2016)
72. Jokar, P., Leung, V.: Intrusion detection and prevention for ZigBee-based home area networks in smart grids. In: IEEE Transactions on Smart Grid (2017)
73. Saracino, A., Sgandurra, D., Dini, G., Martinelli, F.: MADAM: effective and efficient behavior-based android malware detection and prevention. In: IEEE Transactions on Dependable and Secure Computing, vol. 9, pp. 1–12 (2017)
74. Osop, H., Sahama, T.: Quality evidence, quality decisions: ways to improve security and privacy of EHR systems. In: 2016 IEEE 18th International Conference on eHealth Networking, Applications and Services (Healthcom), Munich, pp. 1–6 (2016)
75. Sharma, A., Bhuriya, D., Singh, U.: Secure data transmission on MANET by hybrid cryptography technique. In: 2015 International Conference on Computer, Communication and Control (IC4), Indore, pp. 1–6 (2015)
76. Indumathi, G., Sakthivel, S.: Securely detecting an intruders in MANETs system. In: International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, pp. 1–5 (2014)
77. Hiran, R., Carlsson, N., Shahmehri, N.: PrefiSec: a distributed alliance framework for collaborative BGP monitoring and prefix-based security. In: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security (WISCS '14). ACM, New York, NY, USA, pp. 3–12 (2014)

78. Wagner, C.: MISP: the design and implementation of a collaborative threat intelligence sharing platform. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. ACM (2016)
79. Bouchami, A., Goettelmann, E., Perrin, O., Godart, C.: Enhancing access-control with risk-metrics for collaboration on social cloud-platforms. In: 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, pp. 864–871 (2015)
80. Bennaceur, A., Bandara, A.K., Jackson, M., Liu, W., Montrieux, L., Tun, T.T., Yu, Y., Nuseibeh, B.: Requirements-driven mediation for collaborative security. In: Proceedings of the 9th International Symposium on Software Engineering for Adaptive and Self-managing Systems (SEAMS 2014), pp. 37–42. ACM, New York, NY, USA (2014)
81. Arya, N., Singh, U., Singh, S.: Detecting and avoiding of wormhole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm. In: 2015 International Conference on Computer, Communication and Control (IC4), Indore, pp. 1–5 (2015)
82. Pan, X., Yegneswaran, V., Chen, Y., Porras, P., Shin, S.: HogMap: using SDNs to incentivize collaborative security monitoring. In: Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (SDN-NFV Security '16), pp. 7–13. ACM, New York, NY, USA (2016)
83. Gaurav, K., Goyal, P., Agrawal, V., Rao, S.L.: IoT transaction security. In: 5th International Conference on the Internet of Things (IoT), Seoul, South Korea (2015)
84. Hashemi, S.H., Faghri, F., Rausch, P., Campbell, R.H.: World of empowered IoT users. In: 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 13–24. IEEE (2016). https://doi.org/10.1109/iotdi.2015.39
85. Atzori, M.: Blockchain-based architectures for the internet of things: a survey (2017). Available at SSRN: https://ssrn.com/abstract=2846810
86. Kokoris-Kogias, L., Gasser, L., Khoffi, I., Jovanovic, P., Gailly, N., Ford, B.: Managing identities using blockchains and CoSi. In: 9th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2016), EPFL-TALK-220210 (2016)
87. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. **40**(10), 218 (2016). https://doi.org/10.1007/s10916-016-0574-6
88. Conoscenti, M., Vetrò, A., De Martin, J.C.: Block Chain for the Internet of Things: A Systematic Literature Review, pp. 1–6 (2016)
89. Biswas, K., Muthukkumarasamy, V.: Securing smart cities using blockchain technology. In: 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1392–1393. IEEE (2016). https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198
90. Hardjono, T., Smith, N.: Cloud-based commissioning of constrained devices using permissioned blockchains. In: Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, pp. 29–36. ACM (2016)

Chapter 22
Security, Cybercrime and Digital Forensics for IoT

Hany F. Atlam, Ahmed Alenezi, Madini O. Alassafi, Abdulrahman A. Alshdadi and Gary B. Wills

Abstract The Internet of Things (IoT) connects almost all the environment objects whether physical or virtual over the Internet to produce new digitized services that improve people's lifestyle. Currently, several IoT applications have a direct impact on our daily life activities including smart agriculture, wearables, connected healthcare, connected vehicles, and others. Despite the countless benefits provided by the IoT system, it introduces several security challenges. Resolving these challenges should be one of the highest priorities for IoT manufacturers to continue the successful deployment of IoT applications. The owners of IoT devices should guarantee that effective security measures are built in their devices. With the developments of the Internet, the number of security attacks and cybercrimes has

H. F. Atlam (✉) · A. Alenezi · G. B. Wills
Electronic and Computer Science Department, University of Southampton, University Road, Southampton So17 1BJ, UK
e-mail: hfa1g15@soton.ac.uk

A. Alenezi
e-mail: aa4e15@soton.ac.uk

G. B. Wills
e-mail: gbw@soton.ac.uk

H. F. Atlam
Computer Science and Engineering Department, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

A. Alenezi
Computer Science Department, Faculty of Computing and Information Technology, Northern Border University, Rafha, Saudi Arabia

M. O. Alassafi
Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
e-mail: malasafi@kau.edu.sa

A. A. Alshdadi
Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia
e-mail: alshdadi@uj.edu.sa

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_22

increased significantly. In addition, with poor security measures implemented in IoT devices, the IoT system creates more opportunities for cybercrimes to attack various application and services of the IoT system resulting in a direct impact on users. One of the approaches that tackle the increasing number of cybercrimes is digital forensics. Cybercrimes with the power of the IoT technology can cross the virtual space to threaten human life, therefore, IoT forensics is required to investigate and mitigate against such attacks. This chapter presents a review of IoT security and forensics. It started with reviewing the IoT system by discussing building blocks of an IoT device, essential characteristic, communication technologies and challenges of the IoT. Then, IoT security by highlighting threats and solutions regarding IoT architecture layers are discussed. Digital forensics is also discussed by presenting the main steps of the investigation process. In the end, IoT forensics is discussed by reviewing related IoT forensics frameworks, discussing the need for adopting real-time approaches and showing various IoT forensics.

Keywords Internet of Things · Security · Cybercrimes · Digital forensics · IoT security · IoT forensics

22.1 Introduction

The Internet of Things (IoT) technology is one of the most attractive exploration topics for multiple researchers and governments. This attention comes from the unlimited capabilities provided by this new technology. The IoT simply refers to the expansion of computation and network capabilities to not only computers and mobile phones but also various devices and sensors in the world [1]. It can link almost all physical and virtual objects over the Internet using either wired or wireless communication technologies to communicate and share their data to provide new digitized services that improve our lifestyle. The IoT enables heterogeneous devices with different platforms and computation capabilities to be addressable and to communicate together in an effective way [2]. The advances in network and communication systems allow the IoT to grow and connect billions of things. According to Statista [3], the number of IoT objects will be about 75 billion by the end of 2025.

One of the major issues that threaten the continuity of adopting various IoT devices is security. Protecting data of IoT devices is a very difficult process because of the heterogeneous and dynamic features of the IoT. Currently, building an effective and reliable security technique is one of the highest priorities to consider. Although several researchers have introduced multiple security solutions to the security issue of the IoT, a reliable security technique is yet to be developed to guarantee data confidentiality, privacy, integrity and trust [4].

Digital forensics has become one of the important subjects that need more work to provide new investigation tools. It is being used to tackle the increasing number of cybercrimes. With the developments of the Internet and communication

technologies, the number of security attacks and cybercrimes has increased significantly [5]. The number of data records that were compromised in the world reach about 4.5 billion only in the first six months of 2018 [3]. This number increases every day with no ability to discover attackers and prevent attacks in an effective way. Digital forensics helps to acquire legal evidence uncovered in digital media. It also saves time in the investigation process to determine infected or stolen information which can take hours to identify devices and data affected by the attack.

With billions of heterogeneous devices that contain sensitive and valuable data, the IoT system has become one of the main sources of attacks and cybercrimes. Despite the countless advantages provided by the IoT in different applications, it introduces multiple forensics issues. The IoT system involves billions of devices with poor security measures, which make it an easy target for different security attackers. In addition, the heterogeneity of IoT devices makes adopting one of the classical investigation frameworks being ineffective [6]. Hence, building an IoT-based investigation framework should be one of the highest priorities for security researchers to adapt to various devices and situations of the IoT system.

This chapter aims to present a review of security, cybercrimes and digital forensics of the IoT system. It starts by reviewing the IoT system by presenting its definition and layered architecture. Then, it provides a discussion of the main components and building blocks of an IoT device with showing essential features of the IoT system. Different communication technologies and protocols are also discussed. Then, the challenges of the IoT system are also investigated. This is followed by discussing IoT security including security threats and solutions for each architecture layer of the IoT system. Digital forensics and main stages required to perform an investigation process are also introduced. This is followed by discussing IoT forensics by reviewing related IoT forensics frameworks, discussing the need for adopting real-time approaches and main challenges of the IoT forensics.

The remainder of this chapter is structured as follows: Sect. 2 provides an overview of the IoT system; Sect. 3 discusses security in the IoT; Sect. 4 presents the concept of digital forensics; Sect. 4 discusses IoT forensics, and Sect. 6 is the conclusion.

22.2 IoT Technology

Recent advances in the field of Information Technology (IT) has given rise a new technology called IoT. The IoT concept refers to the ability of different objects of the world to be interconnected and communicated together over the Internet. Today, billions of IoT users are connected to each other using Internet Protocol Suite (TCP/IP) and share various types of data all day long [7]. Opinions are shared, and data are exchanged in more than 100 countries with the help of the Internet.

The IoT is defined as "*An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment*" [7]. The

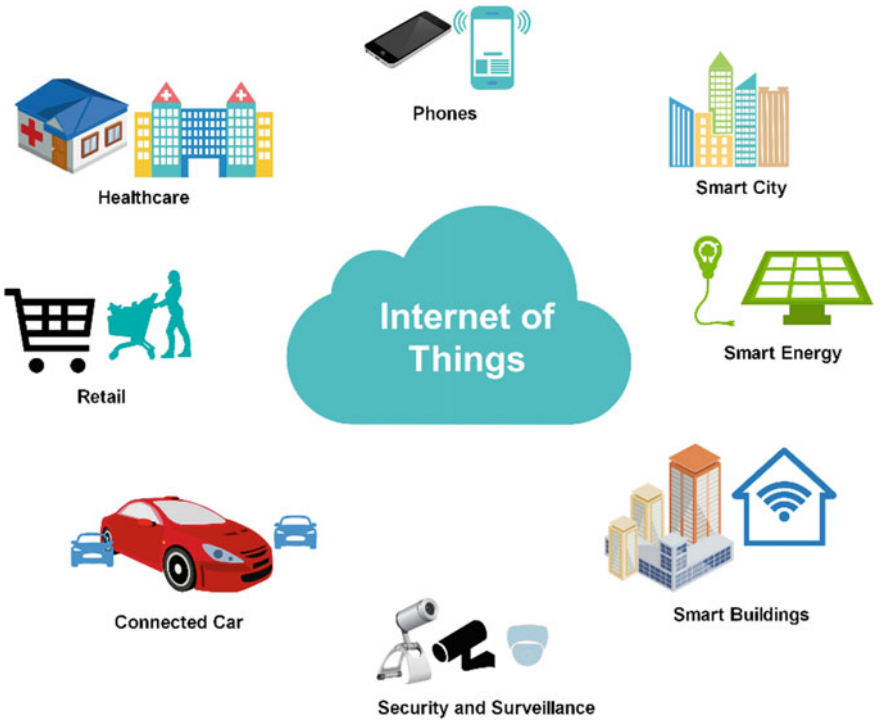


Fig. 22.1 Some of IoT applications

IoT is one of the continuously evolving concepts that emerged from the IT field which attract the attention of IT experts all over the world. It can provide a networked infrastructure for all the physical objects and connect anything at any time [8]. The IoT has provided a unique identity to all of its users and it can be considered as a global network which is connecting people-to-people and things-to-things [9].

The IoT technology has connected most of our world objects over the Internet which allows creating more digitized services. The IoT system involves various applications that have a direct effect on almost all our daily life activities such as smart home, smart city, smart traffic, connected car, connected healthcare, and many others [10]. Figure 22.1 shows some of the IoT applications that are involved in our daily activities.

22.2.1 IoT Architecture

There is a number of data collection technologies in the IoT. The most widely used technology is the Wireless sensor network (WSN) uses multi-hopping and

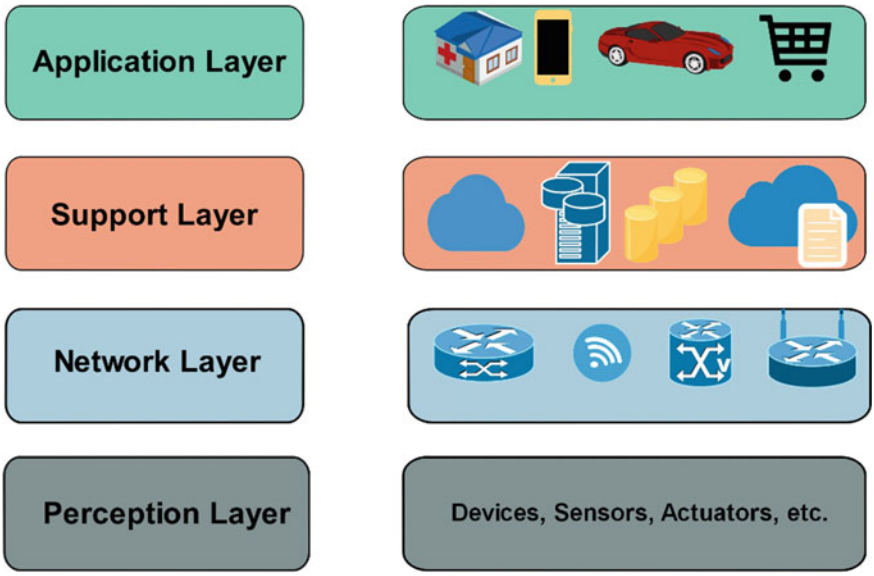


Fig. 22.2 IoT architecture layers

self-organization to maintain control over the communication nodes. In the WSN, a central unit controls the connections of all the distributed nodes [11]. Each node comes with specialized sensors to detect pressure, light and heat. This system works as an integrated model in which nodes perform sensing, collecting data and processing the information in the data. The WSN system is proficient in executing data, quantifying the data, processing and transmission to applications [12]. One of the studies has emphasized the importance of an open architecture for IoT devices to enable connecting a wide variety of network applications [13]. Besides that, the architecture of IoT should be adaptable to enable the integration of data world with the Internet. Previous research has proposed different architecture layers for the IoT to enable further theoretical research [14]. The main architecture layers of the IoT involve perception, network, support and applications layer, as depicted in Fig. 22.2.

(1) **Perception Layer**: This layer contains nano-technology, tagging technology, sensors and intelligence technology to identify the physical objects and collect required information using embedded sensors [15].
(2) **Network Layer**: In this layer, there are communication networks, television networks, WSN, optical fibre networks, closed IP carriers. This layer performs the function of transferring collected data to the processing system to read the information coded in the data.
(3) **Support Layer**: The main processing unit of the IoT is located in the support layer which processes the information from one form into another form. Furthermore, it sends the processed information to the storage and makes it

available whenever required. There is a close association between the application layer and the support layer so that all the functions of IoT devices are performed efficiently [16].

(4) **Application Layer**: This layer contains novel applications that are particularly developed to cater the needs of the industry or users, for instance, some of these specifications for application include, smart sensing of traffics, smart homes, and monitoring the mining processes.

22.2.2 Components and Building Blocks of IoT

The IoT technology can connect anything at any time with the help of any network path [17]. The integration of different components of the IoT system relies on accurate configuration, identification and manipulation of sensors and devices [18]. According to Chandrakanth et al. [19], the essential components of the IoT system involve:

(a) **Hardware**: These components include all the sensors, communication hardware and central units of the IoT system. The main hardware component is the central unit that performs the functions of data storing, data processing and sharing data with the users.
(b) **Middleware**: These components are used as tools to store and analyse data. One of these middleware components is cloud computing, which encompasses various classical technologies such as service-oriented architecture, distributed computing, hardware visualization and grid computing [20].
(c) **Presentation**: The third component is the presentation which visualizes and interpret the data to the users.

The building blocks of the IoT system enables the unification of vocabulary to ensure a smooth exchange of information between different networks. They remove all the subtle concerns of composability and interoperability in the IoT systems [21]. Some of the most important building blocks of an IoT device include sensors, aggregators, e-utility, and communication channel and decision triggers.

1. **Sensors**: It is used to detect the physical properties of an object. These properties are either temperature, weight, acceleration or sound.
2. **Aggregator**: It performs mathematical functions and shifts raw data into an intermediate form of data.
3. **E-utility**: It is either a software or hardware which analyse all the information obtained from the data.
4. **Communication Channel**: It is the medium to transfer stored data, these include wired or wireless communication technologies.
5. **Decision Triggers**: It is used to provide results to satisfy the main purpose of IoT devices.

22.2.3 Essential Characteristics of IoT

The IoT technology has evolved from the integration of the electromechanical system with wireless communication technologies. This integration brought several advantages [22]. The IoT system involves common characteristics, which include:

- **Interconnectivity**: The IoT is the rapidly growing technology which has offered interconnected global information system. It has enabled interconnection of all the communication devices speeding the communication across the world [23].
- **Things-Related Services**: The IoT offers a wide array of services which include not only the technological instruments but also the physical world. In this way, the IoT has proven itself as a technology of modern times.
- **Heterogeneity**: Devices interconnected in the IoT system are heterogeneous with different hardware and network platforms. In this way, a heterogeneous network is formed which is capable of dealing with a diverse range of activities [24].
- **Dynamic Changes**: IoT devices are capable of making dynamic changes in their working modes. For instance, any home use IoT device has an in-built capability of sleeping and waking up, besides that it can also be automatically connected and disconnected with other devices [23].
- **Large Scale**: The IoT system involves billions of devices. The number of IoT objects will reach about 75 billion by the end of 2025 [3]. This constantly increasing network of devices creates a large-scale communication network.

22.2.4 IoT Communication Technologies

The IoT system includes heterogeneous objects and devices. These objects use different communication protocols, networking, and data storage and processing capabilities. The IoT connects billions of heterogeneous objects over the Internet to create new services. Connecting these different devices is not an easy task, hence, communication protocols are considered as the major component that allows all these heterogeneous components to communicate together [1].

This section presents a review of the major communication technologies of the IoT system.

22.2.4.1 Wireless Fidelity (Wi-Fi)

Wirelesses Fidelity (Wi-Fi) is a technology that enables communication between devices through wireless signals. NCR Corporation invented the initial precursor of Wi-Fi in 1991 [25]. WaveLAN is the first-ever wireless product introduced in the market with the speed of 2Mbps. However, the rapid development of wireless

technology has eased the way of novel discoveries and currently, Wireless Local Area Network (WLAN) has connected millions of public locations, airports, homes and offices. In this way, wireless communication has improved immensely. Besides that, today all the consumer electronics, notebooks and hand-held devices have integrated Wi-Fi which has made it a default device [25]. Moreover, entire cities are transformed into Wi-Fi corridors with the help of wireless access points.

22.2.4.2 Bluetooth

Bluetooth is another marvel of advancement in the communication technology which uses short-range radio technology and provides smooth connectivity between daily use devices such as handheld PCs, notebook, printers and cameras within a range of 100 m. Bluetooth devices communicate at a speed of 1 Mbps. Piconet is a common channel adapted by several Bluetooth devices for communication. It has the capacity of connecting 2–8 devices simultaneously for sharing data in the form of text, sound, image, or video [26]. Currently, Intel, IBM, Toshiba, Cisco and HP make the core Bluetooth Special Interest Group to make further innovation in this technology.

22.2.4.3 ZigBee

One important protocol that was developed to improve the features of WLANs is ZigBee. The main features of this protocol are its low cost, short transmission range, reliability, and scalability. ZigBee is another marvel of advancement in the communication technology which provides several advantages. This protocol is the most commonly used in automation devices at home or in industrial control systems and in power systems [27].

22.2.4.4 RFID

Radio-Frequency Identification (RFID) technology is one of the latest network systems for the IoT. In this technology, there are small reading devices which read the message, a radio device and frequency transponders which are known as RF tags. This tag plays a vital role as it contains programmed information which enables the RFID to read the signals. In RFID, there are two different tag system, one is known as an active reader tag and another passive reader tag. The major feature of an active tag is their high frequencies as compared to passive tag. In IoT, the RFID system is used particularly in healthcare applications, agriculture and national security systems [28].

22.2.4.5 NFC

Near-Field Communication (NFC) is a networking technology based on short-range communication to facilitate the transmission of data from one device to another simply by placing them closer to each other. The principle of data communication in NFC is similar to that of RFID. It should be noted that NFC can be used for elaborative two-way communication. NFC is widely utilized in industrial applications, cell phones and online payment system. The main features of NFC are a smooth connection and user-friendly control. Peer -to- Peer (P2P) network topology can be used in NFC [28].

22.2.5 Challenges of IoT

The IoT system is being utilized in various domains in our community. However, there still some challenges that require to be resolved to keep the increasing acceptance rate of IoT devices. These challenges involve:

22.2.5.1 Security Challenges

Technology experts are investigating the potential security concerns to the IoT devices. The most commonly encountered security challenge is the hacking of IoT devices, private e-mails, and confidential data. The pace at which security threats to IoT devices are growing it has risked not only the sensitive information but also the lives and health of its users [7]. Security challenges present the most difficult problem that threatens the successful adoption of IoT devices.

22.2.5.2 Connectivity Challenges

One another major challenge to the future of the IoT is connecting a large number of devices with a common network [29]. Currently, a centralized system is used to authenticate and authorize the information from different nodes. However, this model becomes incompatible to connect billions of IoT device users as the current centralized system will become a bottleneck. The future prospects of the IoT system are based on decentralized networking which allows connecting billions of users simultaneously [17].

22.2.5.3 Longevity and Compatibility of IoT

The current context of development in the IoT is widespread and different technologies are emerging from the IoT system. These evolving technologies require

additional hardware and software which create compatibility issues. Furthermore, there is a lack of firmware in the IoT devices which complicates the problem of their longevity [30]. It is imperative for IoT's future to address the issues of longevity and compatibility.

22.2.5.4 Computation Constraints

The Internet connectivity of IoT devices requires sophisticated communication protocols even for small devices [31]. There are constraints on IoT devices which reduces its speed of information processing. This limitation highlights the requirement of strong security operations so that IoT devices work at an optimum level with minimal resource consumption. The major impact of its size and power constraints is on the integrity and confidentiality of data stored on IoT devices. These systems can be made secure using digital signatures, which require public key infrastructure. However, public key infrastructure encrypts the data using computational and memory resources which are not offered by the current WSNs, particularly with the regular transmission of data required by the system [32].

22.2.5.5 Big Data

The IoT involves a network of billions of objects that produce a massive quantity of data, which is called Big data. The concept of Big data refers to the huge quantity of data that traditional analytical approaches cannot handle it. Numerous challenges are exist with the huge amount of data created by IoT devices especially in security and privacy. Providing suitable data analytics techniques that extract meaningful information is a challenge. In addition, ensuring the integrity of data is another issue that the researchers have to take it into consideration to provide suitable and effective solutions [33].

22.3 Security in IoT

The IoT system is rapidly evolving and is becoming a basic necessity in our daily lives. It forms an important component of national infrastructure and security systems. The main security considerations of the IoT is based on the adopted principles. In the IoT, all the things communicate with other things and are connected through the Internet. One study has reported this system is prone to potential security threats [34]. The high number of security threats of the IoT system render it inapplicable technology in the near future.

This section provides an overview of IoT security. It starts by discussing security threats at different architecture layers of the IoT system. Then, security solutions to mitigate such threats will be presented.

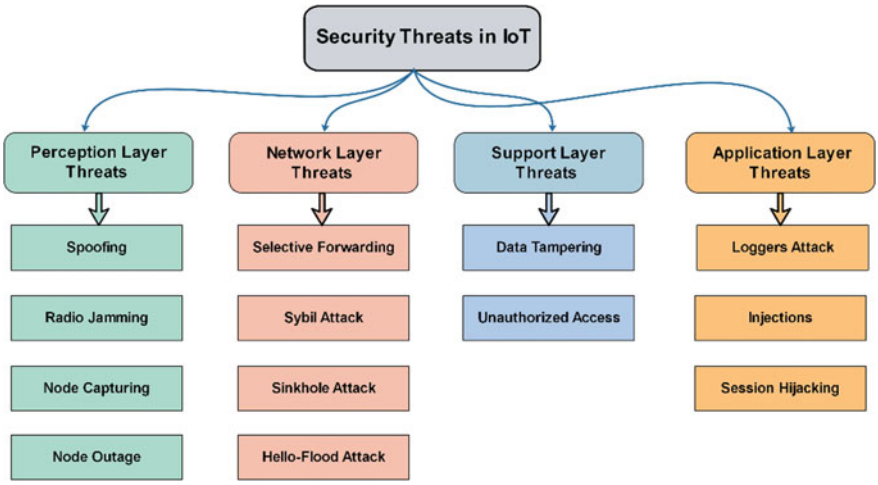


Fig. 22.3 Security threats at different layers of the IoT architecture

22.3.1 Security Threats in IoT

The IoT system involves billions of devices. These devices were designed using poor security measures, which make it a simple object for different types of security threats. This section discusses security threats at each IoT architecture layer, as summarized in Fig. 22.3.

22.3.1.1 Security Threats to Perception Layer

There is a number of security threats to the perception layer of IoT system. The perception layer contains sensors and intelligence embedded technologies such as RFIDs which are prone to threats owing to flaws in security architecture. Some of the most widely encountered threats include the following:

1. **Spoofing**: In this threat, an attacker sends a fake broadcast message to the sensor network, and these networks have no protocol to identify the originality of the message from the source [35]. In this way, attackers usually get access to confidential data and make it vulnerable to further security breaches.
2. **Radio Jamming**: During this security threat, the attackers use Denial of Service (DoS) to block the communication pathways of the nodes and in this way, information is not shared between the nodes of an IoT system [36].
3. **Node-Capturing**: A malicious node physically replaces the sensor node in this attack. In this way, the attacker gains full access over the real node and use it to damage the IoT networks [37].

4. **Node Outage**: Functions of the network are disrupted by logically or physically blocking the network. The main target components of the network in this attack are sensor nodes for collecting, reading and interpreting the data [37].

22.3.1.2 Security Threats to Network Layer

The network layer of the IoT system is also prone to lethal security threats. These threats emerge from various sources. Some of these threats include the following:

1. **Selective Forwarding**: In this attack, the attackers use malicious nodes to selectively block the delivery of some messages and drop these messages to prevent them from propagating in later stages of the IoT operation. In order to conceal the dropped messages, the attackers forward only a few selected nodes. There are various ways that an attacker can use to launch selective forwarding attacks. One most commonly used method is malicious nodes, which drop selective nodes. In this way, the whole system becomes vulnerable to DoS attack [38].
2. **Sybil Attack**: In this attack, a device that has been identified as malicious attempts to take multiple identities to get access into the system [39]. The essential strategy of the intruder is to access the device from more than one place in the form of a single node [40]. During this attack, a single malicious node gives signals of multiple identities to other nodes and thus reducing the effectiveness of their fault schemes.
3. **Sinkhole Attack**: One another critical type of security attack is the sinkhole attack [41]. In this attack, neighbouring nodes attempt to access the limited bandwidth which results in congestion and rapid energy consumption. In this way, a sinkhole is created in the network which makes the IoT system vulnerable to another type of service attacks [42].
4. **Hello-Flood Attack**: This attack is similar to the sinkhole attack as the high traffic on a single channel congest with minor messages. In this way, the main messages are stuck in the congested channels. A single malicious node creates a bundle of useless messages ultimately leading to blockade of channels [36].

22.3.2 Security Threats to Support Layer

The major target of attacks on the support layer is the storage technologies that store all the data from the sensors. Some of these attacks include the following:

1. **Data Tempering**: In this attack, any person who has access to confidential storage technologies tempers the data to gain commercial benefits. During this attack, the attacker manipulates the data and extract confidential information from the inside [43].

2. **Unauthorized Access**: During this attack, unauthorized attacker infiltrates the system and prevent the access of authentic users into the system. Besides that, the attacker also deletes sensitive information and completely damage the IoT infrastructure. One study has reported that these type of attacks are fatal for the IoT system [15].

22.3.3 Security Threats to Application Layer

The application layer of the IoT system includes personalized services depending on the user's preferences. The major security threats to the application layer target these personalized user services. Some of these attacks include the following:

1. **Loggers Attack**: The attacker sends loggers to access confidential data from the network. This information includes important files, E-mail text and passwords. Loggers and sniffers are the most common type of security threat to the application layer. Hackers usually use this method to hack confidential E-mails and password.
2. **Injections**: In this attack, the code of the application is manipulated by accessing it through the server. This is one of the most exploited loopholes in the IoT system and results in data loss, the leak of confidential classified information from the security networks [44].
3. **Session Hijacking**: The attacker exploits the authentication protocols and alters the session management of the networking. In this way, the attacker gains access to the personal identities of the users and use the network just like the real user [44].

22.3.4 IoT Security Solutions

Security is the nightmare of any computer system. Although there are several new sophisticated security approaches, achieving perfect security is nearly impossible. Currently, there are a number of security solutions that are utilized to provide a secure IoT system. This section introduces security solutions regarding architecture layers of the IoT system.

22.3.4.1 Security Solutions to Perception Layer

The main components of the perception layer such as RFID readers, gateways and sensors require additional security measures to protect them against the potential security threats. It has been reported that IoT systems are vulnerable due to lack of

substantial physical security [45]. Therefore, the main initiative to secure the IoT system is to guarantee that the access to confidential data is only granted for authorized users [46]. The IoT system requires robust authentication and authorization protocols to strengthen physical security of the system.

In addition, data recorded by the sensors need a security framework of cryptography which ensure guaranteed privacy of confidential data by processing the information through encryption and decryption. Several studies have demonstrated the effectiveness of cryptographic security protocols and algorithms in IoT security [47]. In a study, two different cryptographic algorithms are compared on sensor nodes and it was found that the Elliptic Curve Cryptography algorithm is more secure as compared to RSA [48]. Few other studies have reported the effectiveness of cryptographic security mechanism to secure the IoT system [49].

22.3.4.2 Security Solutions to Network Layer

In the network layer, the security is provided by protecting two sub-layers. One sub-layer is wireless security which can be protected by creating authentication protocols and key management [50]. For instance, the use of Private Pre-Shared Key (PPSK) secures each connected sensor and object in the IoT system. Wired sub-layer offer a channel for communication between devices in the IoT system. The wired sub-layer can be secured by firewalls and developing an Intrusion Prevention System (IPS).

22.3.4.3 Security Solutions to Support Layer

The support layer is one of the essential IoT layers that involves cloud computing that stores all data of IoT devices. Although the Cloud Security Alliance (CSA) has suggested several security framework standards to solve its security challenges, there are still multiple security challenges. Since the support layer contains data of IoT users and applications, sophisticated security measures should be utilized at this layer. In addition, strong encryption algorithms are required besides an updated antivirus [5].

22.3.4.4 Security Solutions to the Application Layer

Similar to the network layer, there are two sub-layers in the application layers. In one sub-layer, all the local applications are secured using encryption techniques and authentication mechanisms to stop unauthorized access. In the second sub-layer, the national application is secured through authorization, intrusion detection, and access control list [51].

22.4 Digital Forensics

Digital forensics is one of the hottest topics that interest multiple researchers and organizations especially with the increasing number of cybercrimes. This section presents a review of digital forensics by introducing its definition and the main steps needed to conduct a digital investigation process.

22.4.1 Overview of Digital Forensics

The beginning of the technological revolution can be traced back to the 1960s, and since that time the number of crimes committed using computers has grown substantially. As such, digital forensics is now being used to tackle any attack or cybercrime which may be perpetrated, while at the same time improving and acquiring legal evidence uncovered in digital media. NIST defines digital forensics as the process, through science, to identify, gather, examine and analyse data, at the same time as retaining data integrity [52].

The rapid advancement in network technologies has created problems for the accurate and efficient analysis of data. Digital forensics deals with the investigation of data that is recovered from digital devices [53]. The new devices come with updated platforms making it tough for the IT experts to develop new tools to efficiently analyse the recovered data. The main problem is the complexity of digital forensics. For instance, the data from different devices are not easily accessible using traditional methods, sometimes the cumulative dataset is located on multiple sites and even if the traditional digital forensic recover, but the recovered form is not readable on these traditional forensics. Some of the embedded technologies that present new challenges to digital forensics include drones, wearable, medical devices, home automation, vehicles, security systems, and sensor network technologies.

Whenever any incident or crime took place, the forensic team arrive at the scene and collect all the digital devices to gather forensic evidence. The forensic investigator examines and analyses the digital device to collect all the possible evidence pertaining to the crime/incident. During the digital investigation, both the hardware and software digital forensic tools are used. These tools facilitate the investigator to locate and recover the evidence. During the reporting phase, reports prepared by the investigators are presented in testimony. The admissibility of digital evidence is verified by the investigator and provide evidence that no data has been altered during the investigation phase [54].

22.4.2 Digital Forensic Investigation Process

Numerous academics have reached the conclusion that there is no one forensics procedure which can be followed only during all investigations of a digital nature [55]. Despite this, there are a plethora of popular standards [55, 56] which can be applied to the process of digital forensics, including: Digital Forensics Research Workshop (DFRW), Integrated Digital Investigation Process (IDIP), National Institute of Standards and Technology (NIST), and National Institute of Justice (NIJ). Several research scholars and practitioners [55, 57, 58] have agreed on the phases discussed in the NIJ process [59], as shown in Fig. 22.4. These phases involve:

- **Assessment**: Computer forensics examiners ought to pick apart digital evidence rigorously in terms of the case's scope in order to determine which course of action is to be taken.
- **Acquisition**: In terms of its nature, digital evidence is delicate and can be changed, damaged, or permanently deleted as a result of being handled or examined in an inappropriate way. It is best to conduct an examination using a duplicate of the genuine evidence. This genuine form of evidence ought to be obtained in a way that safeguards and maintains its integrity.
- **Examination**. The reason for conducting the examination process is to draw out and assess digital evidence. The word 'extraction', in this context, denotes to the data retrieval from its media.
- **Analysis**: This simply means the data interpretation, which has been recovered, and organising it in a format, which is logical and useful.

Fig. 22.4 Phases of digital investigation of NJR process

- **Documenting and Reporting**: Throughout the forensic processing of evidence, it is vital that notes should be taken regarding the actions and observations, so that they are documented. The conclusion of this process will be preparing a report (written) on the results.

22.5 IoT Forensics

The IoT gives rise to numerous one-of-a-kind, complex problems for those involved in the digital forensics field. There are estimates which state that as many as 50 billion networked devices will exist by 2020, and such devices will be capable of generating a huge amount of data [44]. When vast amounts of IoT data are processed, this will be followed by a proportionate rise in the workloads borne by data centres; because of this, providers will have to deal with newly-emerging problems pertaining to analytics, security and capacity. Guaranteeing that the aforementioned data is handled conveniently is a vital challenge, given that, as a whole, the application efficiency is seriously dependent on the service properties which deal with the data management [60].

As depicted in Fig. 22.5, IoT forensics comprises three digital forensics schemes in total: network forensics, device-level forensics, and cloud forensics [61].

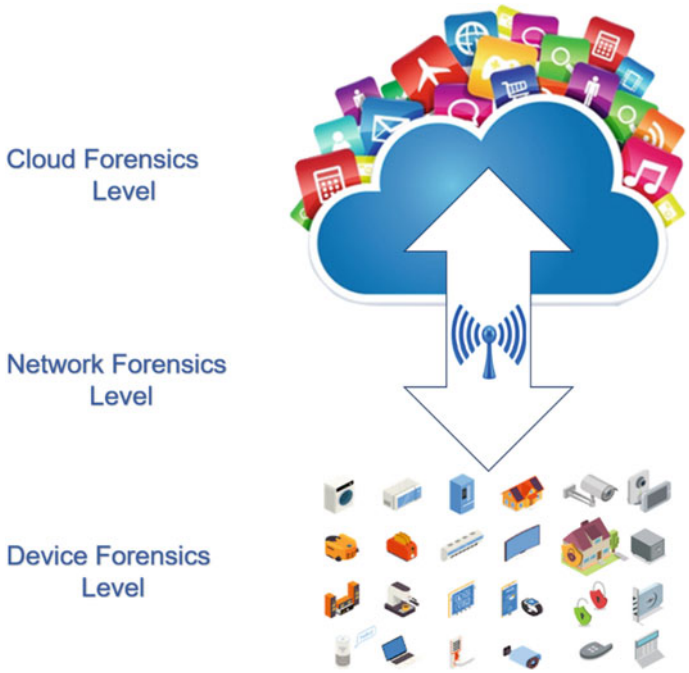


Fig. 22.5 Investigation process of IoT forensics

- **Cloud Forensics**: It will certainly be among the most vital roles in the domain of IoT forensics. As the majority of the IoT devices are characterised by low storage and computational capability, any data which is produced by the IoT networks and IoT devices is kept and sorted in the cloud. The reason for this is that cloud solutions provide numerous different benefits, such as large capacity, on-demand accessibility and scalability, as well as convenience.
- **Network Forensics**: Network logs can be used to identify the origins of different attacks. As such, these logs can be extremely vital when it comes to condemning or exonerating a suspect. IoT infrastructures are made up of different kinds of networks, such as Wide Area Networks (WAN), Body Area Network (BAN), Home/Hospital Area Networks (HAN), Personal Area Network (PAN), and Local Area Networks (LAN). Crucial pieces of evidence can be gathered from any one of the above-mentioned networks.
- **Device-level Forensics**: It could be the case that an investigator needs to gather data from the IoT devices' local memory. If a vital piece of evidence must be gathered from the IoT devices, device-level forensics comes into play.

A plethora of models has been developed in order to address and suits the unique characteristics of the IoT. However, despite this, there are still numerous challenges which are yet to be overcome [62]. For example, particularly noteworthy is the complexity which is faced when data is extracted from the infrastructure of the IoT; indeed, this is because the devices of the IoT can make it more difficult for the investigator to produce evidence that is solid and admissible with regard to forensics [63]. The aforementioned complicated nature arises because of a plethora of challenges, such as uncertainty in relation to the origin of the data and the location of its storage, the inapplicability of the traditional techniques employed for the process of digital forensics, making sure that there is a secure chain of custody, and the data formats [64]. As a result, IoT forensics remains in the process of maturing, particularly since there are numerous challenges which exist and fewer studies in the field. Next section review some of the significant proposed solutions for IoT forensics.

22.5.1 Related IoT Forensics Frameworks

The previously proposed frameworks of digital forensic were compatible with conventional computing. They were not suitable for the IoT context. The previous studies have shown that identification of digital data, its collection, preservation and analysis are cardinal processes of digital forensics [65]. However, there is a need to develop these processes to integrate them with the IoT. There are some challenges in developing IoT forensic system which is discussed in the following sections. Table 22.1 reviews some of the noteworthy proposed solutions for IoT forensics.

Table 22.1 Related IoT forensics proposed solutions

Related framework	Summary of contribution
Meffert et al. [66]	The proposed solution enables the IoT state to collect and log data in real-time by employing a Forensic State Acquisition Controller (FSAC), which makes it possible for data to be obtained from the cloud, an IoT device, or another controller
Hossain et al. [67]	The study proposed a solution which has the potential to ensure that the publicly-available evidence is confidential, anonymous and characterised by nonrepudiation and that there are interfaces which can be used for the acquisition of evidence, as well as a scheme which can confirm the evidence's integrity throughout any investigation into a criminal incident
Chi et al. [68]	A framework proposed in order to obtain and analyse IOT data. The aim of the said framework is to gather data from various contrasting IoT devices and to put forth an evidence format (centralised in nature) specifically for IoT investigations while also formulating an overview of the way in which events take place in a cloud-based environment
Chhabra et al. [69]	A forensic framework (generalised in nature) which has been proposed to address big data forensics in a precise and sensitive way through the use of Google's programming model, MapReduce, which serves as the core for the translation of traffic, extraction, and the analysis of traffic features which are dynamic in nature
Al-Masri et al. [70]	The aim of this framework, which is derived from the DFRWS Investigative Model, is to detect and mitigate cyber-attacks which are perpetrated on IoT systems in early stages
Kebande et al. [71]	A framework designed for an IoT ecosystem which possesses digital forensic techniques which have the ability to assess Potential Digital Evidence (PDE) within the IoT-based ecosystem – evidence which could be utilised to prove a fact

In spite of the fact that a number of solutions have been proposed, there still exist a number of challenges in the field of IoT forensics. The next section provides a discussion of some of the vital challenges being faced by the digital forensics field in the IoT context.

22.5.2 Challenges of IoT Forensics

The current digital forensic is compatible with conventional computing and in some cases cannot be integrated with the IoT infrastructure [61]. The rapid advancement in the IoT and digital forensic need to be integrated to ensure admissibility of digital forensic by transferring the data quickly through the IoT system. According to Taylor et al. [72], there is a need to examine the real environment to enable the integration of digital forensic with the IoT. The potential challenges of IoT forensics include the following:

22.5.2.1 Developing New Investigation Frameworks

In the traditional digital forensic investigation, six steps are followed. However, the integration of digital forensics with the IoT requires new investigation framework. IoT devices generate a large amount of data which has the potential to influence the whole forensic investigation. Thus, large data generated from the scene can create a problem for the investigator to determine devices that were used to perpetrate a crime or launch an attack. Therefore, in the IoT, the evidence is collected to examine the facts about the crime/incident. The collection of data is the most critical phase of forensic investigation and any error during this phase disrupts the whole investigation process. According to research, the currently practised digital forensic devices cannot be switched off to record the accurate time the data was accessed [73]. Therefore, these devices are not applicable for IoT systems. Therefore, it is critical to developing a new framework approach to collect and preserve forensic data using IoT devices. In the IoT forensic, the process of collecting evidence is also complex as compared to conventional methods due to varied formats of data, their protocols and complex interfaces [74]. According to Attwood et al. [75], the recovered data can be temporarily stored on the devices which share a common network with the IoT devices. Therefore, the forensic investigator needs to consider all the potential storage devices to recover all the potential evidence.

22.5.2.2 Multi-jurisdictions

Investigations in IoT forensics are the unclear demarcation of jurisdiction [73]. IoT system data can be transmitted to other cloud services. Therefore, it becomes relatively difficult for the investigator to locate the data from the servers. Besides that, there is physical inaccessibility in collecting evidence from clouds using IoT forensic devices. Hence, it is critical to investigate the issues of multiple jurisdictions before integrating digital forensic with IoT system. Indeed, this kind of situation leads to numerous legal problems for investigators specialising in forensics. Difficulties arise when the time comes to decide which law a particular case should be prosecuted under device jurisdiction, data storage jurisdiction, attacker jurisdiction. In the future, it is vital to rigorously investigate legal challenges which emerge as a result of multi-jurisdictions in the IoT-based environment. There will certainly be a need to use standard techniques in order to examine and assess the plethora of locations and the issues with the networks.

22.5.2.3 Diverse Range of IoT Devices

Rapid advancement in IoT is creating new devices regularly to benefit the users. The services providers are also exploring new options to provide better services to their customers. From a technical aspect, these devices have multiple operating systems simultaneously. This interactivity complicates the IoT devices. This sort of

complexity in the IoT devices can significantly impact forensic investigation procedures. In the current practice, only dedicated tools are used by the forensic investigator. These dedicated tools lack the latest options to accommodate the complexity of the IoT system and therefore IoT forensic is vulnerable to the attacks [76]. Therefore, it is imperative to develop tools that can efficiently adapt to the latest IoT devices.

22.5.2.4 Limitations of IoT Devices' Storage

It is common for IoT devices to be linked with very limited computational resources and memory; in terms of the lifespan of data which is stored in IoT devices, it is short, while data can be written over easily, which leads to the possibility of evidence being lost [65]. There are certainly challenges when it comes to the process of tackling devices which have no, or limited, capacity for storage; among these challenges is the timespan over which the evidence stored in IoT devices can last before it is written over. A common situation is one where IoT application exploits services for data storage and processing which are provided by the cloud. As a result of this, transferring the data over to the cloud could serve as an easy answer to said problem. However, such a transference also constitutes an additional challenge that is related to making sure that the chain of evidence is secure and the approaches used to prove that no modification or alteration of the evidence has taken place [64].

22.5.2.5 Poor Evidence Handling

In digital forensics, it is important to handle all the evidence with the utmost care to prevent tampering of any evidence [76]. The potential issue of tempering and overwriting can be addressed by storing the data in the conventional cloud computing. However, in the IoT forensic the storage of forensic evidence on cloud computing is a complicated process as compared to the conventional process. The lifespan of data stored on the IoT is limited and it is prone to overwriting. Therefore, new techniques are critical to smoothly transit data on IoT devices without any tampering [77].

22.5.2.6 Lack of Forensics Tools

It is commonly held that forensic tools which are available have numerous different limitations and are unable to cope with the technological developments. Within the digital forensics field, the tools which exist are unable to fit with the infrastructure (heterogeneous in nature) of the IoT environment. The huge amount of possible evidence which is produced by many IoT devices will subsequently give rise to new challenges related to the aspect of gathering evidence from IoT infrastructures

which have been distributed [78]. There exists the need for a combination of network forensics and computer forensics tools in order to obtain forensic data and then analyse said data rapidly. It is possible to use traditional forensics tools to gather the data (active data) whilst its integrity is still intact. It is also possible to use specialist network forensics tools to gather further data through the network, e.g. activity logs [79].

22.5.3 Adapting Real-Time Approach for IoT Forensics

The diversity of IoT devices and issues of dealing with IoT constraints can be eliminated in digital forensics by adopting automatic or live forensic investigation. According to Banafa [80], there are three major components for real-time forensic investigation, which include:

- **Time Synchronization**: The time synchronization of all IoT devices used in the forensic investigation, data storage devices and the detection framework are important for real-time forensic investigation.
- **Memory and Storage Requirements**: In IoT forensic investigation, IoT devices should have enough storage memory to process a large amount of digital data and store it for further analysis. However, currently available IoT devices have limited storage capacities, therefore all the recovered digital data are stored in external storage devices.
- **Communication Requirements**: During real-time IoT forensics, strong and smooth communication is critical to ensure that all data are extracted and stored properly without any data tampering.

22.6 Conclusion

The advances in network and communication technologies have helped the IoT technology to connect and communicate billions of things over the Internet and create multiple applications. The IoT can connect almost all physical and virtual objects in the world over the Internet. Although there are indefinite benefits provided by the IoT technology, it introduces novel issues, especially in security. In the same way, IoT forensics has become one of the hottest topics that attract the attention of multiple researchers and organizations especially with the increasing number of cybercrimes. However, due to the heterogeneity of IoT devices, adopting one of the classical investigation frameworks will be ineffective. Therefore, an IoT-based investigation framework should be one of the highest priorities for any organization. This chapter presented an overview of security, cybercrimes and digital forensics of the IoT system. It started by providing a discussion of components and building blocks of an IoT device, essential features, architecture layers,

communication technologies and challenges of the IoT system. Then, IoT security including security threats and solutions regarding IoT architecture layers were presented. Digital forensics and main stages required to perform an investigation process were also discussed. In the end, IoT forensics by reviewing related IoT forensics frameworks, discussing the need for adopting real-time approaches and main challenges of the IoT forensics were discussed.

References

1. Atlam, H.F., Walters, R.J., Wills, G.B.: Internet of Things: state-of-the-art, challenges, applications, and open issues. Int. J. Intell. Comput. Res. **9**(3), 928–938 (2018)
2. Atlam, H.F., Alenezi, A., Alharthi, A., Walters, R., Wills, G.B.: Integration of cloud computing with internet of things: challenges and open issues. In: 2017 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 670–675 (2017)
3. Statista: Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Accessed 15 October 2018
4. Atlam, H.F, Alenezi, A., Walters, R.J., Wills, G.B., Daniel, J.: Developing an adaptive Risk-based access control model for the Internet of Things. In: 2017 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 655–661 (2017)
5. Atlam, H.F., Wills, G.B.: IoT Security, privacy, safety and ethics. In: Digital Twin Technologies and Smart Cities, pp. 1–27. Springer, Switzerland, AG (2019)
6. Perumal, S., Md Norwawi, N., Raman, V.: Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. In: International Conference on Digital Information Processing and Communications (ICDIPC 2015), pp. 19–23 (2015)
7. Madakam, S., Ramaswamy, R., Tripathi, S., Madakam, S., Ramaswamy, R., Tripathi, S.: Internet of Things (IoT): a literature review. J. Comput. Commun. **03**(05), 164–173 (2015)
8. Krotov, V.: The Internet of Things and new business opportunities. Bus. Horiz. **60**(6), 831–841 (2017)
9. Cristina, G.N., Gheorghita, G.V., Ioan, U.: Gradual development of an IoT architecture for real-world things. In: 2015 IEEE European Modelling Symposium (EMS), pp. 344–349. IEEE (2015)
10. Alenezi, A., Atlam, H.F., Wills, G.B.: Experts reviews of a cloud forensic readiness framework for organizations. J. Cloud Comput. (2019)
11. Nair, K., Kulkarni, J., Warde, M.: Optimizing power consumption in IoT based wireless sensor networks using bluetooth low energy. In: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 589–593. IEEE (2015)
12. Shi, Y., Ding, G., Wang, H., Roman, H.E., Lu, S.: The fog computing service for healthcare. In: 2015 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), pp. 1–5 (2015)
13. Ani, J., Gui, X.-L., He, X.: Study on the architecture and key technologies for Internet of Things. Adv. Biomed. Eng. 329–349 (2012)
14. Huang, X., Craig, P., Lin, H., Yan, Z.: SecIoT: a security framework for the Internet of Things. Secur. Commun. Netw. **9**(16), 3083–3094 (2016)

15. Farooq, M., Waseem, M., Khairi, A., Mazhar, S.: A critical analysis on the security concerns of Internet of Things (IoT). Int. J. Comput. Appl. **111**(7), 1–6 (2015)
16. Leloglu, E., Leloglu, E.: A review of security concerns in Internet of Things. J. Comput. Commun. **05**(01), 121–136 (2017)
17. Yehia, L., Khedr, A., Darwish, A., Yehia, L., Khedr, A., Darwish, A.: Hybrid security techniques for Internet of Things healthcare applications. Adv. Internet Things **05**(03), 21–25 (2015)
18. Arseni, S.-C., Halunga, S., Fratu, O., Vulpe, A., Suciu, G.: Analysis of the security solutions implemented in current Internet of Things platforms. In: 2015 Conference Grid, Cloud & High Performance Computing in Science (ROLCG), pp. 1–4. IEEE (2015)
19. Chandrakanth, S., Venkatesh, K., Mahesh, J.Uma, Naganjaneyulu, K.: Internet of Things. Int. J. Innov. Adv. Comput. Sci. **3**(8), 16–20 (2014)
20. Xhafa, F., Bessis, N.: Inter-cooperative collective intelligence: techniques and applications. Springer, Berlin, Heidelberg (2014)
21. Carlo, M.S.A.: An Overview of privacy and security issues in the Internet of Things. McKinsey Q **2**(6) (2013)
22. Atlam, H.F., Walters, R.J., Wills, G.B.: Fog computing and the Internet of Things: a review. Big Data Cogn. Comput. **2**(10), 1–18 (2018)
23. Atlam, H.F., Alenezi, A., Hussein, R.K., Wills, G.B.: Validation of an adaptive risk-based access control model for the Internet of Things. Int. J. Comput. Netw. Inf. Secur. **10**(1), 26–35 (2018)
24. Atlam, H.F., Alenezi, A., Alassafi, M.O., Wills, G.B.: Blockchain with Internet of Things: benefits, challenges, and future directions. Int. J. Intell. Syst. Appl. 40–48 (2018)
25. Pahlavan, K., Krishnamurthy, P., Hatami, A.: Handoff in hybrid mobile data networks. IEEE Pers. Commun. **7**(2), 34–47 (2000)
26. Naimi, L.L., Mark, F.: The Unintended consequences of technological innovation: bluetooth technology and cultural change. IPSI BgD Trans. Internet Res. 50–68 (2010)
27. Ang, Z., Jin, H., Fan, Z., Duan, D.Y: WSN node design and communication realization based on ZigBee protocol. Mod. Electron. Tech. 35–47 (2007)
28. Al-sarawi, S., Anbar, M., Alieyan, K., Alzubaidi, M.: Internet of Things (IoT) communication protocols: review. In: 2017 8th International Conference on Information Technology (ICIT) Internet, pp. 685–690 (2017)
29. Tyagi, S., Darwish, A., Khan, M.Y., Tyagi, S., Darwish, A., Khan, M.Y.: Managing computing infrastructure for IoT data. Adv. Internet Things **04**(03), 29–35 (2014)
30. Jayakumar, H., Raha, A., Kim, Y., Sutar, S., Lee, W.S., Raghunathan, V.: Energy-efficient system design for IoT devices. In: 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 298–301. IEEE (2016)
31. Mulligan, G.: The 6LoWPAN architecture. In: Proceedings of the 4th Workshop on Embedded Networked Sensors—EmNets'07, p. 78. ACM Press, New York, NY, USA (2007)
32. Doukas, C., Maglogiannis, I., Koufi, V., Malamateniou, F., Vassilacopoulos, G.: Enabling data protection through PKI encryption in IoT m-Health devices. In: 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE), pp 25–29. IEEE (2012)
33. Atlam, H.F., Wills, G.B.: Technical aspects of blockchain and IoT. Role Blockchain Technol IoT Appl. Adv. Comput. 1–35 (2018)
34. Sadeghi, A.-R., Wachsmann, C., Waidner, M.: Security and privacy challenges in industrial internet of things. In: Proceedings of the 52nd Annual Design Automation Conference, pp. 1–6 (2015)
35. Mitrokotsa, A., Rieback, M.R., Tanenbaum, A.S.: Classifying RFID attacks and defenses. Inf. Syst. Front. **12**(5), 491–505 (2010)
36. Borgohain, T., Kumar, U., Sanyal, S.: Survey of security and privacy issues of internet of things (2015). arXiv Preprint: arXiv150102211

37. Anwar, Raja Waseem, Bakhtiari, Majid, Zainal, Anazida, Abdullah, Abdul Hanan, Qureshi, K.N.: Security issues and attacks in wireless sensor network. Appl. Sci. **30**(10), 1224–1227 (2014)
38. Sharma, Preeti, Saluja, Monika, Saluja, Krishan Kumar: A review of selective forwarding attacks in wireless sensor networks. Int. J. Adv. Smart Sens. Netw. Syst. **2**(3), 37–42 (2012)
39. Pooja, M., Manisha, S.D.: Security issues and Sybil attack in wireless sensor networks. Int. J. P2P Netw. Trends Technol. **3**(1), 7–13 (2013)
40. Lim, J., Yu, H., Gil, J.: Detecting Sybil attacks in cloud computing environments based on fail-stop signature. Symmetry (Basel) **9**(3), 35–45 (2017)
41. Huang, H., Yin, H., Min, G., Zhang, X., Zhu, W., Wu, Y.: Coordinate-assisted routing approach to bypass routing holes in wireless sensor networks. IEEE Commun. Mag. **55**(7), 180–185 (2017)
42. Kalita, H.K., Kar, A.: Wireless sensor network security analysis. Int. J. Next-Gener. Netw. **1** (1), 1–10 (2009)
43. Ahemd, M.M., Shah, M.A., Wahid, A.: IoT security: a layered approach for attacks & defenses. In: 2017 International Conference on Communication Technologies (ComTech), pp. 104–110. IEEE, (2017)
44. Botta, A., De Donato W., Persico, V., Pescape, A.: On the integration of cloud computing and internet of things. In: Proceedings of the 2014 ACM International Joint Conference on Future Internet Things Cloud, pp. 23–30 (2014)
45. Miessler, D.: Securing the Internet of Things: mapping attack surface areas using the OWASP IoT top 10. In: RSA Conference. https://docplayer.net/6278557-Securing-the-internet-of-things-mapping-attack-surface-areas-using-the-owasp-iot-top-10.html (2015). Accessed 25 Apr 2019
46. Zhao, K., Ge, L.: A survey on the internet of things security. In: Proceedings of 9th International Conference on Computational Intelligence and Security (CIS 2013), pp. 663–667 (2013)
47. Suo, H., Wan, J., Zou, C., Liu, J.: Security in the Internet of Things: a review. International Conference on Computer Science and Electronics Engineering (CCSEE 2012), pp. 648–651 (2012)
48. Jao, D., Miller, S.D., Venkatesan, R.: Expander graphs based on GRH with an application to elliptic curve cryptography. J. Number Theory **129**(6), 1491–1504 (2009)
49. Chung, T., Roedig, U.: DHB-KEY: an efficient key distribution scheme for wireless sensor networks. In: 2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, pp. 840–846. IEEE (2008)
50. Jara, A.J., Ladid, L., Gómez-Skarmeta, A.F.: The internet of everything through IPv6: an analysis of challenges, solutions and opportunities, JoWUA **4**(3), 97–118 (2013)
51. Leloglu, E., Ayav, T., Aslan, B.G.: A review of cloud deployment models for e-learning systems. In: Proceedings of International Conference on Dependable Systems and Networks, pp. 4–10 (2013)
52. Kent, K., Chevalier, S., Grance, T., Dang, H.: Guide to Integrating Forensic Techniques into Incident Response, pp 80–86. Nist Special Publication (2006)
53. Kohn, M.D., Eloff, M.M., Eloff, J.H.P.: Integrated digital forensic process model. Comput Secur. 103–115 (2013)
54. Nik Zulkipli, N.H., Alenezi, A.B., Wills, G.: IoT forensic: bridging the challenges in digital forensic and the Internet of Things. In: Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, pp. 315–324 (2017)
55. Almulla, S., Iraqi, Y., Jones, A.: A state-of-the-art review of cloud forensics. J. Digit Forensics Secur. Law **9**(4) (2014)
56. Ruan, K., Carthy, J., Kechadi, T., Baggili, I.: Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results. Digit Invest. **10**(1), 34–43 (2013)
57. Agarwal, A., Gupta, S., Chand, M.G.: Systematic digital forensic investigation model. Int. J. Comput. Sci. Secur. 118–131 (2011)

58. Pichan, A., Lazarescu, M., Soh, S.T.: Cloud forensics: technical challenges, solutions and comparative analysis. Digit Invest. 38–57 (2015)
59. Ashcroft, J., Daniels, D.J., Hart, S.V.: Forensic examination of digital evidence: a guide for law enforcement. National Institute of Justice, Washington, DC (2004)
60. Macdermott, Á., Baker, T., Shi, Q.: IoT forensics: challenges for the Ioa era. In: 2018 9th IFIP International Conference on New Technologies, Mobility, Security (NTMS 2018), pp. 1–5 (2018)
61. Zawoad, S., Hasan, R.: FAIoT: towards building a forensics aware eco system for the Internet of Things. In: Proceedings—2015 IEEE International Conference on Services Computing (SCC 2015), pp. 279–284 (2015)
62. Chernyshev, M., Zeadally, S., Baig, Z., Woodward, A.: Internet of Things forensics: the need, process models, and open issues. IT Prof. **20**(3), 40–49 (2018)
63. Kebande, V.R., Ray, I.: A generic digital forensic investigation framework for Internet of Things (IoT). In: Proceedings—2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud 2016), pp. 356–362 (2016)
64. Hegarty, R.C., Lamb, D.J., Attwood, A.: Digital evidence challenges in the Internet of Things. Proceedings of Tenth International Network Conference (INC 2014), pp. 163–172 (2014)
65. Raghavan, S.: Digital forensic research: current state of the art. CSI Trans ICT **1**(1), 91–114 (2013)
66. Meffert, C., Clark, D., Baggili, I., Breitinger, F.: Forensic state acquisition from Internet of Things (FSAIoT): a general framework and practical approach for IoT forensics through IoT device state acquisition. In: Proceedings of the 12th International Conference on Availability, Reliability and Security, pp. 1–11 (2017)
67. Hossain, M., Karim, Y., Hasan, R.: FIF-IoT: A forensic investigation framework for IoT using a public digital ledger. In: 2018 IEEE International Congress on Internet of Things (ICIOT), pp. 33–40 (2018)
68. Chi, H., Aderibigbe, T., Granville, B.C.: A framework for IoT data acquisition and forensics analysis. In: 2018 IEEE International Conference on Big Data (Big Data), pp. 5142–5146 (2018)
69. Chhabra, G.S., Singh, L., Varinder, P., Singh, M.: Cyber forensics framework for big data analytics in IoT environment using machine learning. Multimed. Tools Appl. 1–20 (2018)
70. Al-Masri, E., Bai, Y., Li, J.: A fog-based digital forensics investigation framework for IoT Systems. In: 2018 IEEE International Conference on Smart Cloud (SmartCloud), pp. 196–201 (2018)
71. Kebande, V.R., Malapane, S., Karie, N.M., Venter, H.S., Wario, R.D.: Towards an integrated digital forensic investigation framework for an IoT-based ecosystem. In: 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), pp. 93–98 (2018)
72. Taylor, M., Haggerty, J., Gresty, D., Hegarty, R.: Digital evidence in cloud computing systems. Comput. Law Secur. Rev. **26**(3), 304–308 (2010)
73. Oriwoh, E., Sant, P.: The Forensics edge management system: a concept and design. In: 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing, and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC), pp. 544–550 (2013)
74. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of things: vision, applications and research challenges. Ad Hoc Netw. **10**(7), 1497–1516 (2012)
75. Attwood, A., Merabti, M., Fergus, P., Abuelmaatti, O.: SCCIR: Smart cities critical infrastructure response framework. In: 2011 Developments in E-Systems Engineering, pp. 460–464. IEEE (2011)
76. Zulkipli, N.H.N., Alenezi, A., Wills, G.B.: IoT forensic: bridging the challenges in digital forensic and the Internet of Thing. In: Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017), pp. 315–324 (2017)
77. Alenezi, A., Atlam, H., Alsagri, R., Alassafi, M., Wills, G.: IoT forensics: a state-of-the-art review, challenges and future directions. In: The 4th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2019), pp. 106–115 (2019)

78. Alabdulsalam, S., Schaefer, K., Kechadi, T., Le, N.A.: Internet of Things forensics: challenges and case study. In: IFIP International Conference on Digital Forensics, pp. 1–13 (2018)
79. Alqahtany, S., Clarke, N., Furnell, S., Reich, C.: Cloud forensics: a review of challenges, solutions and open problems. In: 2015 International Conference on Cloud Computing (ICCC), pp. 1–9. IEEE (2015)
80. Banafa, A.: IoT and blockchain convergence: benefits and challenges. IEEE IoT Newsl. http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html. Accessed 15 Apr 2019

Chapter 23
Security Vulnerabilities in Traditional Wireless Sensor Networks by an Intern in IoT, Blockchain Technology for Data Sharing in IoT

V. Manjula and R. Thalapathi Rajasekaran

Abstract The Internet of Things (IoT) contributes significantly to transform and modernize the industry and society for digitizing the knowledge, hence that it can be sensed and actuated in real-time. The fast growth of connected devices across the globe anticipated to 50 billion by 2020, due to the intelligent connection of things, people, data, and process. Hence the security complications of IoT applications are essential to deal at various levels, but complexity advances due to the high heterogeneity of devices also lack in performance. A blockchain is a key technology to bring transaction processing and intelligence to devices as well as privacy issues, scalability and reliability problems in the IoT paradigm. The technology inclusion of blockchain and the IoT in the government system could accelerate communication among citizens, companies, and governments.

Keywords Automation · Blockchain · Internet of Things · Security · Privacy

23.1 Introduction

23.1.1 Internet of Things

In the modern digital environment, today we are more connected with the internet-enabled electronic devices. The digital world uses sensors and actuators to interact with the physical world. Internet of Things (IoT) is defined as the entities outfitted with a processor, sensors, and actuators, to communicate with each other to fill a particular need. The Internet has moved toward becoming ubiquitous, is

V. Manjula (✉)
School of Information Technology, Vellore Institute of Technology, Vellore, India
e-mail: manjula.v@vit.ac.in

R. Thalapathi Rajasekaran
Nanosec Infotech Systems, Puducherry, India
e-mail: r.rajthalapathi@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_23

influencing human life in incredible ways by monitoring and controlling a very wide variety of hand-held devices. This tremendous change in behavior of non-living things (objects) to living things (objects) by introducing features like interactions with the real world, smartness to nonliving things. They are interacting with the physical world, work collaboratively to accomplish difficult tasks that involve a high level of intelligence.

The CISCO [1] and IDC [2] forecast report state that the number of IoT devices will be more than the number of populations in the world. But, human populations not a cause for this growth, instead, increase in usage of three to seven digital devices (things) per person in day to day activities (e.g., fans, lights, Refrigerators home appliances and cars). This leads to the fast growth of connected devices across the globe anticipated to 50 billion by 2020. In the physical world, inter-connected things are interacting with machines to humans (M2H), and machines to machines (M2M).

23.1.2 IoT Layered Architecture

Figure 23.1 shows the layer components of IoT Architecture (Jong-Moon Chung, Yonsei University). The IoT devices are built with sensors, actuators, processors, transceivers and several technologies that work together to process and collect data.

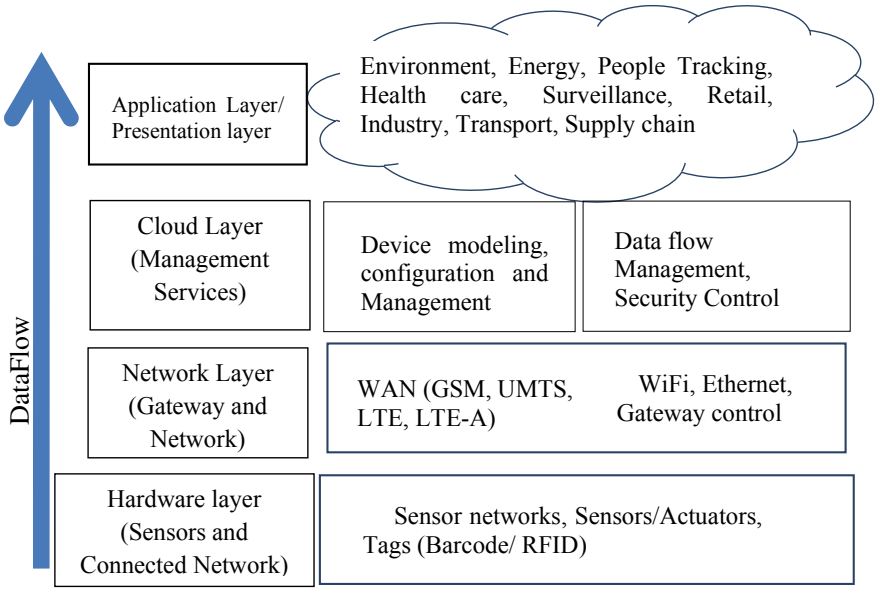


Fig. 23.1 IoT layered Architecture (Jong-Moon Chung, Yonsei University)

Sensor devices and actuator devices are used to interact with the real-world environment.

The IoT devices are generally mounted geologically dispersed locations and they are connected, communicated through the wireless medium. After treating the obtained data, some action required to be considered along the ground of the derived inferences. The nature of actions can be diverse. We can broadcast more or fewer data to other smart things. Sensors, actuators, computer servers, and the communication network form the core infrastructure of an IoT framework is called a hardware layer. This layer also called with different names sensing layer, perception layer [3] and M2M layer. This layer divided into two parts perception node and perceptron networks. IoT devices of sensors or controllers, etc. are part of the perceptron node. The perception network is embedded communication hardware that shares with the transportation network. GPS, Radio Frequency IDentification (RFID) tags, implantable medical devices (IMDs), WSN technology are used in this layer.

The collected data through the sensors have to be stored and processed well to gain valuable results from it. The data storage and processing can be done on the web itself. If any pre-processing is necessary, performed at sensing element or neighboring device. The pre-processed information has been sent to a remote warehousing server, hence the processing ability is too limited in IoT devices. The IoT objects are constraints to their size, vitality, force and processing ability. Hence, this processing is handled by management services in the cloud layer through the internet. Cloud layer is responsible for on-demand storage and computing tools for data analytics and big data. The network layer is gateway and network layer is responsible communication between network to network with Wi-Fi, Ethernet, WAN, LTE to support Internet.

The IoT identifies several application domains like in education, health care, entertainment, energy conservation, social life environmental monitoring, home automation, and transportation, etc. The Application/Presentation layer is responsible for reporting, visualization, and user interfacing.

23.1.3 IoT Application Domains

Figure 23.2 shows the schematic view of end-user and applications fields based on the generation of data on the IoT [4]. The common Internet of Things application domains is home, transport, community, and nation. These domains are interconnected and they are smart home, smart grids, smart city, industrial automation, medical and health care equipment, connected vehicles, etc. Few applications are described below.

The smart city application focuses on two subdomains are smart transportation and smart water systems. Smart transportation function able to manage the city traffics using specialized sensors and provides vital information for further decision making. The objective of the smart transport system is to avoid accidents, to avoid

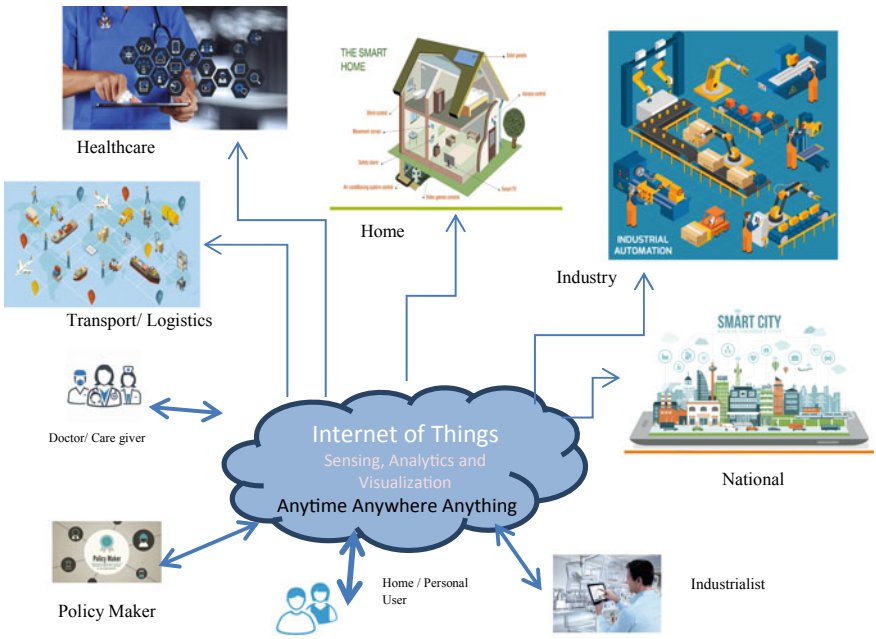


Fig. 23.2 IoT schematic showing the end-users and application

traffic congestion, to guarantee easy and hassle-free parking. The smart water system is used to manage water resources efficiently to get rid of water scarcity in summer and also to predict flood using weather satellite and river water sensors.

23.1.4 IoT Research Challenges

The given research challenges of the Internet of Things in terms of scalability, supportability, processing capability, sustainability, etc., due to massive growth smart things, which connected to the internet [5]. The research challenges are:

i. **Massive Scaling**—A huge number of smart devices being eventually placed and connected in the network, reaches trillions.
ii. **Architecture and Dependencies**—Architecture should allow for easy connectivity, communication, control, and useful application when trillions of things (objects) are connected to the internet.
iii. **Knowledge and Big Data**—It is to develop techniques to convert huge variety and amount of stream data into usable knowledge which is being continuously collected through an IoT world.
iv. **Robustness**—coherent with the neighborhood, reliable service, online fault tolerance, in field maintenance and debugging techniques for a robust system.

v. **Openness**—IoT or sensor domain application is closed-loop control theory. Since controlling activities are automated, actions may not be known; certain actions may require knowing what is happening. Openness may be required in health care, but this leads to security and privacy issues.
vi. **Security and Privacy**—IoT devices are vulnerable to physical attacks because of unattended and remotely placed and accessible; and unsafe wireless communication, internet. Secrecy to be maintained with personal data.
vii. **Human Integration**—i.e., humans and things will operate synergistically. The involvement human being with IoT system is called as human-in-the-loop systems are energy management, health care, and automobile systems applications. The human may involve in control loop are human behavior can be modeled. Here the challenge of how to incorporate the human behavior as part of the system itself.

23.1.5 IoT Security and Privacy Challenges

- IoT devices are often not noticed and remotely placed and accessible which leads to physical attacks.
- In IoT, wireless technology is a communication method, more trendy than wired links. But, the wireless medium is vulnerable and easy to compromise [3]. Hence, security classes interference and interception are vulnerable to wireless technologies. A barrier exists to implement secure and complex security protocols due to the limited high computing resources in the IoT nodes.
- Compromising single point may lead to failure in IoT systems, in the form of a central processing router or gateway. E.g. by Denial of Service attack can severely affect the functionality of the network.

23.1.6 Security for IoT

The recent scenario is highly indicating to as the Internet-of-Everything, which includes the Internet of Things (IoT), Internet of Battlefield Things (IoBT), Internet of Vehicles (IoV), Internet of Medical Things (IoMT) and etc. Security and privacy are two key alarms because of the pervasiveness of such devices in the smart environment, such as smart cities, smart grids, and healthcare systems. The data-sensitive applications such as Healthcare and Military must ensure the privacy and protection of the data, data computations, systems, and connected devices.

The necessity of incorporating ample security in the IoT infrastructure [6] becomes more important in IoT is a key element, because of the enormous amount of growth. Replication of devices (cloning) is a very severe warning in the field of

IoT, due to the simplicity of the environment it becomes easy for the intruder to collect information about configuration and authentication credentials from non-secured node, and re-inject the vulnerable IoT devices in the network [7].

- DoS/DDOS attacks are fine known for the existing Internet, but the IoT is also at risk to similar attacks will require sufficient technique and mechanisms to be disabled or weaken.
- Detection of attacks and get back is to handle with IoT specific threats, such as malicious code hacking attacks and compromised nodes.
- IoT based infrastructures need to be observed with cyber situation awareness tools/techniques. In the lifecycle of the system to take more suitable protective action against attacks and would protect the IoT.
- To support the authorization and usage models that the IoT really needs a mixture of access control and associated accounting schemes due to the heterogeneity and the range of the devices/gateways.
- The IoT wish to handle all modes of action by itself without depending on any human being intervention. To lead to a self-controllable IoT new and sophisticated techniques and methods like machine learning approaches are needed.

23.1.7 Privacy for IoT

With respect to privacy, the information in an IoT system may be personal data; there is a prerequisite to keep the secrecy and limited handling of personal information. The actions are required in many areas are:

i. Cryptographic techniques are used to enable the protection of information to be deposited, processed and shared without the content is accessible to others.
ii. The techniques to be supported for privacy including anonymity, identification, authentication, and data minimization.
iii. Due to the ubiquity and pervasiveness of the IoT devices, a number of privacy implications develop. In order to solve further researches are required, including:

    a. Protection of location privacy, where place can be identified from the things to relevant to people.
    b. The anticipation of personal information by the conclusion, those who would like to keep private, through the surveillance of IoT-related exchanges.
    c. Maintaining the information using key management and decentralized computing is possible as local.
    d. Due to soft identities, where the actual identity of the user can be used to produce different soft identities for specific applications, which can lead to privacy breaches.

23.1.8 Security Threat and Challenges on IoT Features

Table 23.1 summarizes Security Threat, Challenges and openings on IoT features. IoT devices are small, limited-power, internet-connected and able to observing or modifying the physical world. The attacker utilizes this feature and used as a honeypot.

23.1.9 IoT Attack Taxonomy

Figure 23.3 shows the IoT attack taxonomy. IoT attacks categorized based on IoT layers are a physical, network, cloud, and application layer. The Machine to Machine layer attacks is jamming, collision, tampering, deactivation, and exhaustion.

The attacks network layer are hello flood, sinkhole, Sybil, eavesdropping, Denial of Service (DoS), Man in The Middle (MiTM) Attack and selective forwarding attacks. These attacks are also called routing attacks. The Cloud layer attacks are flooding, intersection, spoofing, storage attack, exploit attack and malware attacks. The Application Layer attacks are DDoS, Malicious Code/script injection attack and phishing attack. The security can be classified as perimeter security, network security and information security based on the layer functionality respectively. The autonomic security mechanisms should encompass features of the self-healing and self-protection [8]. Table 23.2 shows the physical attacks features and how it affects security requirements [9]. This table discusses on sensing layer or M2M layer security issue, by an intern about WSN which are at an IoT element of sensing layer [7].

Table 23.1 Security threat, challenges and openings on IoT features

Feature	Threat	Challenge
Interdependence	Bypassing static defenses, over privilege	Access control and privilege management
Diversity	Insecure protocols	Fragmented
Constrained	Insecure systems	Lightweight defenses and protocols
Myriad	IoT botnet, DDoS	Intrusion detection and prevention
Intimacy	Privacy leak	Privacy protection
Unattended	Remote attack	Remote verification
Mobile	Malware propagation	Cross-domain identification and trust
Ubiquitous	Insecure configuration	

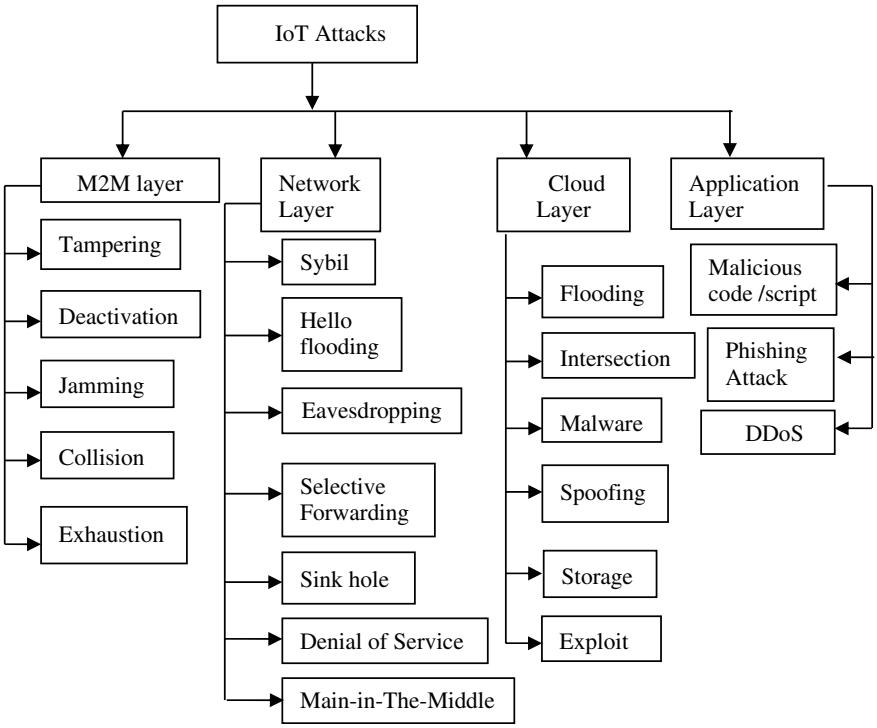


Fig. 23.3 IoT attack taxonomy

23.2 Blockchain Technology

23.2.1 Definition

The blockchain is a principled digital ledger of economic dealings that can be programmed to record not just financial transactions but almost everything of value. Don and Alex Tapscott (authors Blockchain Revolution [10])

Also defined by Seebacher and Schüritz [11] "A blockchain is a distributed database, which is shared among and agreed upon a peer-to-peer network. It consists of a linked sequence of blocks, holding time-stamped transactions that are secured by public-key cryptography and verified by the network community. Once a component is appended to the blockchain, it cannot be changed, turning a blockchain into an unchallengeable record of past activity".

Blockchain is a decentralized ledger technology (DLT), it creates various blocks which hold unique data. Blocks are kept on a different server all over the world. The transactions between two or more parties have been recorded for future reference as block and the end result of blockchain is very hard to corrupt.

Table 23.2 Physical layer attacks and their impacts on security goals

Sl. no.	Types of attack	Attack feature	Security goal requirements
1.	Jamming	The isolated, unmonitored deployment of IoT devices may cause to very high Jamming attack, is a type DoS attack	Threat on availability
2.	Deactivation	A "kill" instruction by unauthorized application or physical destruction of the node, leads to DoS in the multi-hop environment	Threat on availability
3.	Tampering-cause node capture and node replication attack	Physically damage or stop or alter nodes' services Take entire control over the captured node and takeover or compromises the entire WSN/IoT and isolate from any communication The captured node cause displacement or cloning; Software vulnerabilities; Advanced attacker capture IoT devices, record and redistribute it in the area to capture the network and launch a variety of insider attacks, including DoS and DDoS	Threat on confidentiality, availability, integrity, authenticity
4.	Collision	Frequent times of collision leads to a DoS attack. There is a major possibility of collision in IoT, because of the simultaneous occurrence of various set of rules in the WiFi 2.4 GHz band	Threat on availability
5.	Exhaustion	The DoS and tunneling attacks in the network lead to IoT Devices energy exhaustion	Threat on availability

23.2.2 Structure of Blockchain and Working Principle

A blockchain is a growing backward linked-list of records, called blocks, where the blocks are connected using cryptarithmetic. Every block consists of transaction data, a timestamp and cryptographic hash of the previous block. In the Blockchain, tough to corrupt the data of a block and it contains information about the transaction, participants and unique cryptographic block linkage. The first part of the block gives the details about transaction like the amount of purchase, purchase date and time. The second part of the block is given information about who is participating in transactions. The third part is important to distinguish them from other

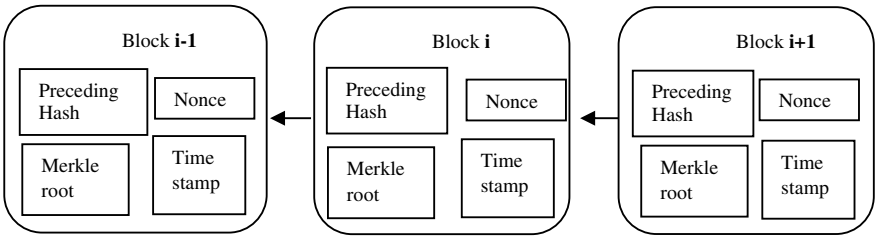


Fig. 23.4 Sample blockchain

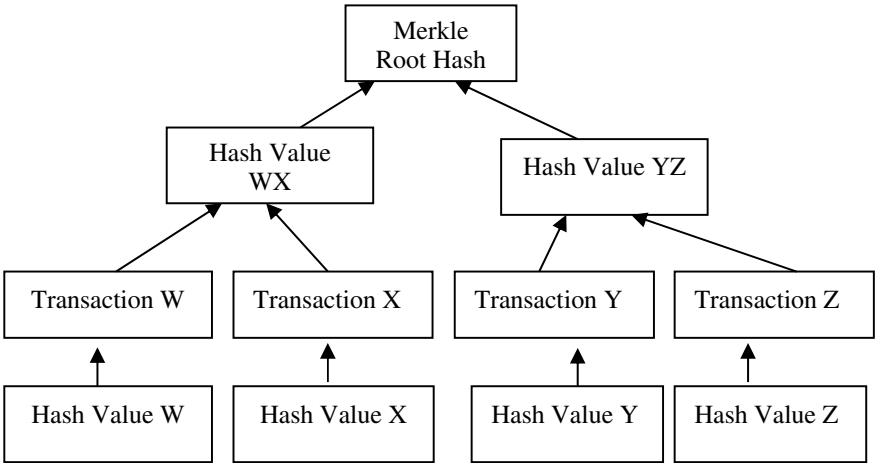


Fig. 23.5 Merkle root hash

blocks by unique Hash code. Figure 23.4 describes the Blockchain, where each block created after the next block holds the hash value of the preceding block's data.

Blocks store information validated by nodes that are cryptographically secured. A blockchain non-recursive append-only. A block on the blockchain capable to store up to 1 MB of data. Figure 23.5 shows the hierarchical structure of a hash tree or Merkle tree, where leaf nodes are labeled with the hash value of block data and Nonleaf node labeled with the hash value of its child nodes labels.

Table 23.3 gives the fields of Block header which contains previous block hash value called as parent block hash. The first block is called genesis block, does not have a parent hash. Figure 23.6 shows the structure of the block [12] which comprises the header and body. In specific, the header consists of version, Merkle tree root hash, block creation time (Time Stamp), nBits, Nonce and hash value of the Parent block. Block version shows which set of block validation rules to be

Table 23.3 Block header

Fields	Description
Block version	Designates the collection of block validation regulations to proceed
Merkle tree root hash	The accumulated hash value of all the transaction in the block
Timestamp	Block creation time (current time as seconds in the universal time)
nBits	Total no of bits which give the target upper bound of a valid block hash
Nonce	A 32-bit field which initializes with zero and increment for subsequent hash calculation
Parent block hash	A 256-bit field which has a hash value that points to the earlier block

followed. The block body comprises counter to give the number of a transaction and transactions details.

A single block can stock a few thousand transactions under one roof subject to the size of the transactions and block size. The position of the block on the chain is called as *height*. The Blockchain validates the authentication of a transaction by asymmetric cryptography.

23.2.3 Characteristics of Blockchain Technology

The two primary characteristics of blockchain technology (Fig. 23.7) are trusted evoking and Decentralized nature [11]. The decentralization feature benefits the formation of a reliable, private, and flexible environment. The integrity of data, Transparency, and immutability are inherent features to facilitate establishing Trust.

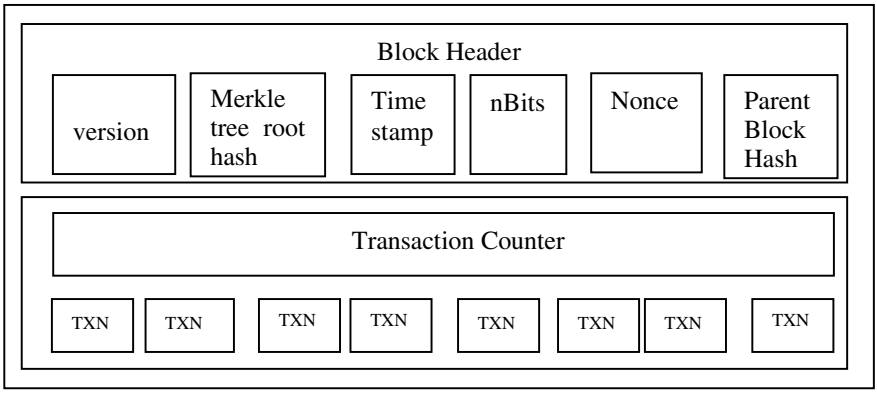


Fig. 23.6 Structure of a block

As blockchain technology is a peer to peer networking, secure communications among the two participants attained by asymmetric key cryptography and the real identities of participants are protected by pseudonyms, called Pseudonymity of participants which ensures a high degree of privacy. Reliability of the system enabled through two factors such as redundancy of data and potential use of automation. The transaction information is stored and shared throughout the networks redundantly and automation reduces the mistakes caused by manual intervention. Blockchain technology makes possible the creation of an open and versatile environment by allowing peer participants to incorporate their own programs and to model their own surroundings by developing and distributing their own codes [13]. For example, a smart contract was a portion of code that serves as an automatic agreement between two parties [14].

Trust [15] attained by ensuring factors of transparency, the integrity of the data and immutability. Transparency has been achieved through recording every action to blockchain and disclosing all transactions records to all the participants in the entire network and cannot be altered or deleted. The new transaction initiated and broadcasted to the entire network and there is no central authority that organizes the system. The users may interact directly, which results in the reduction of friction and ensures trust. Another factor that prompts to trust is the tamper architecture guarantees the immutability by applying consensus algorithm [16] where the transaction added once to a block, it cannot be altered or deleted which in turn added to the blockchain. The integrity of data achieved by storing data directly in the database as well as peer verification of process with all participants and security of transaction attained by public-key cryptography.

In blockchain technology, both trust and decentralization are closely interlinked. The features that ensure the trust are integrity, the immutability of data and transparency. These features are also required in the decentralization of the network in which authentic communications can be achieved without a third party.

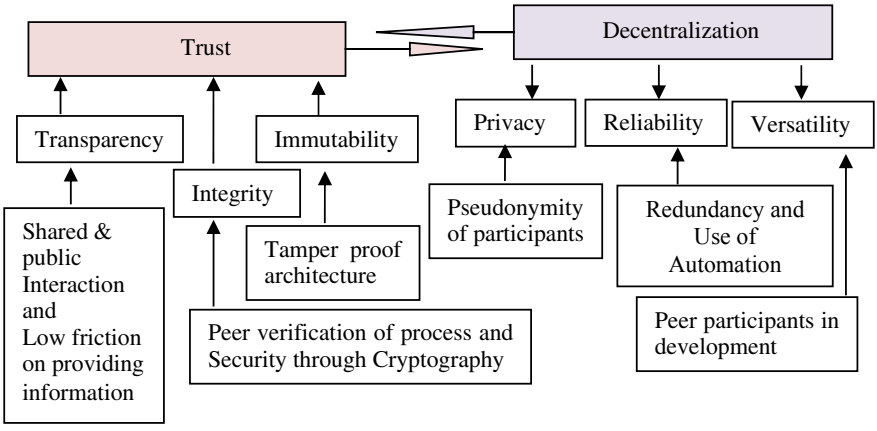


Fig. 23.7 Characteristics and influencing factors of blockchain technology

23.2.4 Classification of Blockchain Technology and Its Features

The blockchain classified based on data accessibility, as public, private, permissioned and permissionless. The Public blockchain has no restrictions permission on accessing blockchain data and transaction submission to include in the Blockchain. But in the private blockchain, limited a predefined list of users, access rights to the blocks and submit the transactions. In a permissionless Blockchain, no restrictions on eligibility for the users to create the transaction blocks and but a permissioned Blockchain has the predefined list of users who can perform the transactions. The public, private and amalgamated blockchain are categories based on the access permissions and network management.

The existing public blockchains implementations are *Bitcoin, Ethereum, Litecoin* and, in common, most cryptocurrencies [17, 18]. The advantage of public blockchain implementations the absence of infrastructure cost, hence its self-sustained network, management overhead reduced. Applications used in private blockchain are performance demanding [12]. An open platform for private blockchain is Multichain [19] used for developing and placing it. Banking and industry use the federated type of blockchain. The tool used for developing federated blockchain is Ethereum. Table 23.4 shows the characteristics of blockchain networks based on their types [20].

Table 23.4 The characteristics of blockchain networks based on their types [20]

Property	Public	Private	Federated
Consensus-PoW	Costly	Light	Light
Mechanism used by	All	Centralized organization	Leader node-set
Identity	(Pseudo) anonymous	Known group users	Known group users
Anonymity	May be Malicious	Trusted	Trusted
Protocol efficiency	Low	High	High
Energy consumption	High	Low	Low
Immutability	Almost impossible	Collusion attacks	Collusion attacks
Ownership	Public	Centralized	Semi-Centralized
Access management	Permissionless	Permissioned whitelist	Permissioned nodes
The time for transaction approval	In minutes	In milliseconds	In milliseconds
Implementations	*Bitcoin, Ethereum, Litecoin*	*Multichain*	*Ethereum*

23.2.5 How Blockchain Resistant to Attack?

Decentralization allows the data to be independent of one central server. The decentralization is an important feature for using blockchain. Computation as well as data collection of the sensor devices done at one spot called centralization. Blockchain uses cryptographic puzzles to provide security. It uses the Proof of Work (PoW) concept for ensuring authorship of transaction/node, required high computational work in the form hash calculation. Addition of new block in the blockchain is called mining and the first block in the chain is called as the genesis block. The block is added at the end of the blockchain, which contains the hash value of its own information and hash of its preceding block. This hash code resistant to alter/modify block and ensures security. Any change in content also reflects in hash code, which affects the verification process, hence blockchain resistant to attack.

The security in blockchain ensured using two processes: signing and verification [21]. Figure 23.8 illustrates how blocks signing and verification processes work in the Blockchain when the transaction took place. The signing process completed with the private key and certificate and the verification process started. During the verification process, the hash value is validated by ensuring hash values are same.

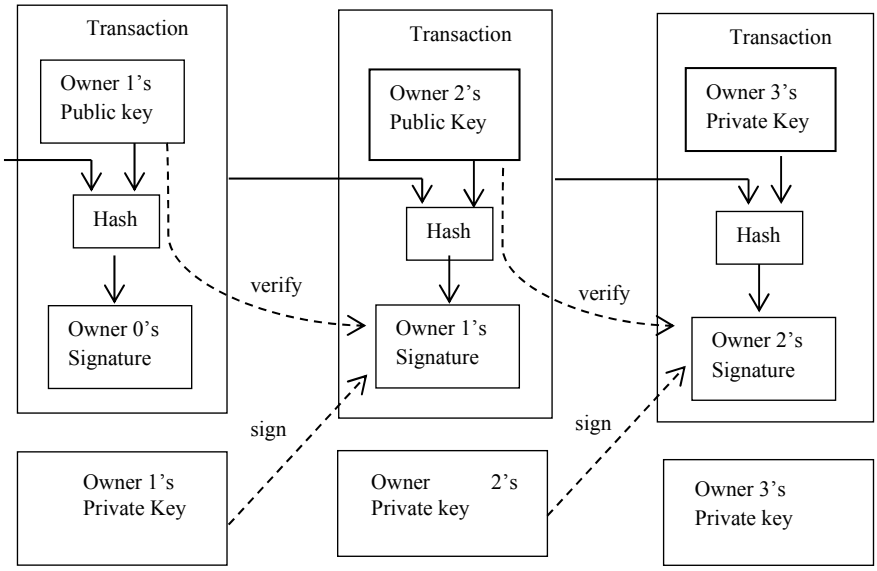


Fig. 23.8 Signing and verification process of transactions

23.3 IoT and Blockchain Integration

In the 4th digital revolutionary Industry, IoT is translating and minimizing the manual process into digital form and obtain huge sources of data from that and gives back as knowledge for further process. This knowledge will provide and administrate the quality of human life through smart applications which also improves the surroundings too. A few years back cloud computing technology has influenced in the area where IoT devices can self capable to make the decision and to proceed the action further into the real-time environment.

In turn, the results of both technologies have proven to be worthy. Similarly, blockchain can improve the IoT with trustable and sharable services, where the data is a reliable one. Data sources are still unchangeable by enhancing their security. If we securely shared the IoT information with the group of members, this would show key changes. For instance, exhaustive discovery in the field of food products is the main objective to confirm food safety. These operations require many participants involvement, like food manufacturer, feeding, treatment, and distribution, etc. Data vulnerability is in the part of the process, the chain could lead to the wrong result and put down the entire process and which may affect the public of the country, huge economic loss to the companies and food sector [22]. Have a good control and proceeds the data sharing among the members will reduce the search time which saves many human lives, also ensures food safety. Moreover, other fields like smart cities, smart homes and smart cars sharing trustworthy information would be possible towards new members improve their services and adoption [23], where this blockchain technology has identified solution for the reliability, privacy and scalability issues related to the IoT paradigm.

23.3.1 Types of IoT and Blockchain Integration

Three types of interactions possible in IoT based on the involvement of blockchain in the communication between the underlying IoT infrastructures [24]. They are IoT inside IoT, IoT and Blockchain integration and A Hybrid design or through blockchain.

(i) **IoT–IoT**: This method provides less delay and high security hence it works offline. The basic quality of the IoT device can capable to share information among them for route discovery and routing mechanism. Blockchain only holds important IoT device information, where IoT communication takes place without using it. This scenario is shown in Fig. 23.9a. This method is suitable where the exchanges exist with low-delay and helpful in the situation with trustworthy IoT data.

(ii) **IoT–Blockchain**: Fig. 23.9b shows, the interaction information among the IoT and blockchain which is not modifiable. Here, all the preferred communications are observable and when their details have been accessed and

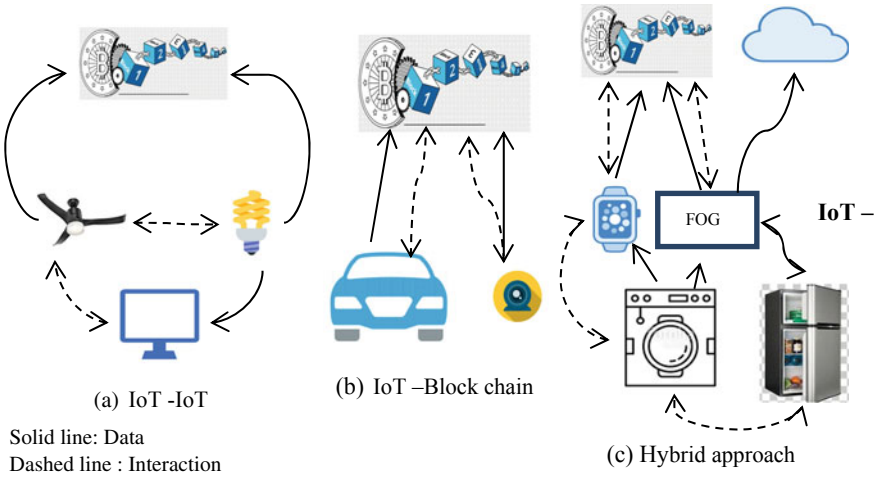


Fig. 23.9 Blockchain integration

viewed by the query in the blockchain. This method increases the smartness of the connected device. Though all the communications are recorded in the blockchain would give way to enhance the bandwidth and data, which invites demand in the blockchain. Also, blockchain stores all the communications related IoT data which demands in bandwidth.

(iii) **Hybrid approach**: Finally, in this method, the design related to the part of IoT's and Blockchain's communication and data part is linked among the IoT devices. One among the major hurdle while using this method is to identify which communication should go via the blockchain during runtime. The arrangement of this method would be the right way to combine these two technologies since both has its own benefits. In this process, to overcome the constraints due to this merge of blockchain and IoT, fog computing and cloud computing technologies are used [25] (Fig. 23.9c).

Alliances between known firms have come together, to aid the two technologies IoT and blockchain. Development of blockchain integrated devices are increasing in the market such as Ethembedded [26] facilitates the fixing of Ethereum nodes on embedded devices like Beaglebone Black, Raspberry Pi, and Odroid. The two projects Raspnode and Ethraspbian [25, 27] both have cryptocurrency full nodes in Bitcoin, Ethereum and Litecoin network on a Raspberry Pi.

Antrouter R1-LTC [28], is a network device (Wi-Fi router) guarantees to mine in Litecoin. Hence, this router mounted in smart homes and act as an edge device of fog computing ecosystem. In Raspnode, extracting interesting pattern performed on IoT devices, but it would be useless since modern mining methods required. There is still plenty of studies is going on to merge IoT devices as blockchain components. The IoT devices suffer various limitations to access, process and store. The cloud infrastructure provides a solution to the above limitations. In spite of that,

additional capabilities required bringing computing closer to end devices, such gateways and edge node can be used as a blockchain mechanism. Hence, edge computing or fog computing could aid this integration to overcome the constraints.

23.4 Secure Data Sharing Using Blockchain in IoT

High-speed communication technology becomes ubiquitous, leverages to interactions among devices (M2M), between machine and people (M2P) as well as technology-assisted interaction among people (P2P). The IoT devices produce data of more than 500 zettabytes per year and grow exponentially due to the usage of IoT technology everywhere (Internet of Everything-IoE) and population growth. By 2020, that number of the IoT devices expected to grow to more than 20 billion due to intelligent interaction among devices, process, people and data.

The integration of two gigantic fields of blockchain technology and IoT technologies may enhance the potential benefits and minimizes the deficiency of one another. The IoT capabilities have been enhanced by minimizing its deficits and maximize its potential abilities [20] by merging with blockchain technology. The objective of this integration is to provide auditable and secure data sharing among intelligent connected devices as well as in diverse sensible scenarios.

As healthcare sector data-sensitive application, blockchain technology provides security in various subdomains like automated health claim negotiation, public healthcare system medical data of the public patients, medical research data, drug imitation, and online access to patients, the accuracy of medicine and clinical trial [29, 30]. In specific, blockchain technology and the use of smart contracts could crack the issues of scientific reliability of results (endpoint switching, missing data, data dredging, and selective publication) in medical experiment [31] as well as problems of patients' informed approval [20].

The major potential growth in the handling of Electronic healthcare patient' record management area, an EHRM consists of patient's medical information, from their clinical report, as well as forecasts and information based on the situation and the clinical development of a patient's entire treatment period. Security and privacy ensured using blockchain method in EHRMs, could be viewed as a procedure through which user can access and upload their health information. The blockchain gives multiple advantages to EHRMs. The information is accumulated in a distributed manner, there is no hub for a hacker to fraudulent or violate, since no owner-centric; the information is updated and available while information from different sources has been collected in a single and integrated information storage area [30].

23.5 Conclusion

IoT Technology will lead a major part in our society for the predictable future, in both military and civilian, internet of battlefield things based on certain IoT based applications, internet of drones (e.g., in military or adversarial contexts), the noticeable IoT vulnerabilities and the possible actions should be automated with minimal human involvement. It is also expected that the blockchain will transform and ensure the security in IoT. This chapter addresses the challenges while the integration of the two technologies'. The technology inclusion of both blockchain and the IoT in the government system could accelerate communication among citizens, companies, and governments.

References

1. Evans, D.: The Internet of Things—How the Next Evolution of the Internet Is Changing Everything. CISCO White Paper (2011)
2. Weissberger, A.: IoT Forecast, 5G & Related Sessions. In: IDC Directions Conference, 28 Feb 2017. Santa Clara, CA. http://techblog.comsoc.org/2017/03/04/idc-directions-2017-iot-forecast-related-sessions/ (2017)
3. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in internet-of-things. IEEE Internet Things J. **4** (5), 1250–1258 (2017). https://doi.org/ 10.1109/JIOT.2017.2694844
4. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29** (7), 1645–1660 (2013). https://doi.org/10.1016/j.future.2013.01.010
5. Stankovic, J.A.: Research directions for the internet of things. IEEE Internet Things J. **1** (1), 3–9 (2014). https://doi.org/10.1109/JIOT.2014.2312291
6. Vermesan, O., Friess, P., Guillemin, P., Sundmaeker, H., Eisenhauer, M., Moessner, K., Le Gall, F., Cousin, P.: Internet of things strategic research and innovation agenda. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, pp. 7–151. River Publishers (2013)
7. Lee, P.-Y., Yu, C.-M., Dargahi, T., Conti, M., Bianchi, G.: MDSClone: multidimensional scaling aided clone detection in internet of things. IEEE Trans. Inform. Forensics Secur. **13** (8), 2031–2046 (2018). https://doi.org/10.1109/TIFS.2018.2805291
8. Ashraf, Q.M., Habaebi, M.H.: Introducing Autonomy in Internet of Things, pp. 215–221. WSEAS Press (2015)
9. Manjula, V.: Resilient protocols for node replication attack mitigation in WSN (2014). http://ir.inflibnet.ac.in:8080/jspui/bitstream/10603/33721/5/05_content.pdf
10. Tapscott, D., Tapscott, A.: Blockchain Revolution. Penguine Random House, New York (2016)
11. Seebacher, S., Schüritz, R.: Blockchain technology as an enabler of service systems: a structured literature review. In: International Conference on Exploring Services Science, pp. 12–23. Springer (2017)
12. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. IEEE (2017). https://doi.org/10.1109/bigdatacongress.2017.85

13. Ølnes, S.: Beyond bitcoin enabling smart government using blockchain technology. In: Scholl, H.J., Glassey, O., Janssen, M., Klievink, B., Lindgren, I., Parycek, P., Tambouris, E., Wimmer, M.A., Janowski, T., Sá Soares, D. (eds.), Electronic Government: 15th IFIP WG 8.5 International Conference, EGOV 2016, pp. 253–264. Springer International Publishing, Cham (2016)
14. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc. (2015)
15. Trusted IoT Alliance. Available online: https://www.trustediot.org/ (2017). Accessed: 01 Feb 2018
16. Nguyen, G.T., Kim, K.: A survey about consensus algorithms used in Blockchain. J. Inf. Process. Syst. **14**(1), 101–128 (2018)
17. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
18. Haferkorn, M., Quintana Diaz, J.M.: Seasonality and interconnectivity within cryptocurrencies—an analysis on the basis of Bitcoin, Litecoin and Namecoin, pp. 106–120. Springer International Publishing, Cham (2015)
19. Greenspan, G. (2015). MultiChain Private Blockchain — White Paper [PDF]. Retrieved from https://www.multichain.com/download/MultiChainWhite-Paper.pdf
20. Casino, F., Dasaklis, T.K., Patsakis, C.: A systematic literature review of blockchain-based applications: current status, classification, and open issues. Telematics Inform. (2019). https://doi.org/10.1016/j.tele.2018.11.006
21. Golosova, J., Romanovs, A.: The advantages and disadvantages of the blockchain technology. IEEE 6th Workshop Adv. Inform. Electr. Electric. Eng. (AIEEE) 1–6 (2018)
22. Buzby, J.C., Roberts, T.: The economics of enteric infections: human foodborne disease costs. Gastroenterology **136**, 1851–1862 (2009)
23. Malviya, H.: How blockchain will defend IoT. Available online: https://ssrn.com/abstract=2883711 (2016). Accessed: 01 Feb 2018
24. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. **88**, 173–190 (2018). https://doi.org/10.1016/j.future.2018.05.046
25. Raspnode. Available online: http://raspnode.com/ (2017). Accessed: 01 Feb 2018
26. Ethembedded. Available online: http://ethembedded.com/ (2017). Accessed: 01 Feb 2018
27. Ethraspbian. Available online: http://ethraspbian.com/ (2017). Accessed: 01 Feb 2018
28. Ant router R1-LTC the WiFi router that mines Litecoin: Available online: https://shop.bitmain.com/antrouterr1ltcwirelessrouterandasiclitecoinminer.htm (2017). Accessed: 01 Feb 2018
29. Mettler, M.: Blockchain technology in healthcare: the revolution starts here. In: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1–3. IEEE (2016)
30. Wang, S.-Y., Hsu, Y.-J., Hsiao, S.-J.: Integrating blockchain technology for data collection and analysis in wireless sensor networks with an innovative implementation. In: International Symposium on Computer, Consumer and Control (IS3C) (2018)
31. Nguyen, Q.K.: Blockchain—a financial technology for future sustainable development. In: Proceedings—3rd International Conference on Green Technology and Sustainable Development, GTSD 2016, pp. 51–54 (2016)

Chapter 24
Blockchain for Security Issues of Internet of Things (IoT)

Riya Sapra and Parneeta Dhaliwal

Abstract Today in the data driven world, technology has amazed us and changed our life completely. Internet of Things (IoT) has made our life easy by making conventional devices like air conditioner, mobile phones etc. autonomous and smart by revolutionizing the machine to machine communication. IoT is able to represent the real world digitally through the deployment of smart applications in various domains. These applications generate enormous amounts of data and also require internet connectivity all the time for communication between the devices. As the data is communicated via wireless networks, the major challenge lies in the domain of security such as data confidentiality, data reliability, data authentication, privacy etc. Blockchain can be the missing link for settling privacy, and reliability issues of IoT. The connected devices and their communications can be tracked and stored on the tamper-proof ledger of blockchain to ensure reliability and data security of IoT network.

Keywords Internet of things · IoT · Blockchain · Security · Privacy · Authentication · RFID · Bluetooth · Applications

24.1 Introduction

With the advent of 5G technology, the mobile networks are getting faster and faster, which is moving everyone and everything to the online world. Every person is connected to the other via internet. The scope of internet in this twenty-first century has increased to the extent that machines also connect and communicate with each other via internet connectivity; this is also called as Internet of Things (IoT). IoT in

R. Sapra · P. Dhaliwal (✉)
Department of Computer Science and Technology, Manav Rachna University, Faridabad, Haryana, India
e-mail: parneeta07@gmail.com

R. Sapra
e-mail: riasapra@gmail.com

S.-L. Peng et al. (eds.), *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Intelligent Systems Reference Library 174,
https://doi.org/10.1007/978-3-030-33596-0_24

simple terms means Internet connected devices which collaborate to complete complex tasks using sensors and actuators. The concept has become a powerful technology to connect everyday objects and convert them into smart objects which can interact with each other and work without human intervention. This makes them susceptible to numerous security threats and privacy issues. These issues majorly arise due to the centralized collection of data or it's processing at the cloud server. Data security and privacy are the most important concerns in devices using IoT. There have been various data thefts due to spoofing [1], eavesdropping [2], unauthorized access [3] and much more.

The devices of IoT are susceptible to a number of security and privacy issues which is most of time ignored or neglected. IBM [4] suggested reviving the centralized yet costly architecture of IoT to a self-managed and self-regulating decentralized architecture which will bring reduced cost, autonomy, security and trust to the IoT environment against network attacks [3]. For this blockchain is the perfect solution for the centralized architecture of IoT. Initially blockchain was considered for financial applications only but because of its decentralized behavior, fault tolerance, immutability, transparency and integrity, it is being used in wide application areas like Big Data [5, 6] cloud computing [7], financial application [8] etc.

Blockchain uses cryptographic hashes to store user's identity and transactions which provides a trust [9] factor to the transactions happening in real time. Also the consensus algorithm makes sure that no false transaction is added to the block by verifying it from the peers. Blockchain is robust and immutable which makes it suitable for resolving the privacy and security concerns of IoT.

24.1.1 Internet of Things (IoT)

The term IoT was first used [10] in 1999 by Kevin Ashton and then formally announced in 2005 by International Telecommunication (ITU). IoT connects devices by attaching embedded sensors to the objects which enable the object to hear, see and act as per the program via internet. This transforms the traditional objects into smart objects paving the way to ubiquitous computing [11], fog computing [12] and much more. The technology is being used in every field of society whether it is homes, offices, schools, bus-stops, railway stations etc. The main aim is to connect the physical and the digital world.

IoT is improving quality of life through various home and business applications. Smart homes [13] provide light automation, AC temperature control, AC automatic on/off, water heater heats automatically at a particular time, TV starts as soon as you reach home, open/close garage, automatic fish/pet food feeder, etc. The devices work automatically as programmed. The other applications include smart electric meter [14], greenhouse monitoring system [15], telemedicine monitoring [16] etc.

24.1.1.1 Features of IoT

IoT has amazed everyone by its capability to automate devices and revolutionize the internet world. Some of the features of the technology are:

- **Connectivity**: IoT is an anytime, anywhere network. The objects or devices in the network must be connected to IoT platform [14] in order to communicate with each other. This connectivity is only feasible through internet. All the devices need high quality internet connectivity so as to establish a high speed messaging service between the devices of the IoT network for a secure bi-directional communication.
- **Sensing**: 90% of the IoT enabled devices have embedded sensors in them to detect the actions happening in the environment. These sensors get activated whenever there is a change or any event happens e.g. The door sensors [13] get activated when it is opened which will communicate the action to the other devices like lights, fans, AC etc.
- **Intelligence**: IoT is meant to make things smart which work either at a specific time or upon a specific action. For example Coffee Maker [13] makes coffee as soon as you enter home or it orders coffee supplies itself whenever the material is going to end.
- **Real Time analysis**: All the devices work in real time scenario, the data or messages are communicated without any delay. In case of sensitive applications like smart car [17], real time analysis of data is critical.
- **Scalability**: In recent scenario, the number of devices [17] connecting to IoT network is increasing day by day due to the massive increase in application areas possible through IoT. This requires the IoT application to be scalable enough to cater the future need. Also the data generated from these devices is too high which requires huge devices to store and process data.
- **Architecture**: Architecture [18] adopted by various applications of IoT will be different from one another as every IoT network needs to connect multiple devices from different manufacturers. This sometimes requires a new architecture design whenever this is a new functionality added to the IoT application.

24.1.1.2 IoT Architecture

IoT must be capable of connecting millions of heterogeneous devices via internet which arise the need of flexible layered architecture. Various layered architectures [19] have been proposed so far by various authors as there is no single consensus for the standard architecture of IoT. Every application of IoT has a different requirement which is the deciding factor for choosing the 3/4/5 layered architecture. All these architectures perform almost the same set of tasks: connecting all the devices wired or wirelessly, gathering and processing data and using the processed data to do the automated tasks.

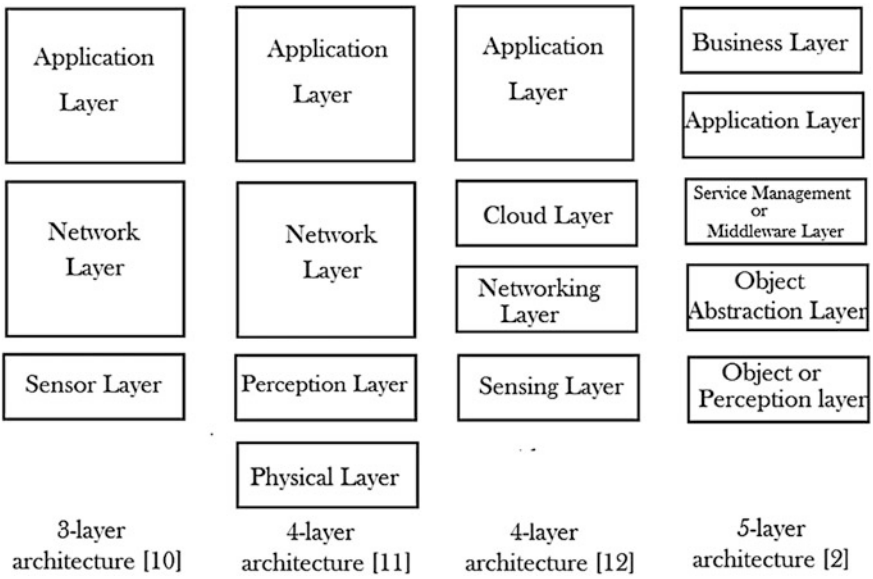


Fig. 24.1 Comparison of layered IOT architecture

A basic three layered architecture [18] consist of sensor, network and application layer. Other applications [10, 20, 21] need more abstraction, so they add more layers to their architecture. The comparison of different layered architecture proposed is shown in Fig. 24.1 Physical layer consist of basic hardware like power supply, smart appliances etc. Object/Perception/Sensor/Sensing layer collects the data from sensors of the objects. The network layer transfer data within devices or from devices to the receivers. Object abstraction layer transfers data which is produced by object layer to the service management layer. Service management/ Cloud layer processes the data, makes decision and updates the application layer. Application layer provides control mechanism and management of application. Business layer helps in analysis of data for building business model, flowcharts based on data analytics from application layer.

24.1.1.3 IoT Technology and Protocols

IoT works on connectivity of devices. For the network to work in an effective manner, the real time transmission of data is required. There are numerous ways for connectivity of devices like Bluetooth, Wi-Fi, cellular etc. These protocols differ in terms of frequency, range, application requirements or data rates etc. The details of the various protocols are discussed and their comparison is given in Table 24.1.

- **Bluetooth**: It is short- range wireless technology protocol to transfer data between short distance devices. Initially, it was used for wireless headsets.

Table 24.1 Comparison of various IoT protocols

Protocol	Standard	Frequency	Range	Data Rate
Bluetooth	Bluetooth 4.2	2.4 GHz	50–150 m	1 Mbps
Zigbee	ZigBee 3.0 based on IEEE 802.15.4	2.4 GHz	10–100 m	250 kbps
Z-Wave	Z-Wave Alliance ZAD12837/ ITU-T G.9959	900 Hz	30 m	9.6/40/100 kbps
Wi-Fi	Based on IEEE802.11n	2.4 GHz & 5 GHz bands	~50 m	150 bps to 1 Gbps
Cellular	GPRS/EDGE (2G), UMTS/ HSPA (3G), LTE (4G)	900/1800/1900/ 2100 MHz	GSM: 35 km HSPA: 200 km	GPRS: 35–170 kbps EDGE: 120–384 kbps UMTS: 384–2Mbps HSPA: 600–10 Mbps LTE: 3–10 Mbps
RFID	ISO/IEC 18000 ISO/IEC 29167 ISO/IEC 20248	120 kHz–10 GHz	10 cm to 200 m	N/A
NFC	ISO/IEC 18000-3	13.56 MHz	10 cm	100–420 kbps
Sigfox	Sigfox	900 MHz	Rural: 30–50 km Urban: 3–10 km	10–1000 bps
6LoWPAN	IEEE 802.15.4 based network	868 MHz, 915 MHz, 2.4 GHz	10–30 m	20 kbps to 250 kbps
Neul	Neul	ISM: 900 MHz UK: 458 MHz White Space: 470–790 MHz	10 km	Up to 100 kbps

Now it is used in a variety of applications like Bluetooth mouse, speaker, printer, barcode scanners etc. Bluetooth works best for low power devices in short radius. It is the key protocol for wearable devices like smart watches. It works in a frequency band of 2.4 GHz, within a radius of 50–150 m and may transmit at 1 Mbps.

- **Zigbee**: Zigbee is another IoT protocol that offers high security, low energy operation, high scalability and robustness. It is used in devices where data is not required frequently and devices are held nearby as it operates in a very short range. Zigbee is used to create personal area network to be used in small scale projects like wireless light switches, traffic management system, home automation system etc. Like Bluetooth, it has a frequency band of 2.4 GHz. It transmits within a radius of 50–100 m with a low data rate of 250 kbps only.
- **Z-wave**: Z-wave is a low energy radio wave technology to transmit data between devices. It is majorly used in home automation devices like security systems, windows, garage door openers, coffee maker, lighting control, locks,

thermostats and swimming pools. It is meant for a reliable communication protocol for sensor enables devices. It has a frequency of 900 Hz with a low transmission range of 30 m only and a low data rate of up to 100 kbps.

- **Wi-Fi**: Wi-Fi is a popular wireless technology for high speed internet. It is used for creating wireless local area network (WLAN) to connect a large number of devices. It is suitable for fast transfer and processing of data but may consume high power. Wi-Fi is based of IEEE family of 802.11 standards and serves in two frequency bands of 2.4 and 5 GHz. It creates WLAN in a range of 30 m only and provides high data rates of up to 1 Gbps depending on the network connection type.
- **Cellular**: Cellular communication is capable of sending large quantity of data at a long distance. There are various categories of cellular network which operates in different frequencies and have different data rates. With every growing generation (2G/3G/4G/5G and so on) of cellular technology, the data rates get faster with increased power requirement. Cellular connectivity has different formats like GSM, GPRSM, LTE etc. which works in different frequency bands and provide different data rates and ranges as shown in Table 24.1 depending on the standard used for cellular connectivity.
- **RFID**: Radio Frequency Identification is an IoT protocol which is used to identify and track objects with RFID tags with the help of electromagnetic fields. It is being used in various industries for Automatic Identification and Data Capture (AIDC) to track the progress and location of objects. It can be attached or implanted to clothes, pets, cash, goods in factory etc. RFID also works in various frequency bands ranging from 120 kHz to 10 GHz and in the range of 10 cm to 200 m.
- **NFC**: Near Field Communication is a simple, low energy and short range IoT protocol for data exchange between electronic devices at a very close distance of less than 10 cm. It is majorly used in smartphones to share digital content, do contactless payment etc. It uses the frequency band of 13.56 MHz with a data rate of 100–420 kbps.
- **Sigfox**: Sigfox uses ISM bands to transmit data between the connected devices. It is used in applications which have low data transfer requirement and have small batteries. It is suitable for M2M applications like smart meters, street lighting, patient monitors, environmental sensors etc. It uses the frequency band of 900 MHz and serves in area ranging from 3 to 50 km depending on the region where it is used. It has a low data speed of 10–1000 bps.
- **Neul**: Neul uses small spectrum of TV White Space and deliver high coverage, high scalability, low cost and low power wireless networks. It is also called weightless, as it competes against 3G, GPRS, LTE and CDMA WAN solutions. Data rates vary from a few bits to 100 kbps on the same single link. It uses 3 different frequency bands: ISM, UK, White Space with 900 MHz, 458 MHz,470–790 MHz frequencies respectively. It can serve an area up to 10 km.
- **6LoWPAN**: 6LoWPAN is an IPV6 based IoT protocol used for Low Power Wireless Personal Area Network. It is used widely in small devices which have

limited power batteries and low data rates requirements. It also uses 3 different frequency bands of 868 MHz, 915 MHz and 2.4 GHz for an area within 10 km with a data rate of 100 kbps.

24.1.1.4 Working of IoT

IoT consist majorly 4 main components: sensors, devices connectivity, data processing and user interface which makes all M2M communication possible as shown in Fig. 24.2. The components are as follows:

- **Sensors/devices**: Sensors [13] are tiny/minute objects embedded to all the IoT machines/devices to collect information. These devices have the capability to collect very minute data from the surrounding environment.
- **Connectivity**: The data collected by sensors/devices is sent to a cloud infrastructure [22] through any of the protocols discussed above in Sect. 1.1.3.
- **Data Processing**: The data on cloud is then processed according to the application requirement and then used to perform the required task for the particular device in the IoT network.e.g. If the sensor is checking the temperature in the room, it will direct the AC to update its temperature according to the room temperature.
- **User Interface**: The information is made available to the end-user in many ways like by triggering alarms, on mobile phones or device display etc.

24.1.1.5 Applications of IoT

The technology has found its place in wide area of applications. The technology is being used in homes, offices, industries, healthcare, farming and everywhere. It has been accepted well for both commercial and personal purposes. IoT has helped ease

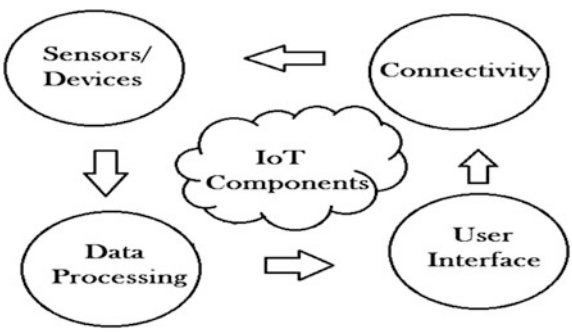


Fig. 24.2 Components of IoT

everyone's life by automating things and providing all the useful information. Lots of industries are using IoT for automating their tasks in their organization. People are using IoT application for their ease, health and entertainment too. Wearable devices like smart watches are a trend now a day. RFID tags embedded in clothes are also being used for security purposes by military. Few of applications are listed in Table 24.2.

Table 24.2 Applications of IoT

Application	Features	Examples/Prototype
Smart home [13]	• Weather sensor • Smoke detector • Automatic temperature controller • Smart lights • Door sensor • Pet feeder • Motion sensor	• Nest learning Thermostat • Ecobee • Amazon echo • August • Philips hue light bulbs • Homey • The air quality egg
Smart healthcare [16]	• Glucose monitoring • Medication dispensers • Smart beds • Real-time monitoring & tracking • Remote medical assistance	• Medtronic GUARDIAN • Philips' medication • Dispensing service • Future path medical's UroSense
Wearables [19]	• Smart watches • Bracelets • Glasses • Insoles—soles in shoe	• Toyota mobility band • Fitbit ChargeHR • Jawbone UP2 • MIT insoles
Connected cars [22]	• Vehicle tracking • Automated emergency management • Real time fleet management • Predictive maintenance	• KaaT connected cars • BMW • Apple • Google
Industrial Internet of Things [60]	• Embedded data collector • Industrial machines monitoring • Data collaboration and processing	• ABB's smart robotics • Amazon's reinventing warehousing • Bosch's track and trace innovator
Smart city [22]	• Garbage bin full detection • Pollution updates • Parking available update • Smart lights • Automatic accident alerts	• Bigbelly smart waste and recycling system • CitySense—smart street lighting • Libelium—Metiora smart parking Sigfox Kit
Smart farming [61]	• Automatic soil quality check update • Automatic water/chemical feeder • Crop nutrient meter	• CleanGrow's carbon nanotube probe • The Open IoT phenonet project

(continued)

Table 24.2 (continued)

Application	Features	Examples/Prototype
Smart grid [14]	• Smart electricity meter • Smart lighting • Automatic faulted circuit indicators • Smart appliances	• Solvera Lynx smart grid • Infographic smart grid • VPP energy smart grid • NEMESYS smart grid
Smart retail [62]	• Smart identification card • Self-billing trollies • Object location identification	• METRO group future Store initiatives • TCIs' smart retail solution
IoT in poultry [63]	• Remote monitoring and management • Real time temperature & humidity maintenance	• PoultryMon

24.1.2 Blockchain

Blockchain [23] is the technology that gained popularity from the onset of cryptocurrencies [24]. It consists of chain of blocks that contain transactions in chronological order. Every block [25] is linked to one another to form a chain by storing root hash of the previous block. Some important concepts of blockchain are as follows:

Transaction: Transaction records happening of an event. In a financial application [8], transfer of any asset or exchange of any value or goods is a transaction. In a healthcare application [26] for data management, any exchange or storing of information is a transaction. In smart contracts [27], any event happening or executing of the arbitrary code is a transaction. So transaction can be any financial transfer, any event change, code execution or data transfer depending on the platform and application for which blockchain is used.

Hash: Blockchain uses the concept of cryptographic functions [25] to store transactions and user identities on the network. These functions take any length input to produce a fixed length output. Even when there is a very small change in input, the output produced by the cryptographic function is totally different which makes it almost impossible to hack. Converting into hashes is also called encrypting the transactions or identities. There are various cryptographic functions like MD2, MD4, MD5, MD6, SHA-0, SHA-1, SHA-2, SHA-3, RIPEND, RIPEMD-128, RIPEMD-160 etc. Table 24.3 shows example of hash generated by MD5.

Block: A block [23] in a blockchain network consists of set of transactions validated by the peers in the network. These transactions are stored in the form of hashes in chronological order. The block has a predefined size as per the blockchain platform. When the block has sufficient number of transactions, it is broadcasted to the network for being appended to the existing blockchain. Figure 24.3 shows the structure of a block in blockchain.

Table 24.3 Hash produced by MD5

Data (string)	Hash produced (MD5)
A sent 10,000 to B	ff81804c4ad895207037929ec7991c9f
A sent 1000 to B	32e85b0110b78369cc973cae73957958
B sent 10,000 to A	7180d213d9c2e77e11789f00dcf805fb
B sent 1000 to A	5fb4d5ad0a1564bf6f3227c31b2ccc50

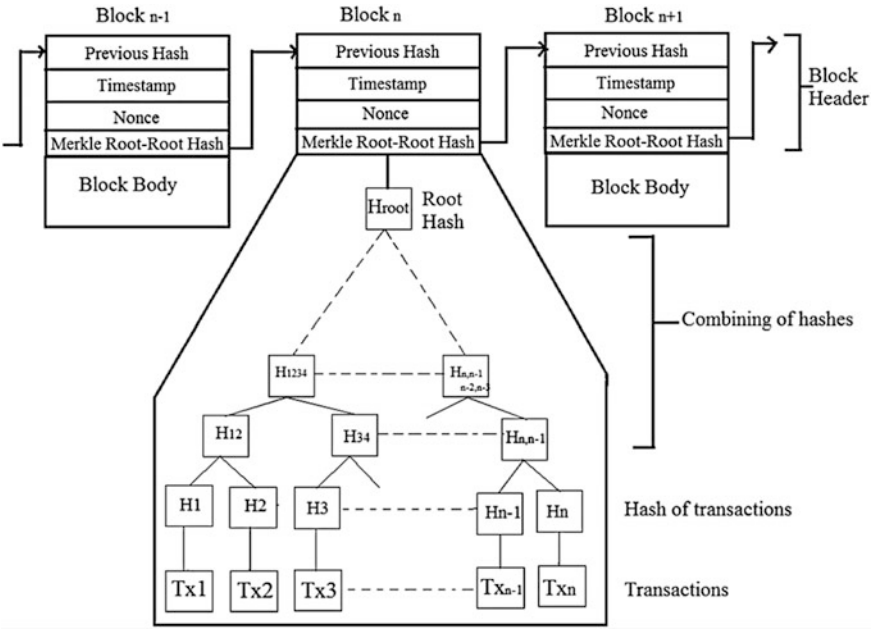


Fig. 24.3 Structure of blockchain

Block header: Every block has two parts: block header and block body. The body of block consists of the transactions stored in block. Block header consists of four components:

- **Merkle Root Hash**: It is the root hash of the block. It is evaluated by combining hashes of the transactions level by level as shown in Fig. 24.3. The transactions of the block are first converted to hashes using cryptographic function. Two adjacent hashes are combined to form one hash at each level till one root hash is evaluated.
- **Previous Root Hash**: It is the root hash of the previous block. All the blocks are connected to each other via previous root hash forming a chain of block.

- **Nonce**: Nonce in the block header is a number, generally a 32 bit number whose value is found by miners so that hash of the block is less than or equal to the current target of the network.
- **Timestamp**: Timestamp indicates the time of creation of the block.

Mining: Mining is the process of creation of block which includes gathering the transactions happening in real time, validating them from peers, converting into hashes, finding the root hash and nonce. Lots of miners involve in mining process. Miners in the blockchain are chosen depending on the category of the blockchain network. As different miners are mining the block at the same time, only one of the blocks created by miners is selected depending on the consensus protocol of the network and is appended to the blockchain. Generally there are rewards for the miner for creating blocks.

Node: Anyone involved in the blockchain network is called peer/node. Node can a miner or the one doing transactions. Depending on the type of task done by node, they can be categorized in three categories.

- **Simple Node**: Nodes involved in doing/sending/receiving transactions are called simple nodes. They are not involved in mining or validating the transactions. Simple nodes don't store the copy of blockchain.
- **Full Node**: Full nodes are also called validator nodes. These nodes store the complete copy of blockchain and help in validating the transactions to be appended to the new block.
- **Miner Node**: Miner nodes also store the complete copy of the blockchain and mine the transactions to create new block for the blockchain. Miner nodes in blockchain compete with each other for their block to be accepted in the blockchain.

Consensus Protocol: Consensus is a method of achieving agreement on one value among peers in a distributed computing system. In blockchain, consensus protocol is the mechanism of choosing the correct block to be appended to the blockchain. It will bring all the peers on a single state of the blockchain network. Proof of Work [24] is the first consensus protocol for the first blockchain application Bitcoin. Other consensus protocol include Proof of Stake [28], Proof of Burn [29], Practical Byzantine Fault Tolerance [30] etc.

Smart Contract: Smart Contract [31] is the programmed category of blockchain which is coded with prior set of rules and milestones to work automatically without the requirement of any third party. These contracts are stored on blockchain and track the progress of operations happening in real time. The concept of smart contract is majorly used in online voting [32], mortgage loans [33], insurance [34], supply chain management [9], protecting copyrighted content [32] etc.

24.1.2.1 Features of Blockchain

Blockchain is a widely accepted technology for a vast area of applications because of its security and fault tolerance. It is distributed computing platform which store data using cryptographic algorithms in an append only manner and makes it tamper proof. Although the concepts of cryptographic functions, consensus and distributed computing are decades old but they got popular with the advent of blockchain in Bitcoin [24]. And then researchers found the technology to be useful in many domains. Blockchain is accepted by various organizations to do their operations like Block and chain game studios [35] uses blockchain as a gaming platform, Corda [8] uses blockchain in supply chain management. Following are some of the features of blockchain as shown in Fig. 24.4:

- **Decentralized**: Blockchain is a decentralized ledger [25] technology in which all the participants of the network maintain a ledger with themselves which have all the validated transactions stored in it and helps in its maintenance by validating and sharing the transactions happening in the network. If few nodes are down in the network, the blockchain network works efficiently as the copy of transactions already happened is with everyone in the network and hence doesn't suffer from single point of failure as in centralized architecture.
- **Cryptographically secured**: All the transactions in blockchain are stored using cryptographic functions [33]. While creating a block, the transactions are stored after being converted into their corresponding hashes. Also the blocks are addressed by root hashes which are made by combining the hashes of all the transactions in the block. This makes it secure from the attackers or any intruder within the network.

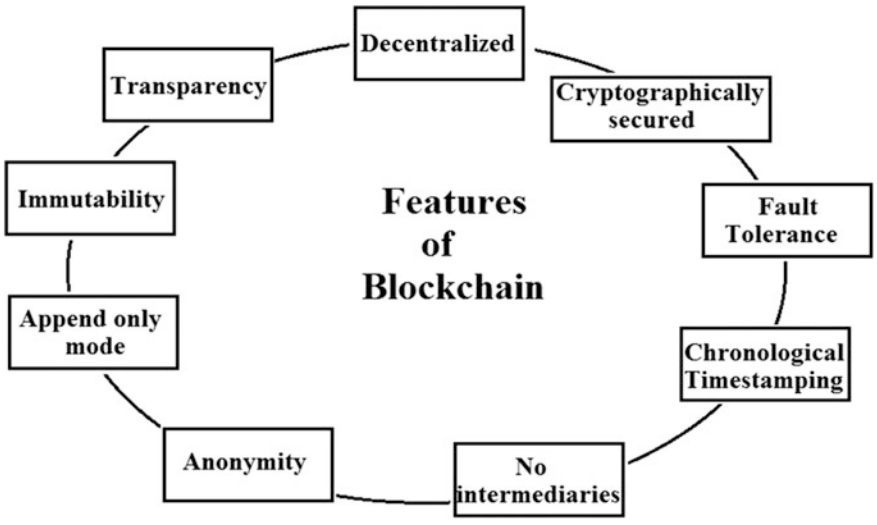


Fig. 24.4 Features of blockchain

- **Chronological time stamping**: The transactions in the blockchain network will have no significance [23] if not recorded with respect to time. Time stamping [25] refers to the time of occurrence of that particular event or transaction. The log of transactions is stored in reverse chronological order of their timestamp so as to order them with respect to time. The older block will have transaction which happened before the transactions in newer block.
- **Append only mode**: The network works by adding transactions to the ledger in a chronological order and doesn't allow editing any transaction back in time. This is called as the append only mode [33] of distributed ledger where the size of blockchain grows with time and no editing is allowed to anyone in the network.
- **Transparency**: In a blockchain network, anyone is allowed to join the network and mine blocks i.e. the transactions and the blockchain network are transparent [34] which can be accessed by anybody at any time.
- **No intermediaries**: For doing any transaction, two parties generally select a third party for the verification and validation of that transaction. E.g. Banks, Stamp papers etc. are third parties which confirm the validity of transactions. In blockchain, there is no dependency [25] on any third party or person as the blockchain network itself verifies the transactions.
- **Immutability**: As blockchain works in append only mode, the transactions cannot be edited or deleted at any point of time which makes it immutable. Once a transaction is stored in blockchain, it becomes permanent and hence immutable.
- **Fault Tolerance**: Blockchain has a decentralized ledger which is shared among all nodes of the network. So if few nodes go down or are not able to access network, blockchain will work normally as it has no dependency on anyone in the network. This makes the blockchain robust and fault tolerant.
- **Anonymity**: User identity is not revealed in blockchain network. Nodes are represented by their blockchain address which is the address generated using the cryptographic function and the public key of the node. This is done in order to keep the user anonymous to the network which ensures user's privacy.

24.1.2.2 Types of Blockchain

Blockchain can be categorized according to two categories: Mining rights and access rights.

Mining Rights: In blockchain, the transactions of the network are validated by peers. These validated transactions are mined/collected to make a block. In blockchain network, mining work may be open to all or done by few selected candidates. Table 24.4. shows the main difference between the two categories of blockchain according to mining rights.

Table 24.4 Permissioned versus permissionless

Permissioned versus permissionless	
Managed upkeep	Public ownership
Trusted	Trust-free
Private membership	Open &transparent
Faster	Slower
Settlement finality	Censorship resistant
Partially decentralized	Decentralized

- **Permissionless Blockchain**: Permissionless blockchain doesn't pose restriction on anyone to be the miner. Everyone in the network can choose the job of mining by paying mining fee and has fair chances to get the mining rewards if its mined block is added to the blockchain network. Permissionless blockchain are more popular with cryptocurrencies, on-chain assets and decentralized applications. E.g. Bitcoin [24], Ethereum [36], Litecoin [29], Holochain [37] etc.
- **Permissioned Blockchain**: Anyone in the permissioned blockchain network can't mine the block. Special permissions or elections are done for selecting the mining candidate. Various blockchain networks give fair chances to everyone in the network to mine the block. Some of the networks also use lottery system to select the miner for their network whereas the other blockchain network may designate a miner or miners to do the job. The number of miners is not fixed. There can be any number of miners in permissioned blockchain at any particular time. E.g. Ripple [9], HyperLedger Iroha [38], HyperLedger SawTooth [38], HyperLedger Burrow [38]. These blockchain are popular in businesses, industry level enterprises, supply chain management etc.

Access rights: Blockchain is a decentralized network of nodes/people. The access rights like joining the network, reading/writing/mining the blockchain are different for different types of blockchain as shown in Table 24.5. According to access rights we can divide blockchain in three categories:

- **Public**: Public blockchain network is the open network of nodes where anyone can join the network without any permission and can execute their transactions. User's identity is hidden by using cryptographic functions and can be used where there is no requirement of any third party. In this network, the consensus algorithms are long and may take more time create block than in private and federated blockchain networks. Transparency in terms of transactions is more than the other types of blockchain. Cryptocurrencies are designed using public blockchains. Dash [39], Bitcoin [24], Litecoin [29] are few of the public blockchain blockchains.
- **Private**: In private blockchain, only the authorized users are allowed to join the network for doing transactions. Private Blockchains are generally restricted to a particular organization with fast transaction approval time due to light consensus algorithms used. These types of blockchain are partially centralized as

Table 24.5 Public versus federated versus private blockchain

	Public	Federated	Private
Participants	Anonymous Could be malicious	Identified Trusted	Identified Trusted
Access rights	Anyone can read & execute the transactions	Permission to read/write is controlled by few predetermined nodes	Permission to read/write is controlled by single organization-owner of the blockchain
Architecture	Decentralized No centralized management	Partially centralized Multiple organizations – Hybrid between public & private	Partially centralized Single organization
Transaction approval time	Long time Approx. 10 min	Short time Less than a second	Short time Less than a second
Identity	Anonymous	Known identity	Known identity
Consensus mechanism	Time consuming algorithm Large energy consumption	Lighter & faster algorithm Less energy consumption	Lighter & faster algorithm Less energy consumption
USP	No middle MAM needed Secure & transparent	Low transaction cost Less data redundancy	Low transaction cost Less data redundancy
Examples	Bitcoin, Litecoin	R3, EWF	Bankchain, Monax

permissions are required to join in or leave the network. HyperLedger [25], Ripple [9] are private blockchain networks.

- **Federated**: These blockchains are similar to private blockchains as permissions are required to join in or leave the network and users are also known. These blockchains are restricted to few identified set of organizations. R3 [36] is one of the federated blockchain.

24.1.2.3 Working of Blockchain

Blockchain works in a decentralized fashion. Every node is to be updated about every transaction happening in the network. This requires a good consensus algorithm [24] to get the network on one copy of blockchain. The working of blockchain consists of following 4 steps:

Step 1: Initializing the transaction: If node A wants to transfer data/money to node B, it is called a transaction in blockchain. Node A initiates a transaction request in the network and it is then broadcasted to everyone else in the network.

Step 2: Validation of transaction: When the nodes in blockchain gets the transaction initiated request, the nodes signal whether it is a valid transaction or not by checking their copy of blockchain at sender's address which signifies the account details of the sender. This makes the blockchain transparent and at the same time anonymous as every node is represented by an address and no real identity is revealed.

Step 3: Creating a new block: If the nodes in blockchain signal a transaction as valid, the miner nodes add the transaction to the new block they are creating. Till now, the transaction is not added to the blockchain. Miner nodes use consensus protocol [24] defined by the blockchain environment to add the transaction to the block. Every blockchain environment uses a different consensus mechanism to create the block.

Step 4: Adding block to blockchain: There are various miner nodes creating block simultaneously. They solve a puzzle to find a unique number to be added to the block. From among the various blocks created, one block is chosen to be added to the blockchain depending on the consensus protocol used by the blockchain environment. The chosen block is broadcasted to the network so that every participating node appends it to their copy of blockchain and the whole network stays in consensus. Once the block is added to the blockchain, the transaction initiated by the sender A is complete. This waiting time from initiation of the transaction to completion of the transaction may vary in different blockchain networks. Generally the waiting time for public blockchain network is more than that of private or federated networks.

24.1.2.4 Applications of Blockchain

The concept of blockchain came into existence after the release of Bitcoin [24] which is a cryptocurrency. Various other cryptocurrencies like Ethereum [36], Litecoin [29], Ripple [9] came to market after Bitcoin. It then became popular for other financial applications like insurance [40], banks [40]. After financial applications, researchers found it useful for other applications like healthcare [41], supply chain management [8] etc. The introduction of programmable blockchain i.e. smart contracts [42] introduced blockchain to various other application areas like energy suppliers [43], entertainment [44] etc. Table 24.6. gives the wide range of applications in the field of blockchain.

Table 24.6 Applications of blockchain

Category	Applications
Cryptocurrency	• **Bitcoin** [24]: First cryptocurrency that introduced the concept of blockchain in 2008. Written as BTC •**Litecoin** [29]: Launched in 2011. Written as LTC •**Ethereum** [36]: Launched in 2015. Written as ETH •**Ripple** [9]: Launched in 2012. Written as XRP
Smart contracts	• **Ethereum** [36]: Smart Contract to build decentralized applications • **Eris** [64]: Platform to create smart contracts for applications • **Bit & Coin AG** [43]: Smart contracts for energy suppliers • **Block and chain game studios** [65]: Smart contract for gaming platform • **HyperLedger** [38]: Platform to create applications with smart contract • **Codius** [42]: Smart contract from the developers of Ripple [9] • **Slock it** [60]: Ethereum smart contracts to rent real world objects
Identity management	• **OneName** [9]: Platform for verifying digital identity. • **Estonia's e-residency** [66]: First blockchain platform to provide e-residency to anyone on the globe.
Financial services	• **ICICI bank** [40]: Using blockchain for paperless transaction within India and abroad • **Bajaj Finserv** [40]: Using blockchain for travel insurance and claim settlement • **HomeSend** [9]: Platform for doing cross border payments • **USC** [67]: Utility Settlement Coin, a blockchain project where 6 international banks joined for streamlining inter-bank settlements
Healthcare	• **Medrec** [41]: Blockchain based application for patients to keep their records safely • **MedicalChain** [68]: Platform for doctors and patients to share electronic records securely
Entertainment	• **KickCity** [69]: Platform for payment for event organizers • **Guts** [70]: Ticketing platform to remove frauds • **Spotify** [44]: Platform to safely connect license agreements and artists • **Matchpool** [71]: Platform for matchmaking for connecting members to their required community
Retail	• **Warranteer** [72]: Platform for product related info and also provide services in case of any malfunction • **Loyyal** [73]: Loyalty platform to provide incentives to customers
Supply chain management	• **Corda** [8]: Platform to connect supply chain to the ecosystem of suppliers and dealers • **IBM Blockchain** [74]: Platform to provide transparency among suppliers and dealers adding traceability at every aspect

24.2 Security Issues in IoT

We have discussed in detail the concepts of IoT and blockchain. IoT is connecting devices wirelessly to have M2M communications in order to ease or improve the life of human beings. Wireless data transfers are prone to vulnerabilities and attacks.

There is a long list of attacks that happened in past which proved a big disaster to the privacy of the organizations and people both. These attacks help us identify the security requirements of IoT applications and finally the solutions for the same.

24.2.1 Security Attacks on IoT Applications

IoT applications are being used from last so many years and have also witnessed a huge increase in the number of applications in every arena of the society. Majority of the applications are for personal purposes as wireless connectivity lack data privacy and integrity. Few of the cyber-attacks that caused havoc are listed as follows:

- **Sinkhole attack**: Sinkhole attack [45] happens at network layer of IoT platform where an intruder attacks one or more insider node to transmit fake routing update so that all the data of the network gets diverted to the comprised node in the network. This will reduce the traffic flow of the network and fool the senders that their sent packet of data has been received by the receiver. This lets the intruder get all the data from the comprised node whereas the receiver didn't get their intended packet of data. Sinkhole is an active attack which may lead to other attacks like DOS attack, selective forwarding attack etc.
- **DOS attack**: In denial-of-Service attack [46], the attacker floods the network with useless messages to create data traffic in order to exhaust the devices/ resources of the IoT network. This attack can also cause the network to shut down by making all the devices completely unavailable. DoS attack can happen at network or application layer in the network. This attack is more dangerous at application layer as it affects the defense mechanism of the network which makes the sensitive information to be stolen easily.
- **Wormhole attack**: In warmhole attack [47], the attackers try to find a strategic place in the network such that they have the shortest route within the nodes. When the attackers publicize their location in the network, the routing table includes the attacker for message passing. The attackers keep listening to the network and record it. The attacker then creates a direct link between each other and forms a tunnel between them to transfer traffic. This causes routing failure and disrupt the topology of the network.
- **Sybil attack**: Sybil attack [48] also happens at network layer of the architecture. In this attack, attacker manipulates few nodes of the network and may create multiple fake copies of the nodes as well. In this way whole of the IoT network is compromised and false information is spread which will increase the traffic and hamper the privacy of the network. False reports will also be generated because of the wrong information sent by the false nodes.
- **Selective Forwarding attack**: The attacker in this form of attack [49] may capture few nodes of the network and restricts their packets to be transmitted which results in packet loss and no organization of packets can be made. So the

network has incomplete information which sometimes is more dangerous to no information. The extreme format of selective forwarding attack is black-hole attack where the attacker restricts all the packets of few nodes for transmission which results in huge data loss and almost communication being done.

- **Hello Flood Attack**: In this attack [50], the attacker uses a high-powered transmitter to send HELLO messages to the nodes in IoT network. The attacker may be sending messages from a far place but seems to be a neighbor to the nodes of network due to the use of high-powered transmitter. The attacker sends messages to all the nodes of network to broadcast false routing information. It may send messages to set a malicious node as parent node. This leads in data loss, high network traffic and false routes.

24.2.2 Security Requirements of IoT

As already discussed, IoT network lacks security features in one or the other way which makes the devices of the network prone to security vulnerabilities. To prevent IoT network from failures, run smoothly and share data safely, certain mechanisms and parameters are required in terms of security and privacy of data. Following are some of the security requirements of IoT applications which need to be met after considering the cyber-attacks already happened:

- **Authentication and authorization**: In an IoT network, only authorized people should be allowed to access the content. For this authorization mechanisms [51] are required to make the communication safe and secure. Unauthorized attacks [52] in IoT mainly arise due to spoofing, authentication breach or lack of proper mechanism for authentication. In this case the intruder may hamper the whole IoT network by stealing sensitive data, flood the network with useless messages or stop message transmission. Authorization mechanisms must be designed to make sure that only the authorized person is given the access to data.
- **No single point of failure**: For data transmission and other services, IoT devices rely on cloud infrastructure which is prone to failure. If the network is down, delay in services is very normal. It may also result in failure of services. The increasing number of IoT devices may also lead to low speed of data transfer. For a fault tolerant IoT network, tamper proof mechanism [53] need to be designed for data transfer.
- **Data confidentiality/Security**: The data in a particular IoT network travels multiple hops to reach the destined device which makes it vulnerable to theft via compromising nodes (if any) in the network. There may be a case that before reaching the destination node, the data is manipulated by the neighboring nodes. This may create a big trouble as proper functioning of IoT network depends on correct data shared between the nodes of network. For this an encryption mechanisms [10] need to be added so as to maintain the confidentiality of the data being shared among devices.

- **Trusted data origin**: In an IoT application, it is sometimes difficult to identify the origin of data. There may also be chances of data manipulation by the neighboring nodes or the compromising nodes [54] which may lead to wrong information being sent to the destined node. This can be resolved by adding the identity of the sender with the message or data being transferred.
- **No third party/Trustless environment**: The data is stored in a centralized environment which acts as a third party. The third party [51] may share the data with anyone else or may manipulate it which leads to security breach. This can be handled using a decentralized distributed environment for keeping multiple copies of the data within the network so that no data is lost or manipulated.
- **Energy efficiency**: The devices in IoT network are generally low battery and low storage devices. If there is attack in the network, it consumes high power because of the flooding of messages in the network which exhausts [53] the IoT resources/devices. For proper working of the IoT network, mechanisms need to be designed to identify such flooded message or attacks in the network.
- **Device Security**: For M2M communication, there needs have a mechanism for device authentication as attacker uses their devices to collect or forge data. As devices themselves cannot check the authenticity of the neighboring devices, some protocol need to be designed for registration of devices in the IoT network before staring any communication with that device.
- **Access Control**: In the IoT network, the data transferred is shared to all the nodes of network. Protocols can be designed to restrict the sharing of data to peers. This will also help in restricting data to unauthorized access in the network.

24.3 Blockchain and Its Impact on IoT

Academicians and industrialists are looking into the features of blockchain to find solution for the security issues of IoT. Following are some of the features of blockchain that are useful for IoT:

- **Address Space**: Blockchain uses a 160 bit/20 bytes address space [54] to provide addresses to the nodes in the network. 20 bytes can generate addresses for 1.46×10^{48} nodes. This means 1.46×10^{48} devices can be given addresses uniquely without the need of reallocating the same address to the devices. This eliminates the centralized authority of IoT i.e. Internet Assigned Numbers Authority (IANA) which provides addresses to the devices. Moreover IANA uses IPv4 or IPv6 addresses which is a 64 or 128 bits addresses, so blockchain will have 4.3 billion more addresses than IPv6. This makes IoT more scalable.
- **Data Authentication**: Blockchain uses cryptographic algorithms to ensure the integrity and authenticity of the transactions happening in the network. For IoT applications, blockchain can be used to prevent the network from any unauthorized access [55] or attack as transactions can be tracked and monitored.

- **Secure Communication**: Various protocols are used for data transmission in IoT as discussed in 1.1.3 but most of them are not secure communication protocols. These protocols need to be clubbed with security protocols like Transport Layer Security (TLS) for secure communication. If IoT transmission are recorded/done via blockchain, there will be no need of any other protocols as blockchain ensures the security and immutability of data.
- **Anonymity**: As already discussed that blockchain provides unique addresses called as Global Unique Identifier (GUID) to all the nodes in the network and this encrypted address is used to identify nodes/devices in the network. This maintains the privacy of nodes in the network. To add further, smart contracts also allow various people to have ownership of a devices distinguished by time or date and the owner at particular time will have complete access to the device during its ownership.
- **Tracking Changed Ownership of Devices**: IoT devices during its lifetime may have different owners, supplier or consumers. This is associated with the identity of that particular device. There are chances that a particular device is being used by different people at different time. In an IoT network, devices form a relationship with humans and services being provided. If the device changes ownership, there need to be a tracking system [56] for the same. TrustChain [57] provides a trusted environment using blockchain to maintain the integrity of transactions in the distributed environment.
- **Trustless Environment**: IoT uses cloud infrastructure to store, process or retrieve data. If IoT works in blockchain environment, there will be no third party dependency as shown in Fig. 24.5. Also with blockchain, there is no single [58] point of failure as it happens in cloud environment.

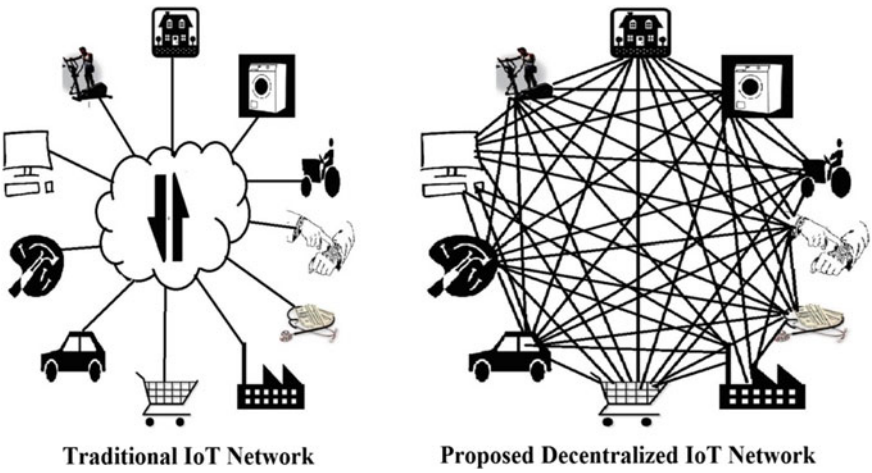


Fig. 24.5 Traditional IoT network versus decentralized IoT network

24.3.1 Proposed Framework for Blockchain Based IoT Network

The concepts and mechanisms associated with blockchain can resolve many of the security issues associated with tradition IoT network. The different architectures proposed by various researchers have already been discussed in Sect. 1.1.2. To combat the challenges of IoT network, an IoT architecture based on blockchain can be used. A framework for Blockchain-IoT (BIoT) architecture has been proposed in Fig. 24.6 in which a blockchain layer has been added to maintain a distributed ledger for all the communication being done within the network. The proposed framework consists of following 4 layers:

- **Sensor layer**: It is the physical layer that collects data from devices embedded with various sensors in IoT network. It includes all the devices from different manufacturers to communicate at the same platform. Blockchain can help with the registration of all the devices, provide an address to the devices, encrypt every message coming from devices with its blockchain address and thereby providing anonymity and security to the IoT network.
- **Network layer**: At this layer, the devices connect to internet and transfer messages to each other. In the BIoT architecture, the messages are encrypted, written on blockchain and are destined to particular devices. All these communications are done at the network layer in an encrypted format which maintains the security of the network.
- **Blockchain layer**: This is a database type of layer which acts as a storage of all the encrypted messages with time stamping in the reverse chronological order. The IoT network can use any type of blockchain: public, private, federated, permissioned, and permissionless depending on its requirement. This blockchain layer will add verification and validation of the transactions. It will also control the access rights and manage device security in the network.

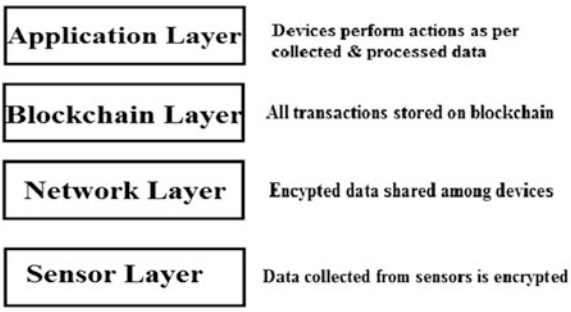


Fig. 24.6 Proposed architecture of Blockchain-IoT (BIoT)

- **Application layer**: The data collected at the sensor layer, processed and communicated at the network layer is stored in the blockchain layer. At application layer, the devices communicate and perform the activity associated with the processed data E.g. In a smart home, when the door opens, the sensors of the door communicate the opening of doors to the coffee maker, room temperature controller etc. These devices then perform the actions associated with the door sensors.

24.3.2 Blockchain Based IoT Solutions

Blockchain seems to be a promising technology for resolving security issues of IoT. The number of applications or platforms of blockchain technology are constantly growing. Table 24.7 provides the insights of few blockchain based platforms which are meant to create IoT applications. These platforms automatically provide the features of blockchain to IoT application for enabling security and privacy. Most of the platforms are still under testing phase. Few platforms like Litecoin [29], Ethereum [36] etc. also have their cryptocurrencies which are used while making any payments in the transactions on IoT network.

Apart from these platforms, there are many applications which use these platforms to build IoT network. Few of them are listed in Table 24.8. It contains applications which choses blockchain or its properties for securing IoT network. E.g. IOTA [59] is not a blockchain application, it uses decentralized ledger for securing its transactions.

Table 24.7 Blockchain platform for IoT applications

Platform	Description
Multichain [75]	Platform for creation of private blockchain for IoT applications to manages devices, transactions and other permissions
Ethereum [36]	Platform for developing IoT application by defining smart contract. It is the most compatible platform for IoT applications
HyperLedger fabric [38]	An open source platform which uses IBM Watson's IoT platform to manage devices and perform data analysis
Litecoin [29]	Platform for IoT applications with fast transaction confirmation time, low computation requirement and efficient storage
HDAC [65]	Smart contract platform for IoT applications for permission based blockchain that uses quantum random numbers as cryptographic algorithm
Quorum [76]	Permission based blockchain platform to provide data privacy by using cryptography and segmentation

Table 24.8 Blockchain IoT (BIoT) applications

Application	Description
IOTA [59]	A distributed ledger for micro payments in IoT. Uses Direct Acyclic Graph for storing transactions providing security and authentication in data sharing among nodes
LO3 Energy [77]	Blockchain based application for smart grid that allows secure transactions for energy sales within the micro grid nodes
Chain of things [59]	A research lab to solve the problem of privacy and security of IoT application by using blockchain solutions
Modum [78]	Application to record environment conditions using sensors. It uses Ethereum for data integrity in supply chain management
Riddle and code [79]	Blockchain based application to secure ownership of digital devices in IoT network. Attaches a chip to the devices to track them
Chronicled [80]	Uses multiple blockchain system to create trusted IoT-supply chain system. Also uses smart contracts for device registration and verification.
MyBit [81]	Uses Ethereum smart contracts to provide services to device owners who can share their devices in the IoT network and get revenues from them

24.4 Conclusion

IoT is an emerging field of technology with its applications widespread in day to day activities. In past few years the technology has done great advancements with new faster protocols being developed to finding new areas of usage. Looking at the trend of increasing number of connected devices, it seems Gartner's prediction [1] of 25 billion connected devices in 2020 will come true soon. This high number of connected devices poses new privacy and security threats to the devices and network. Also the number and intensity of attacks happened in past demands the design of protocols and mechanisms for providing a secure and confidential connectivity within devices.

Blockchain technology seems to be a solution for these privacy and security issues of IoT. It can be used to register the devices of the IoT network which will solve the problem of any intruder getting inside the network. Majority of security attacks as discussed in chapter occur when intruder gets access to the network of IoT devices and steal information. In the BIoT scenario, no unauthorized access is possible which makes it immune to attackers and hence security attacks.

Also if all the data communication is done via blockchain protocols, data will be transmitted after encrypting the message. This provides security and privacy to the devices within network as encryption prevents any information leakage or alteration. Blockchain provides a trustless environment for secure and transparent communication. Our work details both the emerging technologies: IoT and Blockchain with their real world applications. IoT's security issues and attacks have also been discussed. In last, architecture for IoT—Blockchain (BIoT) integration

has been proposed. BIoT integration will definitely be the future of IoT applications especially in cases of data critical applications.

References

1. Farooq, M.U., Waseem, M., Khairi, A. et al.: A critical analysis on the security concerns of Internet of Things (IoT). Int. J. Comput. Appl. **111**(7) (2015) (New York)
2. Sandeep, C.H.: Security challenges and issues of the IoT system. Ind. J. Pub. Health Res. Dev. **9**(11), 748–753 (2018). (India)
3. Pancaroglu, D., Sen, S.: An analysis of the current state of security in the Internet of Things. In: International Conference on Cyber Security and Computer Science (ICONCS'18), Turkey (2018)
4. Brody, P., Pureswaran, V.: Device democracy: saving the future of the Internet of Things. In: IBM Executive Report (2014)
5. Dhaliwal, P., Bhatia, M.P.S., Bansal, P.: A cluster-based approach for outlier detection in dynamic data streams (KORM: k-median outlier miner). J. Comput. **2**(2) (2010)
6. Vo HT, Mehedy L, Mohania M, et al. (2017) Blockchain-based data management and analytics for micro-insurance applications. In: Proceedings of the 2017 ACM on Conference on Information and Knowledge Management, pp. 2539–2542 (Singapore)
7. Kim, H.W., Jeong, Y.S.: Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain. Hum. Cent. Comput. Inform. Sci. **8**(1), 11 (2018)
8. Brown, R.G., Carlyle, J., Grigg, I., et al.: Corda: An Introduction. R3 CEV, p. 15 (2016)
9. Olleros, F.X., Zhegu, M., (eds.).: Research Handbook on Digital Transformations. Edward Elgar Publishing, USA (2016)
10. Ahanger, T.A., Aljumah, A.: Internet of Things: a comprehensive study of security issues and defense mechanisms. IEEE Access **7**, 11020–11028 (2019)
11. Salvador, J.C., Uceda, J.M.R., Muiños, V.C., Lopez, J.R., et al.: Ubiquitous computing and its applications in the disease management in a ubiquitous city. J. Comput. Commun. **6**(03), 19 (2018)
12. Buyya, R., Srirama, S.N. (eds.) Fog and Edge Computing: Principles and Paradigms. Wiley (2019)
13. Tiwari, U.K., Matta, P.: Efficient smart-home architecture: an application of Internet of Things. In: Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE) 2019, India. Available at SSRN 3350330 (2019)
14. Misri, S., Navghare, S., Sawant, S., et al.: IoT enabled prepaid electricity meter. In: 2nd International Conference on Advances in Science & Technology (ICAST) 2019, India. Available at SSRN 3368204 (2019)
15. Singh, T.A., Chandra, J.: IOT based green house monitoring system. JCS **14**(5), 639–644 (2018). (Dubai)
16. Kumar, N.S., Nirmalkumar, P.: An intelligent decision-support system for telemedicine. Appl. Math. **12**(5), 983–993 (2018). (New York)
17. Xu, J., Chen, G., Xie, M.: Vision-guided automatic parking for smart car. In: Proceedings of the IEEE Intelligent Vehicles Symposium 2000, pp. 725–730, USA (2000)
18. Khari, M., Kumar, M., Vij, S., Pandey, P.: Internet of Things: proposed security aspects for digitizing the world. In: 3rd International IEEE Conference on Computing for Sustainable Global Development (INDIACom), pp. 2165–2170. India (2016)
19. Al-Fuqaha, A., Guizani, M., Mohammadi, M., et al.: Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tut. **17**(4), 2347–2376 (2015)

20. Kumar, S.A, Vealey, T., Srivastava, H.: Security in Internet of Things: challenges, solutions and future directions. In: 49th Hawaii International IEEE Conference on System Sciences (HICSS), pp. 5772–5781. Hawaii (2016)
21. Qiu, T., Chen, N., Li, K., et al.: How can heterogeneous Internet of Things build our future: a survey. IEEE Commun. Surv. Tut. **20**(3), 2011–2027 (2018)
22. Kasturi, K., Reddy, P.V., Rao, N.A., Vinod, S.: A review of architecture and applications for Internet of Things. Adv. Nat. Appl. Sci. **10**(9 SE), 261–267 (2016). (Jordan)
23. Sapra, R., Dhaliwal, P.: Blockchain: the new era of technology. In: 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 495–499 (2018) (India)
24. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
25. Niranjanamurthy, M., Nithya, B.N., Jagannatha, S.: Analysis of blockchain technology: pros, cons and SWOT. Cluster Comput., 1–15 (2018)
26. Rouhani, S., Butterworth, L., Simmons, A.D., et al.: MediChainTM: a secure decentralized medical data asset management system. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Canada (2019)
27. Buterin, V.: A next-generation smart contract and decentralized application platform. White Paper **3**, 37 (2014)
28. King, S., Nadal, S.: Ppcoin: peer-to-peer crypto-currency with proof-of-stake. Self-published Paper (2012)
29. Nguyen, G.T., Kim, K.: A survey about consensus algorithms used in blockchain. J. Inform. Process. Syst. **14**(1), 101–128 (2018). Korea
30. Castro, M., Liskov, B.: Practical byzantine fault tolerance. OSDI **99**, 173–186 (1999)
31. Lerner, S.D.: Rootstock: Bitcoin powered smart contracts. White Paper (2015)
32. Buterin, V.: A next-generation smart contract and decentralized application platform. White Paper (2014)
33. Kosba, A., Miller, A., Shi, E., et al.: Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE Symposium on Security and Privacy (SP), pp. 839–858, San Francisco (2016)
34. Gatteschi, V., Lamberti, F., Demartini, C., et al.: Blockchain and smart contracts for insurance: is the technology mature enough? Future Int. **10**(2), 20 (2018)
35. https://www.blockandchain.games/
36. Antonopoulos, A.M.: Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, Inc., CA (2014)
37. Katuwal, G.J., Pandey, S., Hennessey, M., et al.: Applications of blockchain in healthcare: current landscape & challenges. In: arXiv preprint. arXiv:1812.02776
38. Hyperledger ARCHITECTURE. Volume II. Available at, https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf
39. Duffield, E., Diaz, D.: Dash: a privacy centric crypto currency. White Paper (2018)
40. Sheetal, M., Venkatesh, K.A.: Necessary requirements for blockchain technology and its applications. Int. J. Comput. Sci. Inf. Technol. (2018)
41. Azaria, A., Ekblaw, A., Vieira, T., et al.: Medrec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30 (2016)
42. Eze, P., Eziokwu, T., Okpara, C.: A triplicate smart contract model using blockchain technology. In: Circulation in Computer Science, Special Issue on Disruptive Computing, Cyber-Physical Systems (CPS), and Internet of Everything (IoE), pp. 1–10 (2017)
43. http://www.bit-coin.ag/
44. https://www.spotify.com/
45. Baskar, R., Raja, P.K., Joseph, C., et al.: Sinkhole attack in wireless sensor networks performance analysis and detection methods. Ind. J. Sci. Technol. **10**(12) (2017) (India)
46. Shruthi, C., Asha, M.: Dos attack and suspicious activity detection for a book application. Int. J. Sci. Res. Comput. Sci. Eng. Inform. Technol. **3**(6), 175–180 (2018)

47. Palacharla, S., Chandan, M., GnanaSuryaTeja, K., et al.: Wormhole attack: a major security concern in Internet of Things (IoT). Int. J. Eng. Technol. **7**(3.27), 147–150 (2018)
48. Pawar, S., Vanwari, P.: Sybil attack in Internet of Things. Int. J. Eng. Innov. Technol. (IJESIT) **5**(4), 96–105 (2016)
49. Mehetre, D.C., Roslin, S.E., Wagh, S.J.: Detection and prevention of black hole and selective forwarding attack in clustered WSN with active trust. Cluster Comput., 1–16 (2018)
50. Adat, V., Gupta, B.B.: Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommun. Syst. **67**(3), 423–441 (2018)
51. Makhdoom, I., Abolhasan, M., Abbas, H., et al.: Blockchain's adoption in IoT: the challenges, and a way forward. J. Netw. Comput. Appl. (2018)
52. Yu, Y., Li, Y., Tian, J., et al.: Blockchain-based solutions to security and privacy issues in the Internet of Things. IEEE Wirel. Commun. **25**(6), 12–18 (2018)
53. Fernández-Caramés, T.M., Fraga-Lamas, P.: A review on the use of blockchain for the Internet of Things. IEEE Access **6**, 32979–33001 (2018)
54. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. **82**, 395–411 (2018)
55. Dhaliwal, P., Bhatia, M.P.S.: Effective handling of recurring concept drifts in data streams. Indian J. Sci. Technol. **10**(30), 1–6 (2017). (India)
56. Friese, I., Heuer, J., Kong, N.: Challenges from the Identities of Things: introduction of the Identities of Things discussion group within Kantara initiative. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 1–4 (2014)
57. Otte, P., De Vos, M., Pouwelse, J.: TrustChain: a sybil-resistant scalable blockchain. Future Gener. Comput. Syst. (2017)
58. Dhaliwal, P.: An ensemble approach for handling the novel instances in dynamic data. In 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 19–23. India (2018)
59. Pustišek, M., Kos, A.: Approaches to front-end IoT application development for the Ethereum blockchain. Proc. Comput. Sci. **129**, 410–419 (2018)
60. Bahga, A., Madisetti, V.K.: Blockchain platform for industrial Internet of Things. J. Softw. Eng. Appl. **9**(10), 533 (2016)
61. Suma, N., Samson, S.R., Saranya, S., et al.: IOT based smart agriculture monitoring system. Int. J. Recent Innov. Trends comput. Commun. **5**(2), 177–181 (2017)
62. Porkodi, R., Bhuvaneswari, V.: The Internet of Things (IOT) applications and communication enabling technology standards: an overview. In: 2014 International Conference on Intelligent Computing Applications, pp. 324–329 (2014)
63. Smith, D., Lyle, S., Berry, A. et al.: Internet of Animal Health Things (IoAHT) Opportunities and Challenges. University of Cambridge, England (2015)
64. Mattila, J.: The blockchain phenomenon. In: Berkeley Roundtable on the International Economy (BRIE), pp. 2016–1 (2016)
65. Reyna, A., Martín, C., Chen, J., et al.: On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. **88**, 173–190 (2018)
66. Sullivan, C., Burger, E.: E-residency and blockchain. Comput. Law Secur. Rev. **33**(4), 470–481 (2017)
67. http://fortune.com/2017/08/31/banks-ubs-blockchain-settlements/
68. https://medicalchain.com/en/
69. https://kickcity.io/
70. https://guts.tickets/
71. https://www.matchpool.com/
72. http://www.warranteer.com/
73. https://loyyal.com/
74. https://www.ibm.com/blockchain/industries/supply-chain
75. Samaniego, M., Deters, R.: Internet of Smart Things-IoST: using blockchain and clips to make things autonomous. In: 2017 IEEE International Conference on Cognitive Computing (ICCC), pp. 9–16 (2017)

76. Morgan, J.P.: Quorum Whitepaper. JP Morgan Chase, New York (2016)
77. Mengelkamp, E., Gärttner, J., Rock, K.: Designing microgrid energy markets: a case study: the Brooklyn microgrid. Appl. Energy **210**, 870–880 (2018)
78. https://www.chainofthings.com/
79. Modum Whitepaper. Available at https://assets.modum.io/wp-content/uploads/2017/08/modum-whitepaper-v.-1.0.pdf
80. https://www.chronicled.com
81. https://mybit.io/