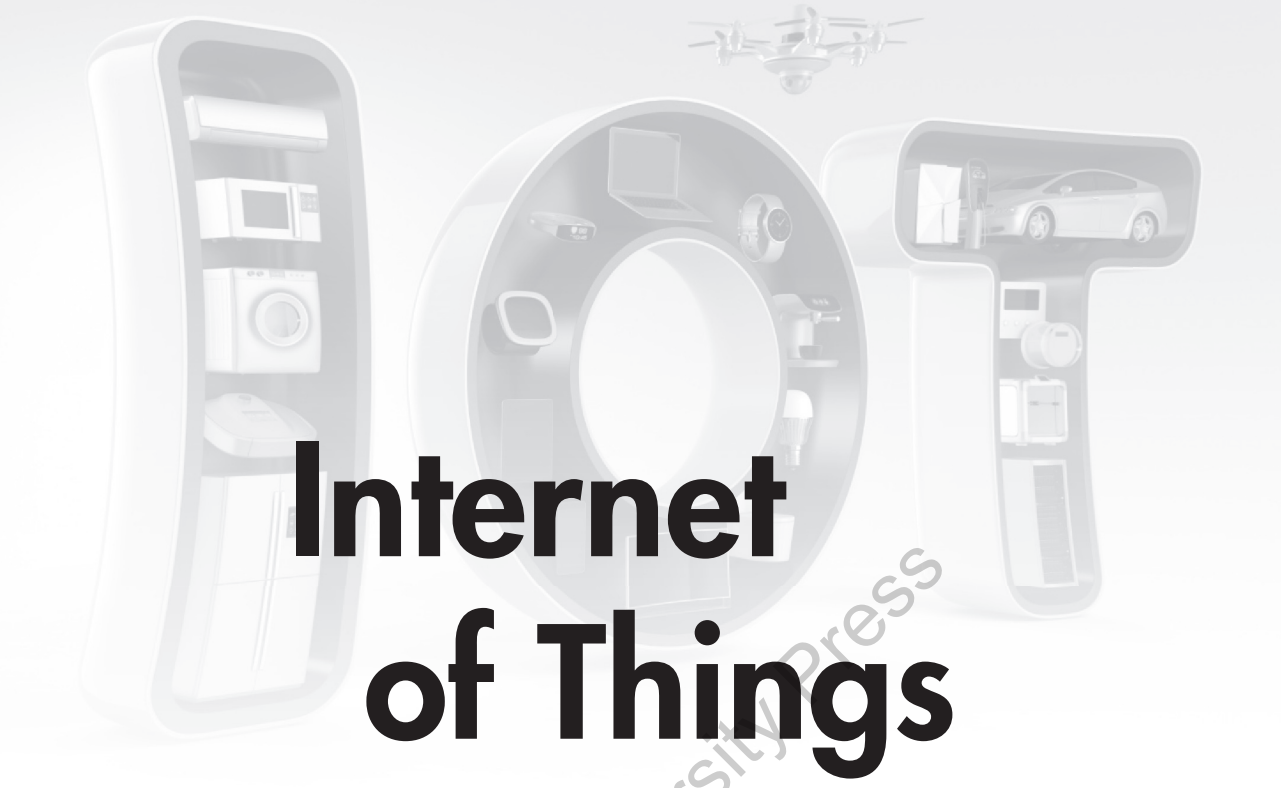


Internet of Things

Surya S. Durbha
Professor,
CSRE, Indian Institute of Technology Bombay (IITB)

Jyoti Joglekar
Professor,
Department of Computer Engineering
K. J. Somaiya College of Engineering (KJSCE)
Somaiya Vidyavihar University (SVU)
Mumbai

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide. Oxford is a registered trade mark of
Oxford University Press in the UK and in certain other countries.

Published in India by
Oxford University Press
22 Workspace, 2nd Floor, 1/22 Asaf Ali Road, New Delhi 110002

First published in 2021

ISBN-13: 978-0-19-012109-9
ISBN-10: 0-19-012109-2
eISBN-13: 978-0-19-099222-4

Typeset in Adobe Garamond Pro and Myriad Pro
by Cameo Corporate Services Limited, Chennai
Printed in India by

Cover image: © Chesky

Cover illustration: by Manoj Kumar

For product information and current price, please visit www.india.oup.com

Preface

The Internet of Things (IoT) is creating unprecedented new business and scientific opportunities that are envisaged to make giant leaps in the way humans interact with Things that were earlier mostly static in nature. The IoT technology is demonstrating the ease of making interaction with our environment more dynamically by embedding devices that host a variety of sensors and actuators capable of providing real-time actionable information.

The interdisciplinary nature of IoT is enabling many cross-domain applications providing a host of services in many areas such as smart cities, healthcare, retail, agriculture, industrial automation, etc. However, with it also comes many interoperability challenges to overcome so that the devices and applications can work without being constrained by the underlying representations and protocols. Towards this, huge efforts are underway by several organizations to develop reference models and standards at every level of the IoT stack. These standards are now gradually making their way into various IoT system implementations.

Another major reason for the widespread interest and efforts for adoption of IoT technologies is the availability of a variety of sensors that are capable of sensing a wide range of variables related to the physical environment, equipment, infrastructures, etc.

The current technologies for integration of IoT with cloud is facilitating the development of highly scalable IoT systems. Several IoT cloud solutions are also providing functionality to perform big data analytics using various approaches such as AI, machine learning, and deep learning, running on high-performance computing (HPC) systems.

Another emerging area is real-time IoT data analysis called edge analytics, which is performed at the edge of the IoT devices to provide situational awareness. This is usually integrated with IoT gateways.

Rapidly evolving electronic device technology such as microcontroller chips, nuclear batteries with large life time, etc. will open new avenues for deploying IoT solutions in inaccessible terrains in the near future. Various business models are emerging on monetization of the IoT systems and holds great promise for high return on investment.

About this Book

Internet of Things (IoT) covers a wide range of topics providing both introductory aspects of IoT as well as recent advances in IoT. A lucid treatment of the subject matter is adopted to enable the reader to easily grasp the concepts and techniques. This book strives to strike a balance between the theoretical content and hands-on material.

The IoT domain contains aspects that are related to both hardware and software, hence, there is a need to provide equal treatment on both those aspects. Various well-known hardware (sensors/actuators, microcontrollers, etc.) are described and how to use them to develop IoT-based systems is also explained. The book discusses the most relevant hardware that is available in the market for

readers to purchase it and begin experimentation. It covers several examples with various hardware. The theoretical material related to the software aspects of IoT is also complemented by focused examples using well-known programming languages such as Java and Python.

The target readers of this book are undergraduate and post-graduate engineering and science students (BE/B.Tech/M.Tech/BSc/MSc), and computer applications' students (BCA/MCA). It can be adopted as a text book for the IoT courses in these degree programs. Further, software engineers, web developers, IoT product designers, educators, and beginners in IoT will find this book useful. We also recommend this book for managerial personnel who are managing IoT systems.

Features of the Book

- Approaches IoT in an application-oriented manner, connecting the foundational aspects of the subject with its relevance in real-life applications and spread with easily understandable examples throughout the book.
- Each chapter begins with a bulleted list under the heading "Chapter Objectives", listing the knowledge the readers would gain after reading it.
- This is followed by a "Recap" box that consists of a bulleted list of key concepts and the relevant sections in the book that the reader needs to be familiar with before embarking on the current chapter.
- Boxed items provided in each chapter describe a particular concept/technology/application in more detail.
- Hands-on programming exercises in Python, Java, Arduino are provided with step-by-step instructions in relevant chapters.
- Discusses use cases with fully working code in an exclusive chapter.
- A section on "Best Practices" is provided for relevant chapters at the end of each chapter, followed by the sections "Further Reading", "Exercises" and "Key References".

Organisation of the Book

The book is divided into five parts and 18 chapters, listed below:

Part I: Foundational Aspects

Chapter 1: Emergence of IoT

This chapter begins with the vision and explanation of various definitions of the IoT from different perspectives and settles on one working definition forming the basis on which the rest of the concepts are explained in this book. The interdisciplinary nature of IoT, the challenges involved in its further evolution and standardization, and contribution factors across various disciplines to the widespread diffusion of IoT are also explained.

Chapter 2: Concept of Smart Things/Objects

This chapter discusses how Things are made smart through sensors, actuators, communication over network interfaces, and connection to the Internet with some motivating examples. The Machine-to-Machine (M2M) concepts are described and the key differences between IoT and M2M are explained.

Chapter 3: Wireless Sensor Networks in IoT
This chapter introduces wireless sensor networks (WSNs) and describes its basic attributes. Further, different network topologies in WSN are presented. The WSN communication patterns such as broadcast, multicast, flooding, gossiping, and other related protocols are discussed. Data aggregation approaches and various routing techniques in WSNs are described. Several real-world applications of WSNs are discussed. Finally, the evolution of wireless sensor networks towards IoT is presented.

Chapter 4: IoT Standards and Protocols
This chapter describes various wired and wireless technologies available. Various layers, protocols, packets, and services are explained. Role of IPV6 in IoT is elucidated. In addition, various low-power wide-area network (LPWAN) technologies specifically designed for low baud rate and long-range communications such as NB-IoT and LoRaWAN are discussed. Several data link layer communication protocols such as WirelessHART, Z-Wave, Bluetooth and ZigBee, DASH7 and LTE-A are introduced.

Part II: Understanding the Nuts and Bolts of IoT Hardware, Software, and Middleware

Chapter 5: Sensors and Actuators in IoT
This chapter describes the perception layer of the IoT. It covers a comprehensive description of various sensors such as those available on a mobile phone like light sensors, environment measuring sensors such as temperature and pressure, medical sensors such as heart and pulse rate sensors, flow and fluid measuring sensors, range and motion capture sensors, and touch sensors. A description is provided for different types of actuators such as servo motor, stepper motor, DC/AC motor, linear actuators such as solenoid and relay. Several application areas corresponding to the sensors and actuators are presented. The subsequent chapters provide a hands-on approach for integration of these sensors with various prototyping kits such as Arduino, Raspberry pi, pcDuino, and Beaglebone.

Chapter 6: Open Hardware in IoT
This chapter explains open hardware technologies available for making IoT applications such as Arduino, Raspberry pi, Beaglebone, pcDuino, and CubieBoardto design a customised board suitable for a specific application. Comparison of different existing open hardware platforms is provided. It discusses how to choose the right platform for a specific application based on the limitations and capabilities of the hardware and complexity of the problem. Further, cellular IoT devices discussed are Adafruit Feather 32u4 Fona, GOBLIN 2, LinkItONE, Hologram Dash, and Arduino GPRS Shield. In addition, a description of industrial microcontrollers such as PLC and RTU is given. A comparison of various hardware platforms based on several attributes such as Size, Weight, CPU, Memory, and Power, as well as Expansion Connectors, Operating System, and Programming Languages is presented.

Chapter 7: IoT Middleware
This chapter begins with the description of the function and high-level description of a middleware followed by an explanation about the fundamental features of a middleware. The need for an IoT middleware is clearly brought out and the functional and non-functional requirements are presented. Various architectures of the IoT middleware are explained with a comparison. The development of IOT services is described based on Services Oriented Architecture (SOA), and various flavours of SOA such as HTTP/REST, HTTP/SOAP, WS-I, and JMS are explained. State-of-the-art IoT Middleware

(OpenIoT, KaaIoT, Node-RED, CHOReOS, LinkSmart, CarrIoT, Oracle Fusion and Google Cloud IoT) both Commercial off the Shelf (COTS) and open source are reviewed along with the main application domains for which they were developed.

Chapter 8: IoT Software Platforms

This chapter introduces the need for developing IoT platforms, and explains the fundamental characteristics of an IoT Platform, and its benefits. A general framework for IoT platforms is presented and each component of that framework is described. Further, the IoT software platforms landscape is described in terms of Commercial IoT platforms (Amazon Web Service (AWS) IoT Platform, Bosch IoT Suite, EVRYTHNG, IBM Watson IoT Platform, Cisco Kinetic IoT, Google IoT Cloud, and Microsoft Azure IoT Suite) and open source IoT platforms (ThingsBoard, OGC SensorThings, Thinger.io, SiteWhere, and ThingSpeak). Some guidelines for choosing an IoT platform are presented. A step-by-step, hands-on exercise using an IoT platform (ThingsBoard) is given towards the end of the chapter.

Chapter 9: Prototyping IoT Applications

This chapter explains the importance of prototyping and its benefits while developing IoT projects with physical objects, software and hardware controllers, sensors, actuators, and Internet. It explains various steps of prototyping with examples in several application domains. The various stages involved in prototyping are explored such as refining IoT product idea, physical and logical design considerations, choosing a specific microcontroller, design of housing for the physical object and moving parts, and developing and enabling web services through which the IoT device shares the information or acts as a smart thing. Various online prototyping tools, APIs for real-time IoT applications, packages for IoT in Python are reviewed. The embedded code writing section explains the use of IDEs, various IoT related programming languages and efficient code writing. A real world prototype example (hands-on exercise) related to smart home is described towards the end of the chapter

Part III: IoT Big Data Science and Analytics

Chapter 10: Big IoT Data Science

This chapter introduces the foundations and principles of big data science from an IoT perspective. The steps involved in the data science process are described with examples written in Python. The concepts of artificial Intelligence (AI) and machine learning including the recently emerging Deep learning approaches are described from an IoT analytics point of view. Concepts of Data lake/Swamp are discussed and the chapter introduces the concept of Edge analytics (chapter 12 is entirely dedicated to edge analytics). Machine learning tools are explained with IoT use cases. The various forms of big IoT data analytics such as descriptive, diagnostic, predictive and prescriptive analytics are described. Further, a section on various approaches for real-time analytics such as event stream and data stream mining approaches is presented. IoT Data stream learners for classification, regression, clustering, and frequent pattern mining are explained with examples coded in Python and R. Further, currently popular machine learning and deep learning tools are reviewed.

Chapter 11: IoT in the Cloud

Elucidates the complementary aspects of cloud computing and IoT. The drivers for integration of Cloud and IoT are explained. How the Cloud IoT paradigm is evolving and various cloud computing service

models are described. Emerging new services such as SaaS (Sensing as a Service), SAaaS (Sensing and Actuation as a Service), SEaaS (Sensor Event as a Service), SenaaS (Sensor as a Service), are explained. Current IoT-based cloud providers and their offerings are given.

Chapter 12: Edge Analytics: Near Real-time Sensor Stream Processing
This chapter begins with the definitions of Stream, its characteristics and Stream processing in the context of IOT, and provides a general framework for stream processing. Various existing platforms are described and compared. The concept of Fog computing, which is an extension of Cloud computing to the edge of the network is described. Edge computing and Edge analytics are described in terms of Event stream processing (ESP) and Complex event processing (CEP). Various open source stream processing tools are introduced. An example walkthrough of performing edge analytics is described. This chapter concludes with a scope for future developments and various applications, which are using the stream processing approaches.

Chapter 13: Embedded High Performance Computing (HPC) for IoT
This chapter introduces the basic elements of embedded high performance computing. It explains the need to address the data throughput requirements of high-density computing applications of IoT. Several IoT application areas, which will benefit from embedded HPC are described. A general framework for developing Embedded HPC applications is presented. Graphics processing Units (GPUs) are explained, and introduction to GPU-based cluster computing is presented. Embedded HPC development toolkits are introduced along with various software tools. IoT applications using embedded HPC are described along with a hands-on example on using an embedded HPC platform (Jetson Nano) for image analytics.

Part IV: Data Management in IoT

Chapter 14: Interoperability in the IoT Ecosystem
This chapter addresses the issues surrounding the seamless and meaningful exchange of data and services between various interconnected IoT networks that have different network and communication protocols, data representations and configurations. The IoT architecture reference model (IoT-A) and its various submodels focusing on the immutable components of IoT domain are discussed. Further, various types of IoT interoperability are described. The concept of an Ontology is introduced, and the W3C standard Web Ontology Language (OWL) for developing ontologies is presented. Semantic sensor web development efforts by various organizations are given. The concept of Web of Things is introduced and its usefulness in enabling interoperability by connecting things and applications to the internet is described. The role of W3C in developing and promoting standards related to sensor networks and IoT are also presented.

Chapter 15: CyberSecurity and Privacy
The chapter begins by describing how everyday things will pose high information security risks in an IoT context and how these risks can percolate to various levels. Subsequently, various security issues related to services, hardware resources, information, and data in IoT are presented. The key attributes; data confidentiality, privacy, and trust are described. The specific challenges encountered in IoT security are elaborated. The specific security issues involved each of the IoT layers (perception, network, and

application) are explained. Further, various forms of cyber attacks on IoT infrastructures are explained with examples. Further, various attacks on user privacy are elaborated and solutions to overcome them are presented. Need for lightweight cryptography for IoT systems is elaborated. Best practices for securing IoT devices are also explained.

Chapter 16: IoT and Business Processes Management
This chapter describes the linkages between IoT and Business Process Management (BPM). BPEL and BPMN are explained, and how they can be used for streaming data from IoT to understand optimal paths, exceptions, and business events is discussed. The BPMN extensions required to incorporate IoT processes into BPM are described with illustrative examples. The services based on Services Oriented Architecture (SOA) and BPM processes reacting to sensor-related data and events are also explained through examples. A BPM and IoT case study is described with supply chain management as the application domain.

Part V: Compelling Use Cases of IoT

Chapter 17: IoT Use Cases
This chapter describes the following applications: Smart Agriculture, Smart Healthcare, Home Automation and Smart goods transportation. The description about the targeted organizations/sectors/people are described in each use case. Further, components that are required to build a specific IoT application (based on the use case) such as sensors/actuators, prototyping boards, connections, middleware, and IoT software platforms are presented, along with the corresponding code/pseudo code to develop such an application.

Chapter 18: Future Outlook
This chapter describes the future outlook of IoT from various perspectives. It is described in terms of a roadmap for the next 5 years on different aspects of IoT such as protocols, sensors, platforms, and new applications.

Acknowledgements

Writing this book has been an interesting, challenging and rewarding experience. It took a lot of effort and time, and felt much harder than any other academic work that I have done before. It would not have been possible without the unwavering love, support and encouragement of my dear wife, Gayatri, daughter, Amruta Varshini, and son, Suryansh Prasad, who created the right ambience at home and bore extended periods of my absence while working on the book.

I am eternally grateful to my father, Dr Prasad Rao, and mother, Dr Pushpa, who both being in the academic line, instilled in me very early on the worth of books, strewing them all around the home and leaving no room without the sight of a book. To my dear sister, Dr Sitalakshmi, I express my gratitude for being there with me through thick and thin. I sincerely thank the co-author, Dr Joglekar, for making this book writing endeavour both pleasant and intellectually stimulating. Thanks to my Ph.D. students, Abhisek Potnis and Rajat Shinde, for helping in the development of some hands-on exercises.

I am highly grateful to Dr Roger King for his mentorship. He once said to me "never say never" and I kept believing it since then. My heartfelt thanks to the excellent folks at the Oxford University Press, India for their inputs, feedback and patience.

Any comments and suggestions for further improvement of the book are welcome; please send them at surya.durbha@gmail.com.

Surya Durbha

First, I would like to thank my co-author Dr Durbha, Professor, CSRE, IIT Bombay for his expert inputs throughout the journey that have culminated in the release of this book.

I appreciate my undergraduate and post-graduate interns for performing IoT experiments with me because of which we could present good use-case examples in this book. Thanks to the Oxford University Press, India team for acting as technical proof-readers and editors for compiling this book.

I want to express my gratitude to my brother, Ajit Joglekar, who helped in designing and polishing the figures and illustrations. My husband, Manmohan Soman, and daughter, Pradnya, have been the driving force to keep me motivated and focused. Many friends, especially IIT alumni from industry as well as academia, have contributed real world inputs. I owe them all my heartfelt thanks. Without all of them, this book would not have been possible.

At this moment, I cannot but remember my late mother Shakuntala Joglekar and late father Vishnu Joglekar for everything that I am today. I would like to dedicate this book to them.

Any comments and suggestions for further improvement of the book are welcome; please send them at jyotij1968@gmail.com.

Jyoti Joglekar

Every effort has been made to contact the copyright holders of the assets used in this title. We, the authors and the Oxford University Press, India, would be pleased to rectify any omissions in the subsequent editions of this title should they be drawn to our attention.

The Oxford University Press, India would like to thank all the reviewers, including:

1. J Kayalvizhi (SRMIST, Chennai)
2. Dr TT Mrinalinee (SSN, Chennai)
3. Dr Tarun Kr. Dubey (Manipal, Jaipur)
4. Mayank Deep Khare (NIET, Greater Noida)
5. Mandeep Kaur (Sharda University, Greater Noida)
6. Akshita Baisware (GHRCE, Nagpur)
7. Manisha Ingle (GHRCE, Nagpur)
8. Dr S Mallika (Kongu Engg. College, T.N.)
9. Dr J Senthil Kumar (Mepco Schlenk Engg., T.N.)
10. Dr P Yogesh (Anna University, T.N.)
11. S Jai Kumar (SRMIST, Ramapuram, Chennai)
12. Dr J Raja Sekhar (Mepco Schlenk Engg., T.N.)
13. Arumugam Umamakeswari (SASTRA, Thanjavur)

Detailed Contents

Preface iii

Acknowledgements ix

Part I: Foundational Aspects 1

1. Emergence of IoT 2

1.1 Background and Vision 2

1.1.1 Background 3

1.1.2 Vision of IoT 11

1.1.3 Various Definitions of IoT 12

1.1.4 Working Definition 13

1.1.5 Key Enabling Technologies 14

1.2 IoT as a Disruptive Technology 18

1.2.1 Motivating Scenarios 19

1.2.2 Multidisciplinary Nature of IoT 22

1.2.3 Challenges Involved in its Further Evolution 23

1.3 Standardization 26

1.3.1 Need for Standardization at Various Layers of IoT 26

1.3.2 Organizations and their Efforts for Standardization 27

1.3.3 Factors for Widespread Adoption of IoT 28

2. Concept of Smart Things/Objects 32

2.1 Thing in the Context of IoT 32

2.1.1 Capability to Sense the Environment 33

2.1.2 Ability to Communicate 33

2.1.3 Computation Capabilities 33

2.1.4 Control Other Things 33

2.1.5 Accessibility 34

2.2 Needs of an IoT Thing 34

2.2.1 Self-existence 35

2.2.2 Self-expression 36

2.2.3 Self-actualization 36

2.3 Commonly Used Smart Things 37

2.3.1 How Can Things Become Smart? 37

2.4 Machine-to-Machine Technology 38

2.4.1 European Telecommunication Standards Institute (ETSI) – M2M 38

2.4.2 M2M Service Layer 40

2.4.3 M2M Applications 40

2.4.4 Key Differences Between M2M and IoT 41

3. Wireless Sensor Networks in IoT 43

3.1 Introduction 43

3.1.1 Wireless Sensor Network (WSN) 43

3.2 Characteristics of Wireless Sensor Network 45

3.2.1 Significant Characteristics of WSN 45

3.3 Types of WSN and their Architecture 47

3.3.1 Multimedia Wireless Sensor Networks 47

3.3.2 Mobile Wireless Sensor Networks 48

3.3.3 Terrestrial Wireless Sensor Networks 48

3.3.4 Underwater Wireless Sensor Network 49

3.3.5 Underground Wireless Sensor Network 49

3.3.6 Architectural Design of WSN 50

3.4 Network Topologies in Wireless Sensor Network 51

3.4.1 Different Types of Topologies in WSN 51

3.5 WSN Communication Protocols 54

3.5.1 Single Channel MAC Protocol *54*
3.5.2 Asynchronous Single Channel MAC Protocol *55*
3.5.3 Pseudorandom Asynchronous MAC Protocol *55*
3.5.4 Medium Reservation MAC (MRMAC) *55*
3.5.5 Multi-channel MAC Protocols *55*
3.5.6 Routing Protocols in WSN *56*
3.5.7 Operating Systems for WSN *57*
3.5.8 Simulation of WSN *57*
3.6 Security in WSN *58*
3.7 Real World WSN Applications *58*
3.7.1 Applications of Wireless Sensor Network *58*
3.8 Evolution of WSN Towards Internet of Things *60*

4. IoT Standards and Protocols 63
4.1 An Overview of Internet Principles *63*
4.1.1 Transmission Control Protocol/ Internet Protocol (TCP/IP) *64*
4.1.2 IoT Reference Framework *64*
4.2 IoT Network Level (Addressing Protocol) *65*
4.2.1 IP Version 4 (IPv4) Protocol *65*
4.2.2 IP Version 6 (IPV6) and its Role in IoT *66*
4.2.3 Classification of IPv6 Addresses *67*
4.2.4 IoT Data Link Protocol *68*
4.2.5 Application Layer IoT Protocols *70*
4.2.6 Mobile Communication *74*
4.3 Low-Power Wide Area Network (LPWAN) *75*
4.3.1 NarrowBand-Internet of Things (NB-IoT) *75*
4.3.2 LoRa — LoRaWAN Protocol *75*
4.4 Wireless Technologies Supporting IoT Applications *76*
4.4.1 WirelessHART *76*
4.4.2 Z-Wave *77*
4.4.3 Bluetooth Low Energy *77*
4.4.4 ZigBee Smart Energy *77*
4.4.5 DASH7 *77*
4.4.6 LTE-A *78*
4.5 Network Layer Encapsulation Protocols *78*
4.5.1 6LoWPAN *78*
4.5.2 6TiSCH *79*

Part II: Understanding the Nuts and Bolts of IoT Hardware, Software, and Middleware 83

5. Sensors and Actuators in IoT 84
5.1 Introduction *84*
5.1.1 Sensors for Different IoT Applications *85*
5.2 Perception Layer of IoT *87*
5.2.1 Active Sensors vs Passive Sensors *87*
5.3 Understanding Some Commonly Used Sensors *87*
5.3.1 Light Sensors *88*
5.3.2 Accelerometers *88*
5.3.3 Gyroscopes *89*
5.3.4 Magnetometer *89*
5.3.5 Global Positioning System *89*
5.3.6 Proximity Sensors *90*
5.3.7 Radio Frequency Identification (RFID) *91*
5.4 Environmental Sensors *92*
5.4.1 Temperature Sensors *92*
5.4.2 Pressure Sensors *92*
5.4.3 Humidity Sensors *93*

5.4.4 Wind Speed and Wind Direction Sensors *93*
5.4.5 Soil Moisture Sensors *93*
5.4.6 Leaf Sensors *93*
5.4.7 Lysimeter *94*
5.4.8 Rain Gauge *94*
5.4.9 Chemical Sensors *94*
5.5 Medical Sensors *94*
5.5.1 Heartbeat Sensor *95*
5.5.2 Pulse Sensor *95*
5.5.3 Blood Glucose Level Sensor *95*
5.5.4 Blood Pressure Sensor *95*
5.5.5 Body Temperature Sensor *96*
5.6 Flow and Fluid Measuring Sensors *96*
5.6.1 Level Sensors *96*
5.6.2 Stream Gauge *96*
5.6.3 Tide Gauge *96*
5.7 Range and Motion Capture Sensors *96*
5.7.1 Distance Sensors *97*
5.7.2 Touch Sensor *97*
5.8 Actuators *99*
5.8.1 Servo Motor *99*
5.8.2 Stepper Motor *99*
5.8.3 DC Motor *99*
5.8.4 Linear Actuators *100*
5.8.5 Solenoid *100*
5.8.6 Relay *100*
5.9 IoT Examples *102*
5.9.1 PSEUDO-CODE for the Sketch to Write an Embedded Programming Code Using Arduino IDE *103*

6. Open Hardware in IoT 108
6.1 Introduction to Internet of Things (IoT) Hardware *108*
6.1.1 IoT Hardware and Technology Stack *109*
6.1.2 IoT Device Hardware Requirements *109*
6.2 Prototyping Boards for IoT *111*
6.2.1 Requirement for Custom Silicon (Customized on Board Chip) in IoT *111*
6.2.2 SoC Classification based on Functionality *111*
6.2.3 Arduino Boards *112*
6.2.4 Raspberry Pi *117*
6.2.5 BeagleBone *120*
6.2.6 pcDuino *120*
6.2.7 CubieBoard Open-Source Hardware *122*
6.3 Cellular IoT Hardware *123*
6.3.1 Cellular IoT Hardware *123*
6.4 Industrial Microcontroller (PLC and RTU) *124*
6.4.1 Programmable Logic Controller (PLC) and Remote Terminal Unit (RTU) *124*
6.5 Various Other Hardware *124*
6.5.1 Hardware to Convert Continuous Signal to Digital Signal *125*
6.5.2 Hardware for Signal Conditioning, Scaling, and Interpretation *125*
6.6 Comparison of Different Hardware Platforms *125*

7. IoT Middleware 129
7.1 Introduction to Middleware *130*
7.1.1 IoT Middleware *131*
7.1.2 Functional Requirements of an IoT Middleware *132*
7.1.3 Non-functional Requirements of IoT Middleware *134*
7.2 Architectures of IoT Middleware *135*
7.2.1 Component-based Middleware *135*

7.2.2 Distributed Middleware *135*
7.2.3 Service-Oriented Middleware (SOM) *136*
7.2.4 Cloud-based Middleware *137*
7.2.5 Node-based Middleware *138*
7.3 State-of-the-Art IoT Middleware *139*
7.3.1 OpenIoT *139*
7.3.2 KaaIoT *139*
7.3.3 Node-RED *140*
7.3.4 CHOReOS *140*
7.3.5 Linksmart *141*
7.3.6 CarrIoT *141*
7.3.7 Oracle Fusion Middleware *141*
7.3.8 Google Cloud IoT *141*

8. IoT Software Platforms 144
8.1 Introduction to IoT Software Platforms *144*
8.1.1 Need and Characteristics of IoT Platforms *145*
8.2 Commercial IoT Software Platforms *145*
8.2.1 Amazon Web Service (AWS) IoT Platform *146*
8.2.2 Bosch IoT Suite *146*
8.2.3 EVRYTHNG *147*
8.2.4 IBM Watson IoT Platform *147*
8.2.5 Cisco Kinetic IoT *148*
8.2.6 Google IoT Cloud *149*
8.2.7 Microsoft Azure IoT Suite *149*
8.3 Open IoT Software Platforms *150*
8.3.1 ThingsBoard *150*
8.3.2 OGC SensorThings *151*
8.3.3 Thinger.io *152*
8.3.4 SiteWhere *153*
8.3.5 ThingSpeak *153*
8.4 Choosing an IoT Platform *153*
8.4.1 Domain of Application *153*
8.4.2 Usability *153*
8.4.3 Interoperability *154*
8.4.4 Scalability *154*
8.4.5 Edge Analytics *154*
8.4.6 Security *154*
8.4.7 Recovery *154*
8.5 Hands-On Using an IoT Platform *154*

9. Prototyping IoT Applications 169
9.1 Introduction *169*
9.2 Prototyping and its Benefits *170*
9.2.1 Prototypes and IoT Product Ideas *170*
9.2.2 Selection of Physical Devices *172*
9.2.3 Sketches and Diagrams *172*
9.2.4 Open Source versus Closed Source Technologies *172*
9.3 Physical Design Considerations *173*
9.3.1 Different Modules for IoT Prototyping *173*
9.3.2 Explore, Sketch, and Experiment *176*
9.3.3 Introduction to Mechanical Design and Methodologies *177*
9.4 Prototyping Logical Design *178*
9.5 Prototyping using API *178*
9.5.1 Application Programming Interface (API) *179*
9.5.2 API for Real-time IoT Applications *179*
9.5.3 Packages for IoT in Python *179*
9.6 Embedded Code Writing *180*
9.6.1 Writing Efficient Code *180*
9.7 Real-World Prototype Example: Smart Home Appliances (Light and Fan) *181*
9.7.1 Design Stage *181*
9.7.2 Test Cases *186*
9.8 Best Practices *187*

Part III: IoT Big Data Science and Analytics **190**

10. Big IoT Data Science **191**

10.1 Foundations and Principles of Big Data Science *192*
10.1.1 Introduction *192*
10.2 Concept of a Data Lake/Swamp *210*
10.3 Relation Between IoT and Big Data *212*
10.4 Big Data Analytics in IoT *212*
10.4.1 Real-time Analytics *215*
10.4.2 Offline Analytics/Analytics on the Cloud *218*
10.4.3 Big Data Analytics Platforms for IoT *233*
10.5 Machine Learning and Deep Learning Tools *234*
10.5.1 Tensorflow *234*
10.5.2 Theano *234*
10.5.3 Keras *234*
10.5.4 Scikit-learn *234*

11. IoT in the Cloud **237**

11.1 Introduction: Cloud Computing and IoT *237*
11.1.1 Evolution of Cloud-based Novel IoT Applications *238*
11.1.2 Cloud Computing Service Models *240*
11.2 Integrating Cloud Computing with IoT *242*
11.2.1 Apache Hadoop *242*
11.2.2 Apache Spark *243*
11.3 Cloud Services *243*
11.3.1 SEaaS: Sensing-as -a-Service *243*
11.3.2 SAaaS: Sensing and Actuator-as-a-Service *243*
11.3.3 SEaaS: Sensor Event-as-a-Service *244*
11.3.4 SenaaS: Sensor-as-a-Service *244*
11.4 Selected Cloud Service Providers *244*
11.4.1 Kaa IoT Platform *244*
11.4.2 ThingSpeak IoT Platform *245*
11.4.3 Google Cloud *247*
11.4.4 Oracle Cloud *248*
11.5 REST-based Web Services for IoT *248*

12. Edge Analytics: Near Real-time Sensor Stream Processing **252**

12.1 Introduction *253*
12.1.1 Stream Processing Workflow *254*
12.2 What is Streaming Data? *255*
12.2.1 Bounded vs Unbounded Data *255*
12.2.2 Time-bound Processing of Streaming Data *257*
12.3 Data Stream Management Systems *257*
12.3.1 Background of DSMS Development *259*
12.3.2 Stream Processing Platforms *260*
12.4 Edge Analytics *261*
12.4.1 Event Processing *263*
12.4.2 Complex Event Processing *264*
12.5 Edge Analytics Walkthrough *270*
12.5.1 Problem Background *271*
12.5.2 Steps to Develop the Air Quality Monitoring Applications *272*

13. Embedded High Performance Computing (HPC) for IoT **282**

13.1 Introduction to High Performance Computing *283*
13.1.1 Parallel Computing *284*
13.2 Embedded High Performance Computing (EHPC) *284*

13.3 Graphics Processing Units (GPU) *285*
13.3.1 General Architecture of GPU *287*
13.4 Need for Embedded HPC Edge Devices *290*
13.5 Embedded HPC Platforms *290*
13.5.1 NVIDIA's Jetson TX1, TX2, and Nano Embedded HPC Platforms *290*
13.6 IoT Applications Development using Embedded HPC *292*
13.6.1 Transportation *292*
13.6.2 Healthcare *292*

Part IV: Data Management in IoT **302**

14. Interoperability in the IoT Ecosystem **303**
14.1 Need for Interoperability in IoT Systems *304*
14.1.1 Various Definitions of Interoperability *304*
14.1.2 Current IoT Systems are in Silos *305*
14.2 Types of Interoperability *307*
14.2.1 Device or Technological Interoperability *307*
14.2.2 Syntactic Interoperability *307*
14.2.3 Semantic Interoperability *308*
14.2.4 Organizational Interoperability *308*
14.2.5 Approaches for Interoperability *308*
14.3 IoT Reference Model and Architecture *309*
14.4 Architecture Reference Model *309*
14.4.1 Reference Model *309*
14.4.2 IoT Reference Model *310*
14.4.3 ITU-T Reference Model *316*
14.5 IoT Reference Architectures *318*
14.5.1 Need for a Reference Architecture *318*
14.5.2 Simplified Outline of IoT Architecture *318*
14.5.3 IoT-A Reference Architecture *319*
14.6 Interoperability using Syntactic and Semantic Approaches *321*
14.6.1 Interoperability at Various Layers of IoT *321*
14.6.2 Syntactic Interoperability Approaches *323*
14.6.3 Semantic Interoperability Approaches *324*

15. CyberSecurity and Privacy **330**
15.1 Introduction *330*
15.1.1 IoT Security Challenges *332*
15.1.2 IoT System Security Domains *333*
15.2 Security Issues in IoT Systems and Privacy Preservation *333*
15.2.1 Three-layer IoT Architecture and Security Issues in Each Layer *335*
15.3 IoT Security Requirements Based on CIA Principles *336*
15.3.1 Denial of Service (DoS) Attacks in Physical Layer *336*
15.3.2 DoS Attacks in Link Layer *337*
15.3.3 DoS Attacks in Network Layer *337*
15.3.4 DoS Attacks in Transport Layer *338*
15.3.5 DoS Attacks in Application Layer *339*
15.4 Security Technologies *339*
15.4.1 Network Connectivity Technologies and IoT Device Security Issues *339*

15.5 IoT System Security Controls *341*
15.5.1 IoT Security for Data Access, Integrity, Availability, and Data Communication *341*
15.5.2 Need for Lightweight Cryptography for IoT Systems *342*
15.5.4 Token-based Access Control *345*
15.5.5 Device Status Monitoring *346*
15.5.6 User-friendly Set-up and Upgrades *346*
15.5.7 Access Control for Availability *346*
15.5.8 IoT Security Controls for Middleware Platforms *346*
15.6 Other Security Controls for IoT Systems *347*
15.6.1 Fault Tolerance *347*
15.6.2 Privacy Preservation Methods *347*
15.6.3 Identity Management *347*
15.6.4 Trust and Governance *348*
15.7 Best Practices for Securing IoT Devices *348*
15.7.1 Tamper-resistant Hardware *348*
15.7.2 Firmware Updates/Patch Updates *349*
15.7.3 Dynamic Testing *349*
15.7.4 Strong Authentication Technique Practices *349*
15.7.5 Use of Secure Protocols and Encryption *349*
15.7.6 Network Division into Segments *349*
15.7.7 Sensitive Information Protection *350*
15.7.8 Encouraging Ethical Hacking and Discouraging Safe Harbour for Unethical Practices *350*
15.7.9 Need for IoT Security and Privacy Certification Board *350*
15.8 IoT Security with Best Practices for Home Automation Application *350*

16. IoT and Business Process Management 354
16.1 Business Process *354*
16.2 Business Process Management *356*
16.2.1 BPM Lifecycle *357*
16.3 Business Process Modeling & Notation *358*
16.4 IoT and Business Process Management *359*
16.4.1 IoT-based Business Processes *362*
16.5 IoT and Business Process Execution Language *363*
16. 6 BPM and IoT Case Study: Supply Chain Management *363*

Part V: Compelling Use Cases of IoT 368

17. IoT Use Cases 369
17.1 Introduction *369*
17.2 Use Case for Home Automation Using Smart Home Appliances *370*
17.2.1 Overview *370*
17.2.2 Existing Home Automation Systems *370*
17.2.3 Problem Statement for the Use Case Home Automation using IoT: A Novel Approach *371*
17.2.4 Block Diagram *372*
17.2.5 Hardware Components Used *372*
17.2.6 Sensors *373*
17.2.7 PIR Motion Sensor Module *374*

17.2.9 Actuators *375*
17.2.10 Software Design: UML Diagrams *376*
17.2.11 Pseudocode *377*
17.2.12 Smart Door Lock System *379*
17.2.13 Component List *380*
17.2.14 Sample Source Code in Embedded C for Arduino Uno Board *382*
17.2.15 Output *383*
17.2.16 Energy Saving and Management using Smart Home Appliances *386*
17.3 Use Case: Smart Goods Transportation *386*
17.3.1 Overview *386*
17.3.2 Problem Definition *386*
17.3.3 Hardware and Software Requirements *386*
17.3.4 Block Diagram of the System Model *387*
17.3.5 Software and User Interfaces of the Smart Goods Transportation System *387*
17.3.6 Pseudocode of the Workflow *388*
17.3.7 Major Functionalities of the Back-end Server System *388*
17.3.8 Performance Requirements *389*
17.3.9 Software Design (UML Diagrams) *389*
17.4 Healthcare Use Case: IoT for Healthcare Devices and Challenges *392*
17.4.1 Teleradiology Platform for Screening Covid19 Patients and Remote Diagnosis using IoT Technologies *392*
17.4.2 A Tele-Radiology Platform Solution for Screening with X-Ray AI Module for Screening/Testing Protocol for Diagnosis and Further Treatment *393*
17.4.3 Hardware Requirements *394*
17.4.4 Software Requirements *395*
17.4.5 Methodologies *395*
17.5 Agriculture Use Case: IoT-based Smart Irrigation *396*
17.5.1 Development of IoT-based Irrigation System *396*

18. Future Outlook 404
18.1 Future Roadmap *404*
18.1.1 Device *405*
18.1.2 Network *406*
18.1.3 Platform *408*
18.1.4 Service *408*
18.2 Expanded Opportunities for IoT Applications *409*
18.2.1 Home Automation *409*
18.2.2 Ambient-Assisted Living (AAL) *409*
18.2.3 IoT-enabled Government Services *410*

About the Authors 413

Related Titles 414

PART I: FOUNDATIONAL ASPECTS

Chapter 1: Emergence of IoT

Chapter 2: Concept of Smart Things/Objects

Chapter 3: Wireless Sensor Networks in IoT

Chapter 4: IoT Standards and Protocols

Emergence of IoT

CHAPTER 1

"There are more people in the world who make things than there are people who think of things to make."

- Syd Mead

OBJECTIVES

- introduce the concept of Internet of Things (IoT)
- understand the various definitions of IoT and converge to a working definition
- recap past and current technologies that aided in the development of IoT
- describe the fundamental components of an IoT system
- present various game-changing applications that IoT is driving
- understand how technologies in various disciplines are enabling further evolution of IoT
- explain the issues in the development of disparate IoT systems based on a variety of technologies, and discuss the need for standardization of IoT systems at various levels
- overview of the role of various organizations that are actively involved in the standardization process and their activities

OUTCOMES

- understand the historical context and background of IoT and describe the IoT vision
- describe various definitions of IoT given by different organizations and able to synthesize a definition of your own
- describe key enabling technologies that converged in the development of IoT
- appreciate the interdisciplinary nature of IoT
- understand the need for standardization at various IoT layers
- name various IoT standards and the organizations that are involved in developing them

1.1 BACKGROUND AND VISION

The Internet has dramatically changed the way we conduct our daily life and has become the de facto way of communication. It has spread so deeply in our society that a lot of our routine activities are now driven by technology and are highly dependent on the Internet. By using mobile devices, we are able to conduct both personal and official businesses more efficiently. For example, with just a touch on the mobile screen, a host of services are available, such as ordering food, buying shoes, arranging meetings, keeping in touch with people, and buying tickets. Having Internet connectivity has become a way of life and will continue to percolate in many areas, which are previously unimagined.

It has revolutionized many domains and brought in many new applications to the forefront. The last decade has seen an accelerated synthesis of research in several path-breaking technologies, particularly in the areas of semiconductors, networking, and information processing. In addition, there has been a significant drop in the prices of sensors, transmitters, processors, and computing infrastructure. These have revolutionized both the information and communication technologies (ICT) and non-ICT areas. Consequently, a new paradigm has emerged called the Internet of Things (IoT), which aims to make things (physical objects) smart using sensors/actuators and digitally identifiable over the Internet so that these can be seamlessly accessed and controlled remotely. Further, these things have the ability to react in real time to the events in the environment that they exist, and send information to humans as well as other things autonomously to enable them to contextually respond for decision-making.

Gartner, a leading research and advisory company, predicts that by 2020, there will be 20.8 billion IoT devices connected around the world, overtaking the number of personal computers and smartphones. Another estimate by Cisco projects that nearly half of the devices connected to the Internet by 2023 are IoT devices (see Fig. 1.1).

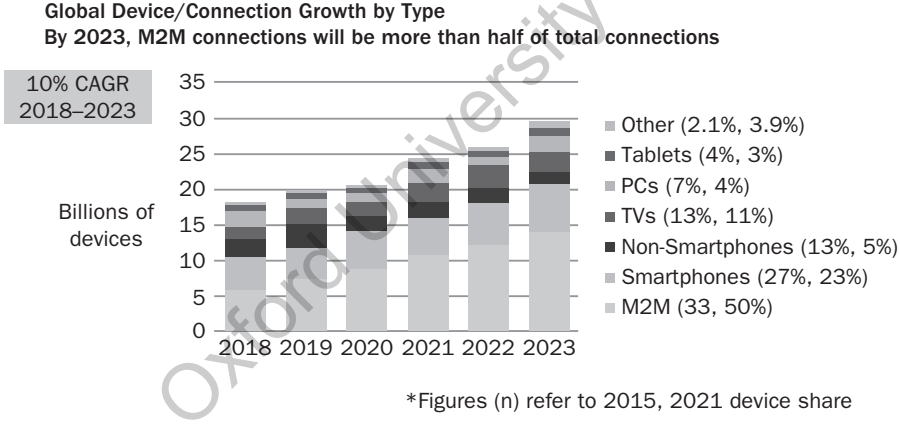


Fig. 1.1 Number of Devices Connected to the Internet by 2023; Half (51%) of Them are IoT Devices

(Source credit: Cisco)

To understand this fast-paced development and adoption of IoT technologies in a better way, it is necessary to travel back in time and look at the key events and technologies that helped shape the current IoT. The historical context of the emergence of IoT is described in the next section.

1.1.1 Background

Although IoT has emerged recently, its roots go back to about two decades. In 1982, a Coke machine at Carnegie Mellon University (CMU), was fitted with micro-switches and was connected to a computer to show how many coke bottles were left in the machine, so that anyone can just ping to it before going

to the vending machine to pick up a bottle. At that time, CMU was part of the ARPANET, so other universities were also able to find out the number of coke bottles left. Thus, it became one of the very early examples of an IoT device.

In 1991, ubiquitous computing was proposed by Mark Weiser (Weiser, 1991). In 1995, Siemens developed the first Machine-to-Machine (M2M) communication application. It was used for sales terminals. In the year 1998, the Internet protocol IPv6 was developed and launched by the Internet Engineering Task Force (IETE) to overcome the IP address exhaustion problem of IPv4. IPv4 had only 32-bits, that is, a total of 2^{32}, which are not enough to handle the huge number of IoT devices currently and for future expansion. IPv6 is 128-bits, so a total of 2^{128} addresses are theoretically possible, which are more than enough to cope with the ever expanding IoT devices in the coming years.

In the year 1999, Bill Joy wrote about Device-to-Device communication in his taxonomy of Internet (Pontin, 2005). In the same year, the Auto ID centre at MIT was working on the Radio Frequency Identification (RFID) technology for asset tracking and supply chain management, where companies will be able to track their products and reduce operating costs. The team comprising of Kevin Ashton, Sanjay Sarma and David Brock, developed a way to connect objects to Internet via a RFID tag, making

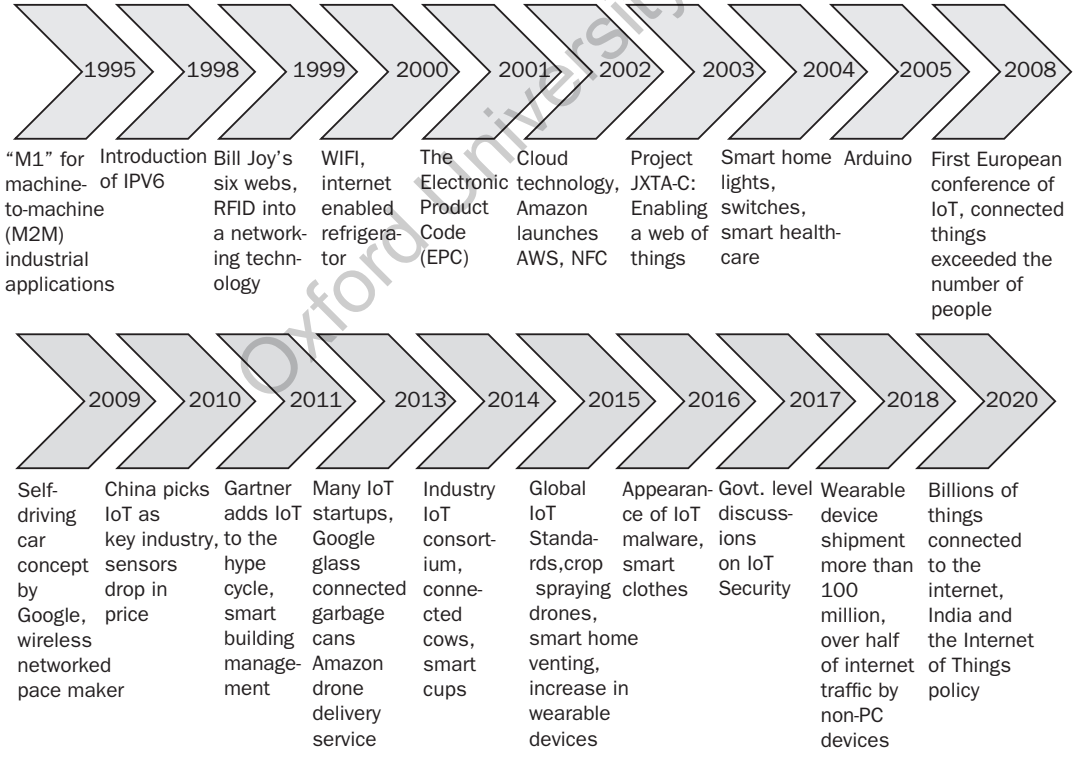


Fig. 1.2 Timeline of IoT Technology Maturity

BOX 1.1: VARIOUS AUTO-ID TECHNOLOGIES

Barcodes, RFIDs, QR Codes, and NFC

Barcodes, QR Codes, RFID, and NFC are all systems for conveying large amounts of data in a small format.

Standard UPC-A barcode

Barcodes These are limited to 20 alphanumeric characters and data is stored only in the horizontal direction. UPC consists of 12 numeric digits that are uniquely assigned to each item at the point of sale. The bars represent numbers. These are inexpensive as they can be printed on paper or plastic. The data on the barcodes cannot be rewritten. Barcodes help to identify the type of the item, but not an individual item. The line of sight is important to scan the code properly. Reading items using a barcode could be time consuming as it can only read one item at a time.

Radio Frequency Identification (RFID) It uses electromagnetic fields to read and capture information stored of an object by reading a unique tag attached to it. It can be used for identification, authentication and tracking of items. It can store 1000s of characters.

1. **Passive RFID:** Ultra High Frequency (UHF) Passive RFID Tags operates in 860 ~ 960 MHz and has a read range of about 1 meter. Generation 2 (Gen2) RFID tags can have a read range of up to 12 meters. The new generation of tags, that is, Gen3 and Gen4 are based on new silicone IC and read ranges can reach up to 16 meters.
2. **Active RFID:** It operates in the Ultra high frequency at 433 MHz. These can have a read range of up to 500 meters. Another variant of the active RFID is the 2.45 GHz. Super High Frequency tags. These can have a read range of up to 100 meters. The advantages of the active RFID are: (1) ability to obtain real-time location information, which is useful in any location and tracking applications (2) data on the RFID tags can be rewritten and reused (3) identification of individual item rather than only the item type is possible with it, that is, it gives a count of the number of items that are present in a particular product. An RFID can read potentially 100s or even 1000s of tags simultaneously. Currently, many quick payment systems, anti-car theft devices use 13.56 MHz RFID systems.

Quick Response (QR) codes It is a type of two-dimensional barcode first designed for the automotive industry. The code consists of black modules embedded in a square pattern on white background. It can work both in horizontal and vertical directions and can hold up to 300 times the information that could be encoded in a UPC barcode. QR codes can be quickly read and scanned from any direction.

Near Field Communication (NFC) NFC technology has its roots in RFID. When two electronic devices are brought close (within 4 cm) to each other, a communication is established and data can be exchanged. Normally a 'Tap' is done with the item and the required information is transferred. These are used in many applications such as identity/key cards and credit cards. An NFC-enabled smartphone can be used to make several types of transactions such as payments in a retail store. NFC tags are inexpensive and are becoming quite popular currently.

it a networking technology (Roberti, 2005). A majority of sources attribute Kevin Ashton for coining the term 'Internet of Things' in a presentation he made for Proctor and Gamble (P&G), in which he emphasized the need for a standardized way to make computers understand the real world. The important aspect of this endeavour is connecting the Internet to the physical world (objects connection using RFID) through wireless sensing networks (WSNs). It was a pioneering solution at that time because there was no widespread usage of Internet Protocol (IP) configurations by mobile networks then. See Box 1.1 for more details on various Auto-ID technologies.

In the year 2000 (Fig. 1.2), the Internet-enabled refrigerator was launched by LG. The consumer could get the information about the temperature, freshness of the food, and nutrition information on a LCD screen attached to the refrigerator.

In 2001, David Brook, proposed the Electronic Product code (EPC) to address the issue of tracking a product throughout its lifecycle. He suggested a unified product directory for this purpose. The EPC provides a unique identity to any object. It is designed to be stored on a RFID tag. Bernard Traversat in 2003 (Traversat et al., 2003) published the paper 'project JXTA-C: Enabling the web of things' in which a standard and open source set of protocols for ad hoc, pervasive, peer-to-peer computing were proposed for the Web of Things.

By the year 2004, major transition for smart things has gained and many publications were describing various smart devices in areas such as healthcare, smart bulbs/switches, and transportation. For the first time, Walmart deployed RFIDs on a large scale to keep track of its inventory.

The open hardware-based microcontroller Arduino appeared in 2005. It was developed by faculty members at the Interaction Design Institute (IVREA), Italy. It brought with it a revolutionary change in the embedded computing arena. With its intuitive interface and ease of programming, it enabled non-domain (e.g. non-electronics background) people also to venture into smart devices development. The product ideas were limited only by the resourcefulness and imagination of developer. Several online web portals sprung up offering various sensors, electronic components, and PCB shields that could be easily put together to prototype quickly. Further, several community-based online forums were formed to help developers ideate, implement, and exchange information about innovative IoT devices. In the same year, Ubiquitous Network Societies emerged, almost 15 years after the Ubiquitous term coined by Mark Weiser, who described it as:

(i) A new era in which small non-traditional computing devices will be embedded in everyday objects invisibly at work in the environment around us.
(ii) The applications that are built on the concepts of ubiquitous computing will use these non-traditional computing devices in a large number.
(iii) The computing devices will have sensors to measure various environmental parameters and be able to act independently based on certain predefined conditions.
(iv) The computing devices are mobile and have geographical location and usually the devices in a neighbourhood are often used for a particular task. Hence, communication networks should connect these devices together in an ad hoc and spontaneous manner, and form temporary networks to facilitate anywhere, anytime, always-on communications.

The year 2008 marked the first European conference, which took place in Zurich, Switzerland. During that time, several key industry players such as those from semiconductors, communications, networking, and Internet providers, have made vital contributions to further promote the growth of IoT.

Google launched the ambitious self-driven cars project in 2009, it has heralded a new era in autonomous vehicles area. It is significant from an IoT perspective as it combines the major components of an IoT system, ranging from sensors/actuators that are deployed on various parts of a car (e.g., wheels, bonnet, bumper, and seats) and also those that allow measuring the surroundings around it. These inputs are fed through various models and are continuously learned and used to trigger responses to various events happening inside and outside of the car (e.g., seat belts, temperature, detecting pedestrians, and lanes). Another device that made its entry in the same year was the wireless networked pacemaker that is inserted directly into the heart without surgery and can deliver electric pulses to the heart for its proper functioning.

The fast-paced developments happening in the IoT area prompted China to declare IoT a key industry and included it in its 12th 5-year plan. A national IoT centre was established in Shanghai in the same year. Across the country several initiatives begun on developing a range of standards, industry chains, and applications, which aimed at creating an industry worth more than CNY 500 billion over the coming decade.

Gartner, a leading research and advisory company added the IoT to its hype cycle in 2011. It tracks specific technologies and their advancement through a life cycle from 'technology trigger' to 'plateau of productivity'.

The year 2011 also saw the emergence of the smart building concepts. McGlinn et al., 2010, define Smart Buildings as an environment, which is "able to acquire and apply knowledge about the environment and its inhabitants in order to improve their experience in that environment" (Cook and Das, 2007). Smart buildings are characterized by real-time measurement and monitoring of various building management infrastructure [e.g., Heating, Ventilation, and Air Conditioning (HVAC)], external environment such as weather, noise, light, people movement, and energy pricing, and optimize energy consumption and ambience in the building. This can be achieved by IoT devices measuring various parameters in and outside the building. Such real-time data can be used to perform smart analytics (e.g., Edge analytics) and trigger intelligent control mechanisms.

Buoyed by the great potential of IoT and its wide commercial applications, several start-ups began to emerge in the year 2013. Google glass also appeared in the same year. However, it was discontinued in 2015 due to privacy and safety concerns (a new version of Google glass is launched for enterprise applications in 2018). Amazon's Drone-based delivery prototype was announced in 2013 and named it 'Prime Air'. Due to restrictions by Federal Aviation Administration (FAA), the project could not take off immediately. The first delivery happened in UK in 2016 as a proof of concept. IoT application for garbage management was also demonstrated in the same year called the connected cans that can send an alert when the garbage can is full so that the pickup can be planned by the garbage-collecting trucks. The industrial Internet Consortium (IIC) was founded in 2014 to "accelerate the development, adoption and widespread use of interconnected machines and devices and intelligent analytics" (IIC, 2018). Several industries in areas of Energy, Healthcare, Manufacturing, Mining, Retail, Transportation, and Smart Cities are involved in IIC.

Fig. 1.3 IoT-based Smart Cup Capable of Sending Nutritional Information to a Smart Phone

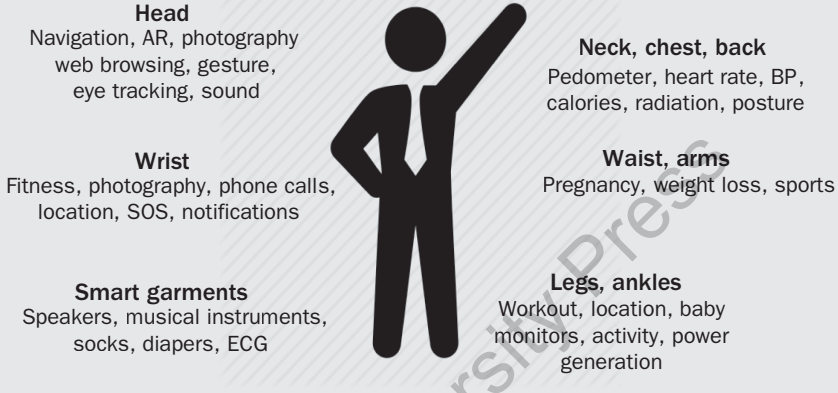
Connected cow was an interesting application that appeared in the same year. It has transformed the dairy industry by enabling the dairy companies to monitor individual cows by tagging with RFID and other health monitoring sensors and transmit the information in real time to help monitor health and other location specific attributes. This led to more focussed treatment for diseases (if any), and also provide optimal nutrition, thus boosting the milk yield. Currently, many companies including Microsoft, Huawei, and Fujitsu are involved in providing IoT-based solutions for this purpose. A 13-ounce smart cup named 'Vessyl' made its first appearance around this time (see Fig. 1.3). Any beverage poured into it is recognized and the related nutritional value is displayed on the smartphone. Further, it can also keep track of the drinking habits of the user and provide that information via a smartphone.

The year 2015 saw the emergence of global IoT standards with a meeting in Geneva, Switzerland. A group called the IoT global standards initiative (IoT-GSI), which is part of International Telecommunication Union (ITU) was formed whose aim is to promote a unified approach for developing standards for IoT to enable it to scale at the global level.

The year 2015 also saw the emergence of drones in agriculture. Drone-based sensing was demonstrated in the areas of crop health monitoring, irrigation equipment monitoring, and weed detection. The ability to monitor at high temporal frequency made this technology very attractive to the farmers. Another area that saw the use of IoT is the smart home venting systems that allows adding room-by-room smart vents that can control the central air conditioning installations. This enables to distribute the airflow from rooms that are over conditioned to those rooms that need more air. All these can be achieved by IoT devices and smartphone applications. The wearable devices market also emerged in the year 2015 (see Box 1.2).

BOX 1.2: WEARABLE DEVICES

Wearable technology is related to the development of devices that are worn directly on body or on the user's clothing, which helps to track a user's data related to health and fitness, location, emotions, gestures, and other reflexes of the human body. The wearable technology can help the user to continuously record, monitor, and analyse internal and external stimuli and react based on certain preset controls.



A wearable device can have sensors, computing architecture and display. Depending upon the parameter (e.g., pulse, gesture, etc.) that is being tracked, the wearable may use the computing on its device (very limited) or delegate an external device such as a smart phone to do the computing. Similarly, the display on a wearable depends on the amount of information that needs to be shown. If it is limited, then it is displayed on the wearable itself (e.g., smartwatches); otherwise, it is shown on a smartphone, nearby display, or ear buds (verbal communication).

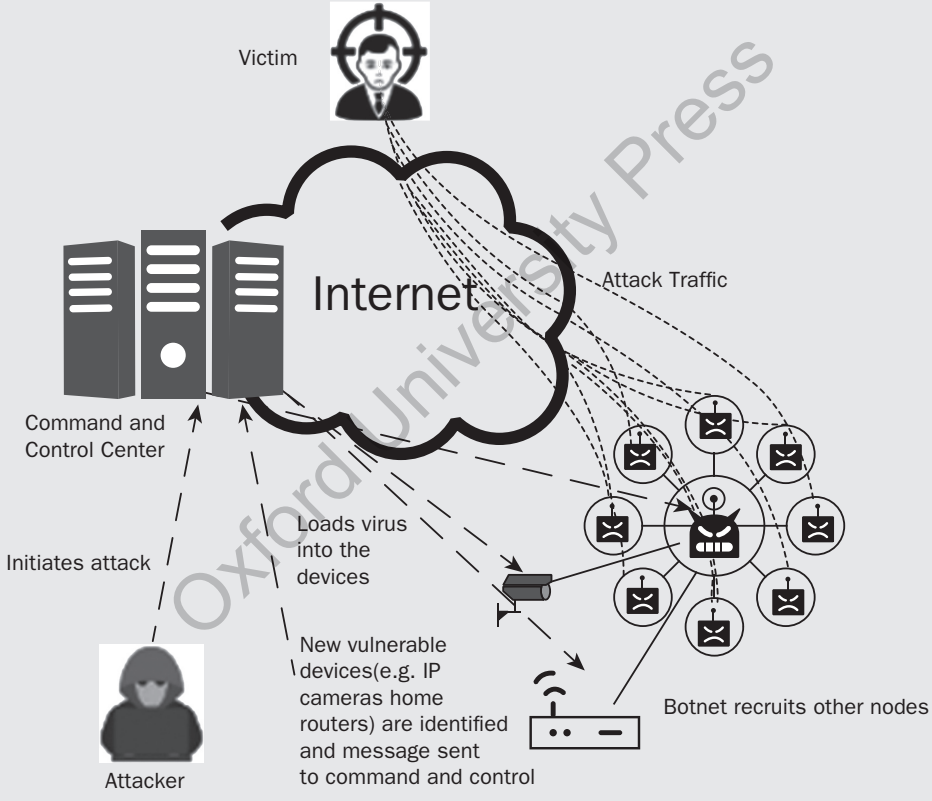
Due to increasing adoption of wearables, the global wearables shipment is expected to reach 2.5 billions in 2023. Currently it is in the early phases, and mainly dominated by healthcare, activity, and fitness wearables.

In 2016, IoT reached the peak of inflated expectations. It is expected that it will take another 5 to 10 years for the technology to mature and reach a stage where it could be widely adopted. Similarly, several key components of it, such as IoT platforms, IoT architectures, and wide-area IoT networks, have not peaked (i.e., reached a high level of expectations yet) and are also expected to reach the plateau of productivity in another 5 to 10 years. Whereas, other components such as IoT services, IoT edge architecture, IoT for customer service, and messaging platforms such as MQTT are expected to quickly reach wide adaptability in a span of another 2 to 5 years. Another key component for real-time decision-making in IoT systems is the event stream processing (although developed independently of IoT) has reached high expectation levels for its application in IoT edge analytics. Many event stream processing engines are emerging, but it is expected to take another 5 to 10 years, for it to be completely adopted and integrated with IoT edge analytics. Another, closely related innovation are the low-cost development boards (e.g., Arduino, Raspberry Pi, etc.), which have played an important role in enabling users from diverse disciplines to work in IoT. These low-cost development boards and related

programming interfaces have reduced the complexity of developing certain class of electronic products, particularly those that are useful for IoT.

In August 2016, the Mirai malware appeared and targeted under-secured networked devices running Linux OS systems into bots and recruited them to be part of a larger botnet network that can trigger large-scale attacks. The devices that were affected by this malware were mostly IP cameras and home routers (see Box 1.3). Smart clothes that monitor the wearer's physical condition began to appear in the wearable segment of IoT in 2016 (see Box 1.2).

BOX 1.3: MIRAI MALWARE CONVERTED INTERNET OF THINGS INTO BOTNET OF THINGS



In October, 2016, Paras Jha, Josiah White, and Dalton Norman used their Mirai botnet, which is a piece of malware that gets installed on under-secured IoT devices such as IP Cameras, home routers. These then become bots and are recruited by other bots and form a network known as a botnet. The attacker then initiates a Distributed Denial of Service (DDoS) attack. In this case, they attacked the domain name server (DNS) Dyn causing the shut down of a number of major websites including Twitter, Reddit, and the New York Times. Subsequently they were indicted by a court in Alaska and have pleaded guilty to charges that carry a sentence of up to 5 years in prison.

(Contd)

Box 1.3 *(Contd)*

The main functionality of the Mirai malware was to search for under-secured IoT devices by scanning wide-ranging IP addresses and finding those devices, which can be easily accessed based on a dictionary of user-name/passwords (usually the default factory set credentials). Subsequently install the virus and make it as a part of a bigger network. Next, based on the instructions received from the command and control centre, use this network of bots to launch DDoS attacks on specified targets.

The security aspects of IoT received wide attention in 2017 owing to the large-scale attacks that happened in the preceding years. The US government enacted a bill called the 'Internet of Things Cybersecurity Improvement Act 2017', which basically mandates all the IoT devices that are sold to the government to have security measures and these include wearables, sensors, IoT tools, etc. Further, compliance in terms of including industry standard protocols, passwords that can be changed (controlled) by the users and do not have any known vulnerabilities (as defined by the National Institute of Standards (NIST)) (NIST, 2018).

In 2018, the number of wearables that were shipped crossed 100 million units. IoT is providing a great market opportunity for companies involved in IoT hardware manufacturing, Internet service providers, and application developers. The global IoT market is expected to have a compound annual growth rate (CAGR) of nearly 27 per cent from 2018 to 2024.

The IoT market is fast gaining ground and many industry leaders such as Google, Amazon, IBM, CISCO, Samsung, Intel, and Apple have announced new products in the IoT landscape. Along with these, a plethora of start-ups are testing ground. The industry is investing mainly in the areas of manufacturing, healthcare, transportation, consumer electronics, smart cars/fleets, home automation, and utilities.

By the year 2020, billions of things are expected to be connected to the Internet.

1.1.2 Vision of IoT

The vision of IoT can be perceived from four major perspectives (Fig. 1.4):

Things perspective The persistent and reliable availability of anything that is of interest to the user, which could be connected in anyway using a variety of technologies. Further, these connected things should be available to be accessed at anytime and from any location. This is similar to the ubiquitous computing concept that was there much earlier before the advent of the IoT.

Standards and semantics perspective Access of the things should be seamless, which is possible only if well-defined standards are adhered to by the providers of these things as they are highly heterogeneous in nature. In addition, the things should be interoperable, that is, the ability to integrate data from heterogeneous IoT devices is a must, otherwise, many IoT applications will be very specific to a particular application domain and cross-domain integration becomes highly challenging. Hence, standards are necessary in every component of the IoT architecture.

Internet perspective The aforementioned two are possible only if the things are able to communicate with people and people with things (people 2 things, i.e., P2T), and further, among things themselves (things 2 things, i.e., T2T), so that certain level of autonomous decision making is achieved. Hence, the web enablement or web addressability is one of the prime goals of IoT.

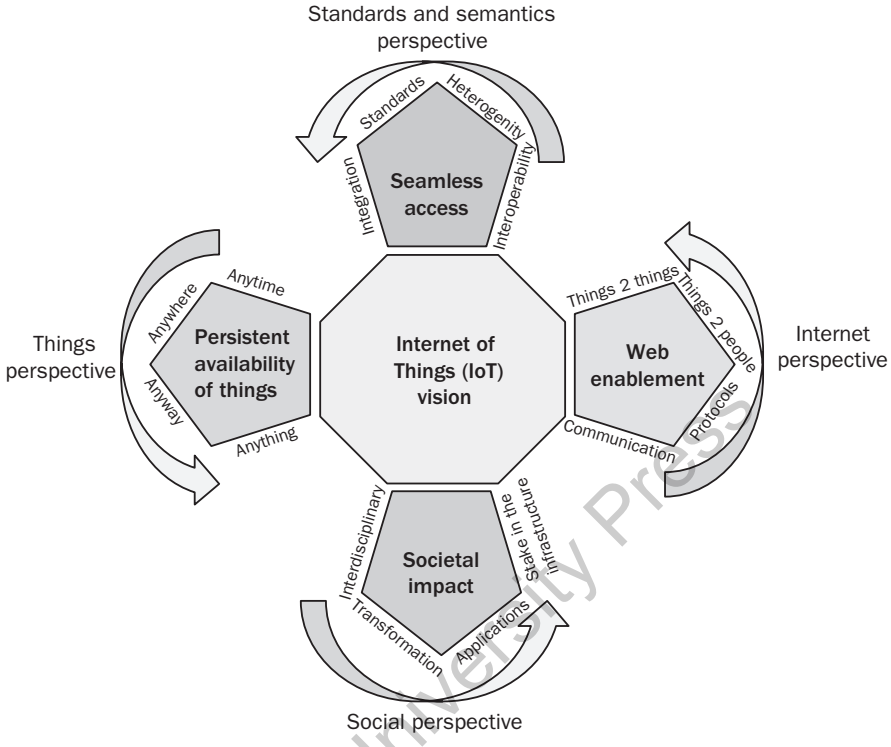


Fig. 1.4 The Vision of IoT from Four Different Perspectives

Social perspective The societal impact of the IoT is primarily driven by the acceptance of the users and their perceived value that it would bring to their lives. It is envisioned that the IoT infrastructure will be owned by the stakeholders in some form of democratic process, who will develop, maintain, and take in directions that are congenial for their growth. The society will be benefited by a spectacular transformation of traditional services into IoT-based smart services that provides applications that are much easier to use and provides far-reaching benefits. These IoT services also operate in an interdisciplinary mode, where they can be easily integrated and a common set of services will come together and cooperate in real time to address a particular problem. Several applications such as monitoring air pollution, improved water conservation, and increased production of food grains.

1.1.3 Various Definitions of IoT

The understanding of IoT is being approached from various perspectives and based upon a particular domain and its view of the components involved in the IoT systems. There may be specific emphasis on particular modules that are important in that domain. Hence, there is no global consensus on an overarching IoT definition. Indeed, there have been efforts by organizations such as IEEE to lead an initiative for developing a definition of IoT. Following are some selected definitions of IoT.

1.1.3.1 IEEE Definition

IEEE led an initiative in 2015 on developing a definition for IoT. In the special issue of IEEE on Internet of Things, IoT is defined as:

"A network of items, each embedded with sensors, which are connected to the internet."

1.1.3.2 ITU Definition

The international Telecom Union (ITU) defines IoT as:

"A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies."

1.1.3.3 IETF Definition

The Internet Engineering Task Force (IETF) is playing a crucial role in the development of several standards for IoT. They define IoT as:

"IoT will connect objects around us (electronic, electrical, non-electrical) to provide seamless communication and contextual services provided by them. Development of RFID tags, sensors, actuators, mobile phones make it possible to materialize IoT which interact and cooperate each other to make the service better and accessible anytime, from anywhere."

1.1.3.4 OASIS

Organization for the Advancement of Structured Information Standards (OASIS) is a non-profit consortium that drives the development, convergence, and adoption of open standards for the global information society. It describes IoT as:

"System where the Internet is connected to the physical world via ubiquitous sensors."

In addition to standard bodies such as IEEE, IETF, and ITU, there are several projects that have also given definitions of IoT such as:

1.1.3.5 IoT-A

Internet of Things Architecture (IoT-A) developed an *Architecture Reference Model (ARM),* which addresses the issues of heterogeneity in IoT-related technologies. IoT-A defines it as:

"It can be seen as an umbrella term for interconnected technologies, devices, objects and services."

1.1.3.6 Texas Instruments

Texas instruments in its paper on evolution of Internet of Things defines IoT as:

"The IoT creates an intelligent, invisible network fabric that can be sensed, controlled and programmed. IoT-enabled products employ embedded technology that allows them to communicate, directly or indirectly, with each other or the Internet."

1.1.3.7 Gartner

"The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."

1.1.4 Working Definition

Based on the aforementioned definitions, it is useful to have a working definition whose spirit will be used as the foundation for the rest of the contents of this book.

IoT = Sensing + Communication + Computation + Web Application

"Making things (objects) to sense the environment in which they exist, communicate, access, actuate, and process data autonomously with other things in a network, and also with humans via web applications."

1.1.5 Key Enabling Technologies

The enabling technologies of IoT are distributed in several layers of the IoT systems. The technologies at each of these layers are specialized and serves some key purposes for the functioning of that layer. These can be categorised into four major categories (Fig. 1.5).

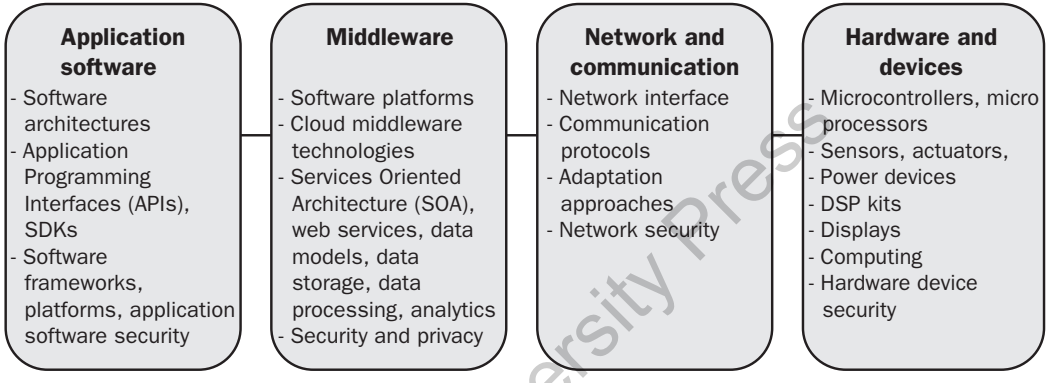


Fig. 1.5 Major Categories of Enabling Technologies for IoT

1.1.5.1 Applications and Software

Currently, the IoT technology is being applied in a variety of fields due to its immense potential to create more smarter ways of performing various tasks in those domains. IoT applications have emerged in many domains such as healthcare, transportation, smart cities, industry, and energy management. Most of the traditional approaches in these domains are getting transformed by using the new IoT system functions to build practical applications. The main enabling technologies for IoT in this layer are:

Application Programming Interfaces (APIs) The application programming interface, or API enables to integrate the 'things' of IoT and act as a glue between the IoT devices and the network (e.g., Internet). It provides an interface for other applications to interact with your application without having direct access. From an IoT perspective, device level APIs can be used to enable applications to communicate with devices. For example, Google IoT product NEST is a smart Thermostat that can control via a mobile phone the temperature in a home/office setting. While the manufacturer of NEST has provided the core applications to interact with the NEST device, they also provided an API. Using the API, developers can connect and use the NEST data in their own applications and sell them. Development of APIs that allow to securely expose connected IoT devices to users are one of the key enabling technologies for IoT. Many IoT-based APIs are available.

Software Development Kits (SDKs) Software development kits have pre-built functionality to make them easier to work than an API thus making them easier to integrate in an application. For example, the amazon IoT SDK allows hardware devices to connect device gateway and device shadow. Similarly, the Azure IoT has three main IoT SDKs including device SDKs, service SDKs, and Gateway SDK.

1.1.5.2 Middleware

The purpose of an IoT middleware is to function as a mediator between the hardware (IoT devices) and the application layers. Its primary tasks include collection, aggregation, filtering, and processing of data from heterogeneous devices over a variety of protocols and network topologies. Some examples of IoT middleware are Google Fit and Apple's HealthKit, which allows users to access and control their fitness data generated by variety of devices (e.g., wearables) and mobile applications. Xively is another IoT-based middleware that allows sensors to connect to its platform easily and store the data persistently, so that it can be seamlessly retrieved anytime. Node-RED is an open-source IoT middleware platform from IBM, which provides a visual tool to compose an IoT application by simply dragging and dropping its various components.

Some of the enabling technologies in these areas are:

IoT platforms An IoT platform is designed to seamlessly manage any kind of connected device, irrespective of the underlying protocols. The IoT platform can:

- Connect various components of the IoT system such as IoT sensors and devices
- Enable communication between different hardware (e.g., edge hardware) and software irrespective of the underlying protocols
- Handle authentication, security, and privacy
- Device management functions such as monitoring, troubleshooting and administration
- Enable aggregation, analysis and visualization of data

These IoT platforms are in between the data collected at the IoT gateways and the end application. It is estimated that the IoT platform market share will cross over $22 billion by 2023.

Data storage Cloud-based data storage is the most common form in IoT rather than storing it on the premise of where the data is collected. Although, it increases the cost, the main advantage is the connectivity it provides to the users. Users can access the data from the device, anytime and from anywhere.

Data processing One of the key functions of an IoT middleware is the ability to manage the huge data that is being generated by the IoT devices. This kind of data can be considered as big data. The attributes of big data such as Velocity, Volume, Variety, Value, and Veracity are present in the data generated by the IoT systems. Various IoT Middleware provides the ability to do analytics on both continuous streaming data as well as data that is stored. A publish/subscribe kind of middleware can provide functionality for continuously processing of the data using various data processing functions such as preprocessing, filtering and data mining approaches.

Edge/Fog computing Various other forms of computing technologies are becoming key enablers in the middleware domain such as Edge computing, which facilitates the computation to be performed on computing infrastructure available close to the devices and sending the result directly to the relevant application. There is a no collection point or cloud in this type of computing. Fog computing is another emerging approach, where the computation is placed at the edge of a network.

Security and privacy Due to the vast amounts of data stored and managed by the IoT middleware, the main concern is of security and privacy. Many cloud middleware systems provide authentication and authorization services. Recently, new security algorithms and tools have been developed to address the requirements of low powered IoT devices.

1.1.5.3 Ubiquitous Connectivity

It is expected that billions of devices are going to be connected to the Internet in the near future. In addition to this connectivity, the devices themselves need to communicate with other devices as well as various other forms of computer systems (e.g., Gateway). As these devices are energy constrained, the optimization of energy during wireless communication is of utmost importance. These communication technologies can also be distinguished in terms of the system performance, frequencies, Medium Access Control (MAC) scheme, and standardization process (i.e., open vs proprietary).

The key enabling technologies in this area can be classified into proximal range, short range, short/medium range, medium range, and long range.

Proximity Each IoT application has its own requirement depending upon the environment in which the IoT system is deployed. The communication protocols such as Radio Frequency Identification (RFID), Near Field Communication (NFC) work in the proximity range, that is, 0 to 10 meters. Several applications particularly in the retail sectors uses NFC for bill payment at checkout by just such as payment at retail checkout by tapping a credit card with an item having an NFC tag.

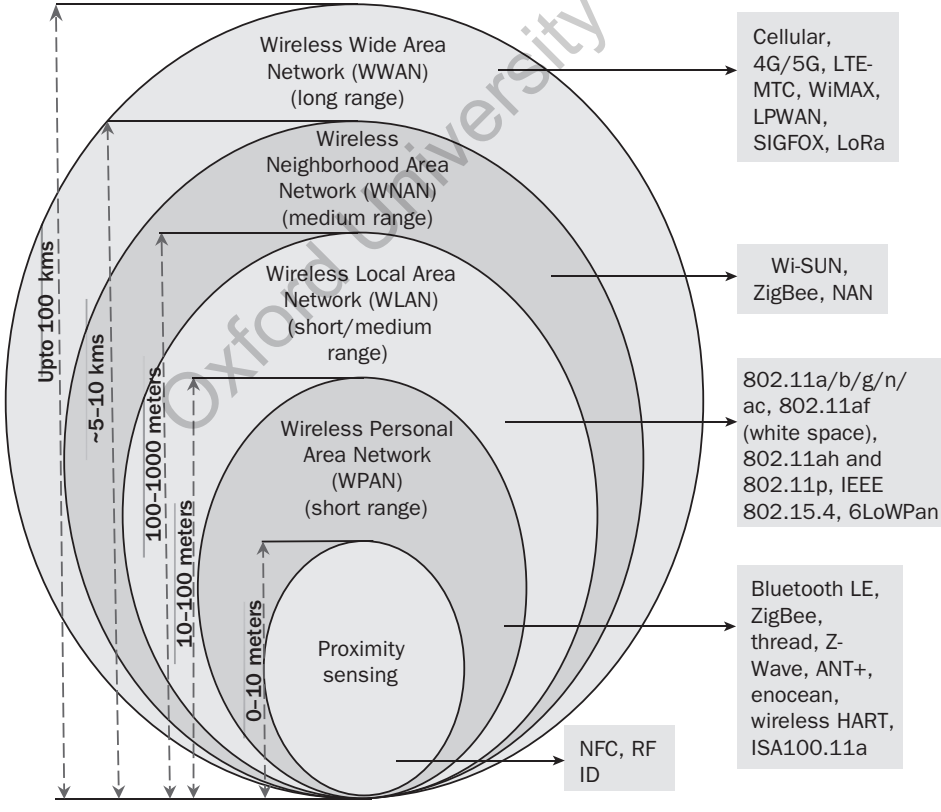


Fig. 1.6 Various Types of Short-, Medium-, and Long-range Connectivity in IoT

Short range In the short-range communication space, applications such as Wearables, Home automation, and Healthcare are popular. Key enabling technologies for this type of communication are Wi-Fi, Z-Wave, ZigBee, IrDA, Bluetooth, Bluetooth Low Energy, and Radio Frequency Identification (RFID) (see Fig. 1.6).

Short-to-medium range In this range of communications, Wi-Fi is a popular technology for many years now. IEEE developed a set of five (designated as a, b, g, n, and ac) media access control (MAC) and physical Layer (PHY) specification for wireless local area network (WLAN) called the IEEE 802.11. These are abbreviated as BGN, ABGN, and A/B/G/N/AC in the specifications for wireless routers, Wi-Fi access points, and Wi-Fi in portable devices. However, since these Wi-Fi protocols have fairly large energy consumption, they are not very useful for IoT devices due to their low-power requirement. To overcome this issue, duty cycling (i.e., keeping the chips in sleep mode for most of the time) and other energy-harvesting methods are being developed. A low power Wi-Fi standard emerged called IEEE 802.11ah. Another enabling technology that is specifically developed by IETF for IoT is the 6LoWPAN, which defines the mechanisms for transmitting IPv6 (128-bit Internet scheme that offers about 3.4×10^{38} unique addresses to accommodate the requirements of the IoT) packets on top of IEEE 802.15.4 networks which defines low-data-rate, low-power, and short-range radio frequency transmissions for wireless personal area networks (WPANs).

Long range There are two main options available for IoT system developers to enable long-range communication in their systems.

Cellular These technologies operate in the licensed spectrum. The key technologies in this space are GSM, WCDMA, 3G/4G/5G, LTE-MTC, and WiMAX providing high-quality voice and data services. The 3rd Generation Partnership Project (3GPP) is a collaboration between groups of telecommunications standards associations that developed Narrowband IoT (NB-IoT), which is a Low Power Wide Area Network (LPWAN) radio technology standard.

Unlicensed low power wide area network The technology in this area uses the unlicensed spectrum and mostly proprietary in nature. Technologies such as SIGFOX and LoRA are popular for machine-type communication (MTC) applications addressing the ultra-low-end sensor segment.

1.1.5.4 Hardware and Devices

Miniaturization and composability Novel hardware developments are enabling the development of ultra-compact wireless. Advancements in the miniaturization of the hardware mainly through the use of the microelectromechanical systems (MEMS) technology is enabling the development of a new generation of devices that are ultra-compact and have high computing ability. Further, nano-electromechanical systems (NEMS)-based sensors are miniaturizing the sensors to nanometres size. Wearable medical devices that are almost invisible to other individuals are currently available. The Moore's law states that the density of transistors on silicon chips doubles every 2 years. This is evident from the fact that today's devices (e.g., smartphones) have the computing power of yesteryears high end computing systems and even supercomputers. Further, the increased ability to put together complex systems from simpler components is enabling the development of revolutionary products in many areas.

High durability The IoT sensors are expected to work in harsh situations. In many field-based applications, these sensors are deployed in open environments, exposing them to the elements of weather for years. Some of these sensors are explicitly required to withstand harsh extreme environments such as extreme temperatures, vibration ratings, and dust and liquid resistance. Hence, durability of these sensors is of great concern.

Improvements in System on Chip (SOC) architectures Some key advancements happened in the area of SOC architectures specifically designed for IoT devices such as application processors (high end) (are usually based on technologies adapted from mobile phone/tablet architectures) microcontrollers (low end), and smart analogue.

Lower costs One trend that is driving greater adoption of IoT is the lowering of the cost of the sensors. It is estimated that the average cost of the sensors will drop to $0.38 by 2020, down by $0.92 as compared to 2004. This is helping to sense and acquire more data from a variety of environments and develop more data-driven intelligent applications than before.

1.2 IOT AS A DISRUPTIVE TECHNOLOGY

The term disruptive technology was first coined by Harvard professor Clayton Christensen, he later named it as disruptive innovation. The reason it is called as disruptive is due to its impact on an existing business model and the current system/society.

A disruptive technology (a hardware, software, networking, etc.) has the potential to replace an existing technology or a well working system that is already in place. From a product perspective, it could be something that begins small and steadily moves up the market and eventually becomes a threatening competitor to the existing products, and may eventually replace them.

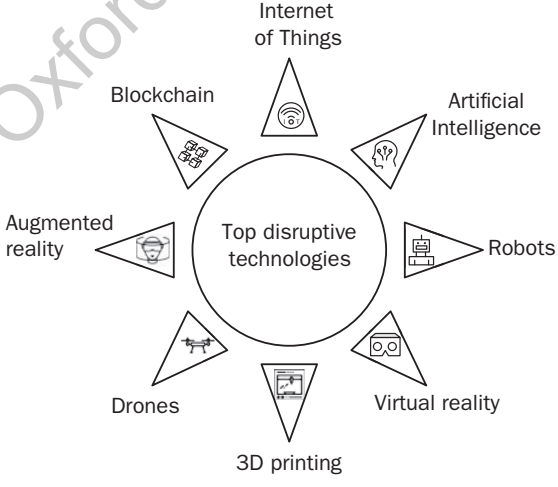


Fig. 1.7 Internet of Things (IoT) Along with Other Disruptive Technologies (Projection for the Year 2020)

Currently, IoT is considered as one of the top disruptive technology along with other technologies such as artificial intelligence, robotics, and virtual reality (see Fig. 1.7). Section 1.2.1 discusses some selected areas that IoT is already playing a crucial role and acting as disruptive technology.

1.2.1 Motivating Scenarios

1.2.1.1 Home and Personal Space

The personal space IoT centres on a person's space. It includes all objects implanted or wearable by the person such as implanted sensors, smartwatches, Google glasses, ECG sensors, and smartphones. It also includes all fixed or mobile objects and devices that come into contact (or reachable) with wearable objects on the person. Devices are reachable when they are within the wireless transmission radius of one another.

Smart buildings IBM is building a solution with the Watson IoT platform and IoT-enabled sensors for tracking every asset in the building using that information in their IoT platform. This will facilitate the owners of the building to understand, monitor, and control of installations such as Heating, Ventilation, Air Conditioning (HVAC) systems, to enable to monitor remotely. The burden of facility management is overtaken by smart sensors that capture every pulse of this infrastructure and to enable remote diagnostics and analysis.

Smart elevators KONE, the elevator company, is trying to understand how people are using the elevators. By using sensors, they are assessing how people move through buildings and estimating how much time can be reduced for the elevator wait. They conclude that even 2 or 3 minutes reduction in the waiting time will make a huge difference in moving people to their relevant floor.

1.2.1.2 Social

Food security In February 2018, a meeting at Rome was organized by the Food and Agriculture Organization (FAO) of the United Nations (UN). During that meeting Vicente Muñoz, Chief Internet of Things Officer, Telefónica said "The future of agriculture hinges on the adoption of technologies such as the Internet of Things (loT), Big Data and Artificial Intelligence". Further, FAO's director General José Graziano da Silva was of the opinion that the greatest challenges currently faced by humanity is in their fight against hunger, poverty, and effects of climate changes in agriculture, further he said:

"Access to reliable information, including that related to changing weather patterns, is essential to empower farmers, especially those who live in developing countries."

To address the above issues, investment and integration of new technologies such as IoT that will enable farmers to connect with real-time information (e.g., Agro-meteorological) about their farms and facilitate the use of simple and intuitive tools that are data driven to decrease uncertainty and mitigate risk. IoT's contribution is this sector is gaining wider acceptance. Several areas are currently getting transformed by the use of smart sensing systems for monitoring and management of various field tasks and parameters such as soil health, irrigation scheduling, nutrients, and early pest and disease prediction and warning.

Reducing food wastage A Chicago-based tech start-up, Ovie, developed a smart food storage system based on the IoT concept that will eliminate waste and change the way people eat, save, and shop for food. The system tracks the food items in the fridge and sends reminders to eat those before getting spoiled.

Water ATM Piramal Sarvajal, a mission-driven social enterprise, is committed to leveraging technology to bring community-level safe drinking water to the underserved. The organization has developed and implemented innovative market-based drinking water solutions in 16 states in India. Their infrastructure includes remotely monitored water purification units and solar powered, cloud connected water kiosks called water ATMs (see Box 1.4).

BOX 1.4: WATER ATM FOR DISPENSING SAFE DRINKING WATER

Peeth is a village in the heart of the Aravallis in Rajasthan. It is one of the most backward districts of the country and faces a serious water shortage. In Peeth, 84% of the population gets its drinking water from the local well, polluted with dangerously high levels of fluoride and other heavy minerals. Surveys showed that although the locals were aware of hazards of drinking polluted water, but the only alternative was a single private drinking water supplier, who charged ₹2 per litre and only catered to 40 families. Thus, the villagers welcomed the Sarvajal Kendra, as a much-needed solution. Today, the facility serves more than 200 families daily, ensuring they get safe water delivered at their doorstep.

Adapted from www.sarvajal.com; www.downtoearth.com; www.thehindu.com

1.2.1.3 Healthcare

Currently, IoT in Healthcare is being adopted in many areas. It can not only improve the existing healthcare systems, but also enable transformative ways (see Box 1.5) in which the patient gets treatment and care. It is estimated that the global IoT healthcare market to reach over USD 160 billion by 2020. The concept of 'Connected medical devices' is ushering new era in personal fitness and wellness area. Some of the use cases are:

- Remote diagnosis and follow up monitoring
- Memory disabilities monitoring
- Early intervention for detection of critical signs
- Monitoring patient fall
- Timely medicine alerts and enhanced drug management
- Healthcare assets monitoring and tracking

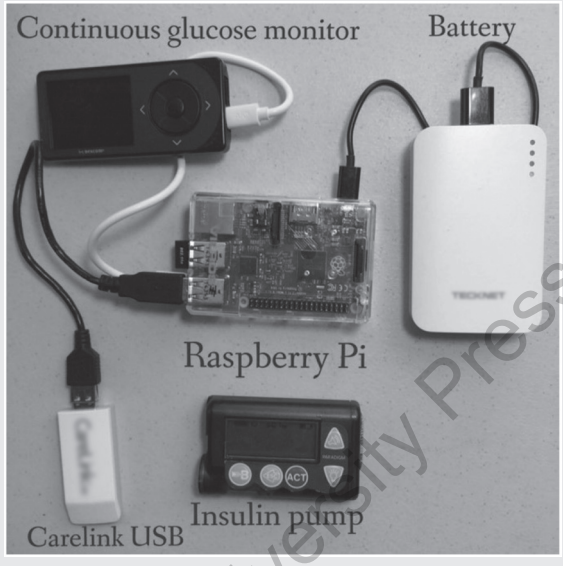
BOX 1.5: OPEN ARTIFICIAL PANCREAS SYSTEM DEVELOPMENT

Dana Lewis and her husband Scott Leibrand have hacked Dana's CGM (continuous glucose monitor) and her insulin pump. Using the data feed from the CGM and a Raspberry Pi computer, their own software completes the loop and continuously alters the amount of insulin Dana's pump delivers. Its success led to the unveiling of the open artificial pancreas system project. "The Open Artificial Pancreas System project (#OpenAPS) is an open and transparent effort to make safe and effective basic Artificial Pancreas System

(Contd)

Box 1.5 *(Contd)*

(APS) technology widely available to more quickly improve and save as many lives as possible and reduce the burden of Type 1 diabetes."



Adapted from www.diyps.org; www.healthline.com; www.itas.kit.edu; www.openaps.org

1.2.1.4 Environmental

Saving critical species The International Union for the Conservation of Nature (IUCN) maintains a database of the extinction risk of animal species called the IUCN red list. It reveals that the number of threatened species rose globally from roughly 10,000 in 2000 to over 25,000 in 2018. In the wake of such a revelation, it is necessary to take urgent action to protect these animals from extinction. Many organizations around the world are adopting IoT-based technologies to help identify, track, and protect them. The ruggedness of the terrain, remoteness, and real-time information gathering are some of the aspects of the problem that IoT is able to address. For example, in South Africa, IoT devices enabled collars are sending location and heart rate of Rhinos, which is helping the authorities to monitor them and immediately send rescue teams if they find the animal in distress.

Monitoring and reducing air pollution The effects of air pollution are causing serious problems worldwide. At the individual level, poor air quality is leading to several debilitating conditions in humans such as asthma, attacks, lung cancer, heart diseases, and chronic bronchitis. According to the American Association for the Advancement of Science (AAAS), it is the world's fourth reason for deaths. IoT-based air quality monitoring devices are highly capable of measuring various air quality parameters such as surface ozone, NO_2, SO_2, and particulate matter (PM2.5/PM10), and relay this information in real-time to the authorities to help track the zones of high pollution. Low power wide

area network (LPWAN) technologies such as LoRA are enabling the development of dense air quality monitoring networks due to its ability for long-range connectivity and low-power consumption. An urban sensing project called the 'Array of Things (AoT)' is being carried out in Chicago to collect real-time data on the city's environment for a more healthier, more efficient, and more livable city. The list of sensors includes environmental sensors, air quality sensors, and light and infrared sensors.

Improving water conservation Water conservation and management is essential in many facets of human lives. The various current practices are time consuming and lack real-time tracking and alerts for timely intervention to reduce wastage of water. Out of many applications of IoT in this area, two applications are described as follows:

- Smart water meters that can be used to detect leakage of pipes in the water delivery infrastructure (e.g., water grid). It also can help to precisely understand the water consumption behaviour of the users through data analytics and make and send alerts in real time. Further, by analysing the requirement of water in an area, adjustments to the optimal supply of water can be achieved.
- Water quality aspects can be studied by the deployment of IoT sensors in the water supply network to measure various water quality parameters to quickly react to those conditions when the water quality is deemed below the safe level.

For more compelling use cases, the reader is referred to Chapter 17.

1.2.2 Multidisciplinary Nature of IoT

IoT is driven not only by people who have specific background in Information and communication technologies (ICTs), but also by non-IT people who are showing significant interest in understanding the IoT ecosystem and contributing to its development using their own domain specific expertise. Institutions are increasingly feeling the need to have personnel particularly those who are involved in systems development to understand a host of disciplines to help them design complex IoT systems. Hence, multi-domain research and development teams are currently preferred in the development of IoT system. As shown in Fig. 1.8, there are a multitude of disciplines that are involved in IoT, each of them have their own set of requirements and goals. However, the domain expert in any of these areas, for example, a person with Transportation systems development, has to work with a person who knows about sensors and their deployment, and in turn need to work with an Information Technology (IT) person to help develop the software and integrate with the system. Similarly, doctors and electronics and communication technology engineers have to work hand in hand to develop new IoT devices for healthcare. In addition, social scientists are required to understand about the societal aspects of the developed technology. This line of thought can be extended to many sectors such as defence, environmental monitoring, energy, and industries, who are currently building transformative IoT solutions Therefore, it can be seen that for any of the technology that is being developed in IoT, there are multidisciplinary teams (members with varied but complimentary experience) involved to make the idea take shape and finally come out with tangible product.

Fig. 1.8 Interdisciplinary Nature of IoT Encompasses a Variety of Domains

1.2.3 Challenges Involved in Its Further Evolution

The main challenges involved in the further evolution of IoT are as follows:

1.2.3.1 Technological Challenges

The technological challenges that could impede the future evolution of IoT include the following:

IoT system design considerations Currently, there are a variety of protocols (network, communication, data protocols, etc.) that are being used by various organizations/entities to design, develop and implement IoT systems in diverse domains. This is leading to non-interoperable systems, whose integration and access is becoming very challenging. Unless, standards are implemented in every step of the IoT systems development process, there will be many systems that could become unusable and obsolete. For example, users will end up with an IoT system (e.g., home automation), which will become highly vendor dependant and is no longer able to integrate with other systems implemented by a different vendor.

Maturity and integration with existing technology Currently, most of the IoT technologies have not reached a matured phase where they are guaranteed to continue to grow in a particular direction. Hence, an IoT solution provided using a particular technology may soon be abandoned and a new technology used for the same functionality. Therefore, products that the user is using may no longer be useful, since the technology is no longer supported by the vendor. Integration with existing technologies and overhead due to constant requirement for upgradation of existing the hardware infrastructure is another barrier that needs to be crossed for greater adoption of IoT.

Standard operating procedures (SOPs) The lack of well understood and standard operating procedures for IoT devices maintenance, response, and incident management are aspects that need to be strengthened to streamline the processes involved in the IoT systems. Since, it is a rapidly evolving cluster of technologies, the best practices are scattered and few. Hence, there is a need to document and guide developers on the best approaches.

Security The security aspects of IoT are a major concern to its widespread proliferation in the future. It is considered as crucial barrier for widespread acceptance of IoT. Malicious attacks and hacking of IoT devices (e.g., baby monitors, smart fridges, thermostats, health and medical machines, cameras, etc.) can pose significant security nightmare. The main challenges include (ACE-OAuth, 2018):

(i) Authentication and authorization for secure communication Authentication allows establishing the identity of an entity. Whereas authorization determines whether an entity (a device or a user) has access rights to resources and to what extent (i.e., level of permissions, e.g., read/write). In the case of IoT, authentication enables to establish the identity of various IoT devices deployed in a shared environment, hence maintain the integrity of the IoT device and data. Trust is the backbone for ascertaining the identity of an entity. In computer-networked environments, passwords are the most common way of authentication of human users. However, in a machine-to-machine interaction, cryptography-based authentication and authorization mechanisms are useful, where cryptographic keys are commonly used. A digital certificate issued and digitally signed by a certificate authority (CA) contains a public key and identity of the owner. The IoT devices can use these digital certificates for authentication and create the required Trust for all parties in the network. However, such CAs are non-existent at present for the IoT domains. Hence, efficient ways to deploy the keys and manage them is an ongoing effort. Further, current security protocols and cryptography approaches require good amount of memory space, which is difficult to implement on low-powered IoT devices. Therefore, the challenge is to develop approaches for deploying and managing the keys that can adapt without causing additional overheard on the IoT node (Yang, et al., 2016). In addition, the authorization and access control should be customized based on the type of the IoT Node (Li, et al., 2017). Recently, IETF proposed the authentication and authorization in constrained environments (ACE-OAuth) framework for IoT devices. It is based on OAuth 2.0 (OAuth is a widely used open standard for delegation) and Constrained Open access Protocol (CoAP).

(ii) Privacy IoT devices that collect sensitive user's data are posing an immense threat to an individual's privacy. For example, data gathered by sensors related to health, home appliances usage, tracking devices for phones, work habits, etc. could be transmitted to a cloud service or a third party

without the user being aware of it. Existing privacy approaches are user-centric, that is, it is based on individual's preference to the content and quantum of data that he/she deems to be sharable and what remains private. The data-collection entities are obligated to inform the users about the intended usage of the acquired information. However, in the case of IoT nodes that are collecting private information, there is a threat to privacy at (i) endpoints where each IoT node emits the data, and (ii) data obtained from networked IoT nodes, which are collected, combined, and analysed to reveal a pattern and thus giving out more sensitive information. In addition to data privacy issues, IoT device deployment at sensitive areas and across socio-cultural borders requires a new way to understand the implications of privacy invasion.

1.2.3.2 Connectivity

Huge challenges need to be overcome for ensuring connectivity of billions of devices in IoT. Many technologies are available for enabling connectivity in IoT such as those in the unlicensed spectrum, low-power wide area networks (LPWAN), cellular, and satellite-based technologies. These are at various stages of maturity and continuously evolving in terms of the core technologies and applications to IoT. The future of these connectivity solutions depend on the adaptability to the vast array of diverse IoT devices and applications, as the requirements vary in terms of data capture rate, data transmission rate, latency, storage, etc. Hence, connectivity needs are based on the device and its particular characteristics. Therefore, no single technology will be able to cater to all the needs of the IoT systems. Integration and interoperability of various connectivity solutions will be a key factor for seamlessly switching between various IoT devices implementing varied connectivity technologies.

1.2.3.3 Societal Drivers

Issues of privacy and trust are going to be the main drivers for the wide acceptance of IoT. There is a need for various institutions (public and private) to implement mutually agreed and standardized privacy procedures into their systems and the core IoT system architecture is built on the foundations of privacy, trust, and data protection. For example, an IoT device could capture the location of the user to give location-based services, but does not use that data for any other purpose, such as tracking the individual. Similarly, the data captured by the device may send only the summary and does not transmit the original raw data, or the data lives only for a short period or anonymised so that it cannot be identified with any particular user. Such kind of approaches will make the user to feel protected when using privacy friendly IoT applications. Currently, such things are not fully implemented in the IoT ecosystem. The current focus is more on giving better functionality and user experience rather than focusing on implementing the principle of *Privacy by Design.* According to it, starting from the fundamental building blocks in the IoT system development, privacy is given utmost importance and embedded in each and every process of the system development. Such systems are robust and have better chances of gaining the trust of the consumer.

1.2.3.4 Uncertain Returns on Investment

The investment in IoT according to the market reports is very high (see Box 1.3). However, businesses are struggling to understand and make an estimate of the return on investment (ROI) due to the emerging nature of the IoT technology and lack of historical data or business cases (World Economic Forum report, 2015) that could be used as a benchmark or point of reference to estimate the ROI.

1.3 STANDARDIZATION

The massive scale of IoT comprises billions of devices and subsystems. To be able to interconnect them and derive meaningful information requires that these heterogeneous systems need to be interoperable, that is, the ability to work with any underlying protocols, data models, and content types. Since, there are many public and private stakeholders involved in IoT, there will be many proprietary and open solutions in various domains with each solution providing its own IoT infrastructure, devices, APIs, and data formats due to which it becomes challenging to integrate them. To achieve interoperability and enable scaling up of IoT, standards are required.

1.3.1 Need for Standardization at Various Layers of IoT

As IoT is a multi-layered system comprising of various layers related to sensing, networking, communication, session, etc., standardization is required at each of these layers (the architecture reference model of IoT is explained in Chapter 14). Considering this need, several standards have been proposed with a focus on specific requirement in the development of an IoT system. For example, the data link layer connects two things or thing and gateway device that connects a group of things to the Internet. Various short-, medium-, and long-range protocols have been developed for connectivity (see Figs 1.6 and 1.9). Specialized routing protocols were developed to enable several IoT devices to communicate and aggregate information and then send it on to the Internet. Further, in the network layer, among other protocols such as UDP, 6TiSCH, and THREAD, the 6LoWPAN is developed for power constrained devices, standardizes a way to carry packet data in the form of IPv6 over IEEE 802.15.4. The messaging among various components of the communication subsystem is addressed in the session layer. Among them, the Constrained open Access protocol (CoAP) was developed by IETF Constrained RESTful Environments Working Group (CoRE). It works on UDP or UDP analogue. The Message Queuing Telemetry Transport (MQTT) originally developed by IBM works on the TCP/IP. More details on the IoT standards and protocols are discussed in Chapter 4.

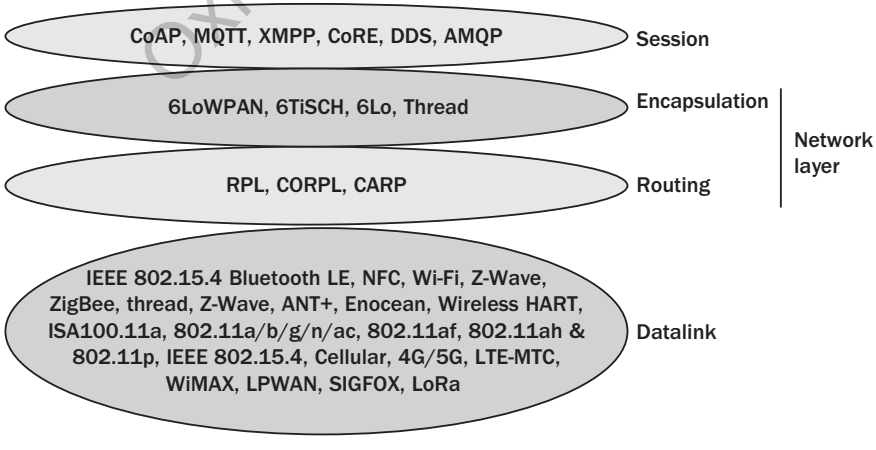


Fig. 1.9 Variety of Standard Protocols Currently Available for IoT

1.3.2 Organizations and Their Efforts for Standardization

Various organizations are involved in the IoT standardization efforts. Following are some key institutions and their contributions:

Institute of Electrical and Electronics Engineers (IEEE) IEEE is a global, professional engineering organization whose mission is to foster technological innovation and excellence for the benefit of humanity. The standards body of IEEE called the IEEE standards association is involved in developing standards, specifications, and best practices for IoT. The IEEE P2413 defines an architectural framework for the IoT, including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains.

ETSI (European Telecommunications Standards Institute) ETSI develops standards for information and communications technologies (ICT), including fixed, mobile, radio, converged, broadcast, and Internet technologies. In the IoT space, it works with ONE M2M (another standards body) to provide standardized M2M interfaces. The goal is to enable IoT devices to connect seamlessly and to ensure that they are network agnostic. From an M2M standpoint, various M2M technologies are supported by ETSI such as smart appliances, smart metering, smart cities, smart grids, e-health, and intelligent transportation systems. Further, specific to IoT, ETSI is working in the areas of: security for the IoT, low power supplies in the IoT, radio spectrum requirements, and embedded communications modules.

OneM2M It is a Global standards initiative for M2M and IoT. It has over 200 member organizations. It works in a partnership mode with various standards organizations and provides a detailed standard for M2M/IoT in the areas of architecture, interfaces, security, communication protocols, etc. The oneM2M-layered model consists of network layer, common services layer, and the applications layer. The goal is to have applications to share common infrastructure, environments, and network elements to enable interoperability. The common services layer can be readily embedded within various hardware and software and provides functions that M2M applications across different domains commonly need (e.g., data transport, management, discovery and policy enforcement, security/encryption, etc.). The Representational State Transfer (REST)-based architecture of oneM2M allows the use of multiple protocols such as HTTP, CoAP, MQTT, or WebSocket to work with oneM2M application servers worldwide.

Internet Engineering Task Force (IETF) It is an open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. Its mission is to "make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet." Within IETF, specific IoT-based focus is towards:

6LoWPAN 6LoWPAN is IPv6 adaptation layer and header compression mechanism that is suitable for low power constrained IoT devices and networks.

Routing Over Low power and Lossy networks (ROLL) ROLL establishes routing protocols for constrained-node networks.

Constrained RESTful Environments (CoRE) CORE extends the Web architecture to most constrained networks and embedded devices.

International Telecommunications Union (ITU) It released the ITU report on The Internet of Things in 2005, which describes the various visions of IoT, and terms IoT as an 'ubiquitous network'. It published recommendations in the areas of tag-based identification services, ubiquitous sensor networks (USN), and ubiquitous applications in next-generation networks. Specifically for IoT, this organization contributed towards IoT terminology, common requirements and capabilities, APIs and protocols for IoT, IoT testing, network, security, and privacy protection aspects of IoT. Further, various focus groups were formed for several application areas such as e-health, smart grids, home networks, smart sustainable cities, and smart water management.

Object Management Group (OMG) It developed the Data Distribution Service (DDS) for IoT. It is a middleware protocol and API standard for data-centric connectivity. It is pub/sub standard, which enables scalable, real-time, reliable, high performance, and interoperable data exchanges between publishers and subscribers. In a data-centric system, the focus is on user-defined data (the data model). The middleware understands the context of the data and ensures that all interested subscribers have a correct and consistent view of the data.

OASIS It is a standards body that is responsible for providing a lightweight publish/subscribe reliable messaging transport protocol suitable for communication in M2M/IoT contexts where a small code footprint is required and/or network bandwidth is at a premium.

1.3.3 Factors for Widespread Adoption of IoT

IoT-based technologies are driving a wide range of application areas that have stagnated and lacking much innovation in the preceding years of IoT. It has already permeated in various walks of life. The various factors that led to the widespread adoption are mainly due to the technological advancements and economic viability in the areas of the following.

1.3.3.1 Technology Viewpoint

Communication and network Connectivity is one of the key pillars of IoT. There are a host of technologies that are being developed (some of them have already reached mature levels) and in multiple ranges (short, medium range) which are enabling the IoT revolution gain widespread acceptance. Customized versions of Internet protocols for low-powered devices such as the 6LoWPAN, which is based on the IPV6 Competing wireless technologies such Cellular (4G/5G) and LPWAN (e.g., LoRA) technologies are giving the IoT system developers options to develop IoT networks that can be deployed in remote challenging areas. More details are presented in Chapter 4.

Computing A computing revolution has happened in the last decade, with new paradigms of computing emerging such as the cloud computing. It has completely changed the way in which data is stored, processed, analysed, and disseminated. The low-cost nature and always available kind of computing resources is an attractive alternative to the user as compared to in-house computing infrastructure.

The IoT has considerably gained by cloud-based infrastructure, since there is a need to process data from a very high number of sensors, which requires considerable computing power. Organizations and individuals working in deploying IoT-based solutions can now subscribe to a cloud-provider for a considerably low rate and quickly deploy the IoT solutions. Various cloud providers (e.g., Amazon Web Services (AWS) IoT, IBM Watson IoT, etc.) are providing off the shelf IoT platforms to enable end-to-end management of the IoT resources. Further, the emergence of 'Data Science' area has ushered in new ways for analytics, both at the edge of the IoT network through streaming data processing analytics and also batch-processing/offline approaches that includes machine learning-based techniques.

Low-cost devices Sensors and their integration with IoT is becoming affordable. Due to it, an ever-increasing number of domains are able to use IoT sensors to drive their processes; these solutions are contributing towards developing automation in several sectors.

1.3.3.2 Consumer Viewpoint

From a consumer perspective, usefulness, price, connectivity, security, and privacy are the main enablers for high adoption of IoT products. The IoT products such as wearables in the fitness and wellness area have already showed high promise due to the practical use and affordable pricing. As the consumers get more educated in the value that IoT products bring to their daily lives, greater will be the adoption. Companies have already embarked on targeted campaigns to create consumer awareness and change their perception of this new technology.

REVIEW QUESTIONS

1. Describe the historical context that led to the emergence of IoT.
2. Describe various Auto-ID technologies.
3. What is the vision of IoT? Explain the different perspectives from which IoT's vision can be understood.
4. Various organizations have defined IoT. Describe in what aspects these are similar (if any). What components or parts of these definitions are similar?
5. Give your own definition of IoT. How is it different from other definitions?
6. What is an enabling technology? Describe the key enabling technologies of IoT.
7. Explain the evolution of a disruptive technology.
8. Why is IoT considered as a disruptive technology?
9. Give some motivating scenarios where IoT has been a disruptive technology.
10. What is the need for IoT standardization?
11. Give an overview of IoT Standards and mention the organizations that are involved in IoT Standardization and their specific roles.
12. What is leading to the widespread adoption of IoT?

REFERENCES

1. ACE-OAUTH [ONLINE]. Available at: https://tools.ietf.org/pdf/draft-ietf-ace-oauth-authz-13.pdf [Accessed 2/10/2018]
2. Array of Things [ONLINE]. Available at: https://arrayofthings.github.io/ [Accessed 2 Oct 2018]

3. Blowers, M., Iribarne, J., Colbert, E., Kott, A. (2016). The future Internet of Things and security of its control systems. arXiv preprint arXiv:1610.01953.
4. Buckman, A. H., Mayfield, M., Beck, S. B. M. (2014), What is a Smart Building? *Smart and Sustainable Built Environment*, 3(2): 92–109.
5. Christensen, C. (2013), The innovator's dilemma: when new technologies cause great firms to fail. Harvard Business Review Press.
6. Coke Machine, The Only Coke Machine on the Internet, Carnegie Mellon University, School of Computer Science [ONLINE]. Available at: https://www.cs.cmu.edu/~coke/history_long.txt [Accessed 2/10/2018]
7. Cook, D. J., Das, S. K. (2007), How smart are our environments? An updated look at the state of the art, *Pervasive and Mobile Computing*, 3(2): 53–73.
8. Gartner. (2018), Gartner worldwide IT spending forecast for 2018, 2018. Available at: https://www.gartner.com/newsroom/id/3845563 [Accessed 2/10/2018]
9. IIC: Industrial Internet Consortium. Available at: https://www.iiconsortium.org/
10. IEEE. (2015), Towards a definition of Internet of Things. Available at: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf [Accessed 2/10/2018]
11. IoT-A, Internet of Things – Architecture IoT-A Deliverable D1.5 – Final architectural reference model for the IoT v3.0.
12. ITU, International Telecom Union (ITU) [ONLINE]. Available at: https://www.itu.int/en/Pages/default.aspx [Accessed 2/10/2018]
13. IETF [ONLINE]. Available at: https://www.ietfjournal.org/internet-of-things-standards-and-guidance-from-the-ietf/ [Accessed 2/10/2018]
14. IIC (2018) [ONLINE]. Available at: https://www.iiconsortium.org/index.htm [Accessed 2/10/2018]
15. Kim, H. Lee, E. A. (2017), Authentication and authorization for the Internet of Things, *IT Professional*, 19(5): 27–33.
16. Li, F., Hong, J., Omala, A. A. (2017), Efficient certificateless access control for industrial Internet of Things, *Future Gener Comput Syst*.
17. Ma, H. D. (2011), Internet of things: objectives and scientific challenge, *Journal of Computer Science and Technology*, 26 (6): 919–924.
18. McGlinn, K., O'Neill, E., Gibney, A., O'Sullivan, D., Lewis, D. (2010), SimCon: a tool to support rapid evaluation of smart building application design using context simulation and virtual reality, *Journal of Universal Computer Science*, 16(15): 1992–2018.
19. McKinsey. (2015), The Internet of Things: mapping the value beyond the hype, June, 2015.
20. Montori, F., Bedogni, L., Felice, M.D., Bononi, L. (2018), Machine-to-machine wireless communication technologies for the Internet of Things: taxonomy, comparison and open issues, *Pervasive and Mobile Computing*, 50: 56–81.
21. Mauro, C., Ali, D., Franke, K., Watson, S. (2018), Internet of Things security and forensics: challenges and opportunities, *Future Generation Computer Systems*, 78: 544–546.
22. Nguyen, H. H, Mirza, F, Asif N. M., Nguyen, M. (21017). A review on IoT healthcare monitoring applications and a vision for transforming sensor data into real-time clinical feedback. *2017 IEEE 21st International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Wellington, pp. 257–262.
23. NIST. (2018) [ONLINE]. Available at: https://www.nist.gov/ [Accessed 2/10/2018]
24. OASIS [ONLINE]. Available at: https://www.oasis-open.org/orgf [Accessed 2/10/2018]
25. Pontin J. (2005). ETC: Bill Joy's Six Webs. *MIT Technology Review* [Retrieved 17/11/2013]
26. Roberti, M. (2005), The History of RFID Technology - RFID Journal [ONLINE]. Available at: http://www.rfidjournal.com/articles/view?1338. [Accessed 2/10/2018]

27. Texas Instruments [ONLINE]. Available at: http://www.ti.com/lit/ml/swrb028/swrb028.pdf [Accessed 2/10/2018]
28. Traversat, B., Abdelaziz, M., Doolin, D., Duigou, M., Hugly, J-C., Pouyoul, E. (2003), Project JXTA-C: enabling a Web of Things. *HICSS*, 2003: 282.
29. The Societal Impact of the Internet of Things [ONLINE]. Available at: https://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf [Accessed 2/10/2018]
30. World Economic Forum (2015). Industrial Internet of Things: unleashing the potential of connected products and services, 2015 [ONLINE]. Available at: http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_ Report2015.pdf [Accessed 2/10/2018]
31. Weiser, M. (1991), The Computer of the 21st Century, *Scientific American*, 265: 94–104.
32. Yang, Y., Cai, H., Wei, Z., Lu, H., Choo, K.-K. R. (2016), *Towards Lightweight Anonymous Entity Authentication for IoT Applications*, Springer, Cham, pp. 265–280.
33. Yu, T., Sekar, V., Seshan, S., Agarwal, Y., Xu, C. (2015), Handling a trillion (unfixable) flaws on a billion devices: rethinking network security for the internet-of-things, *Proceedings of the 14th ACM workshop on hot topics in networks*, ACM, p. 5.