Internet of Things (IoT) A Quick Start Guide

A to Z of IoT Essentials

Chitra Lele

www.bpbonline.com

FIRST EDITION 2022

Copyright © BPB Publications, India

ISBN: 978-93-89845-860

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Distributors:

BPB PUBLICATIONS
20, Ansari Road, Darya Ganj
New Delhi-110002
Ph: 23254990/23254991

MICRO MEDIA
Shop No. 5, Mahendra Chambers,
150 DN Rd. Next to Capital Cinema,
V.T. (C.S.T.) Station, MUMBAI-400 001
Ph: 22078296/22078297

DECCAN AGENCIES
4-3-329, Bank Street,
Hyderabad-500195
Ph: 24756967/24756400

BPB BOOK CENTRE
376 Old Lajpat Rai Market,
Delhi-110006
Ph: 23861747

Published by Manish Jain for BPB Publications, 20 Ansari Road, Darya Ganj,
New Delhi-110002 and Printed by him at Repro India Ltd, Mumbai

www.bpbonline.com

Foreword

I am extremely delighted and honoured to write the foreword for the young software engineer and academic author Chitra Lele's latest book—*Internet of Things (IoT) A Quick Start Guide.*

The Internet of Things (IoT), the convergence of the digital and physical worlds, has emerged as one of the fundamental digital trends today. While it took from the dawn of civilization to 2003 to create 5 exabytes of data, we now create the same volume of data in less than 2 days. In this regard, IoT is a big enabler of data origination and economic value creation. IoT today is an integral part of many technology-enabled solutions from fitness trackers to health care equipment to asset management platforms to smart homes and cities.

Basically, IoT is now embedded into the lives and the operations of consumers, enterprises, and governments. At the same time, IoT solutions will continue to grow in the coming years making profound impact all around. In 2021, the number of IoT devices was about 20 billion and by 2030, the number of IoT devices is expected to jump to 125 billion. McKinsey Global Institute predicts that the economic impact of IoT will be between $4 trillion and $11 trillion by 2025.

Overall, the technology landscape is increasingly moving towards ecosystems—a set of wireless and interdependent entities that work together to provide holistic and integrated products and services. Hence for IoT technologies to work together, one should have a solid understanding of not only the devices such as sensors and actuators, but also have a good knowledge of the complete ecosystem including software/interface, network, cloud, protocols, analytics, solution providers, privacy, and security.

In this backdrop, this book provides a holistic and a practical approach for an integrated, scalable, and holistic IoT ecosystem. This book is broken down into 6 logical chapters that are easy to read and digest. *Chapter 1* provides an excellent overview of IoT, while *chapter 2* (architecture), *chapter 3* (data management) and *chapter 4* (security, privacy, and interoperability) provide deep technical details. The book rounds off well with *chapter 5* (novel use cases) and *chapter 6* (future trends). Overall, this book provides valuable insights and strategies to integrate new experiences across diverse devices, software, data and platforms in the IoT ecosystem.

Chitra's book is an earnest attempt to bridge the gaps in knowledge and to help the readers understand the deeper dynamics of IoT. The book believes in the concept of teach by example. All the tools needed to facilitate quick understanding of complex concepts are provided in this book.

Today, IoT provides consumers, businesses, and governments with new opportunities to innovate products and services and to enhance performance and create value. The future is connected and connectivity brings timely and controlled access to the data and insights thereby enabling the creation of improved processes, products, and business models. I strongly believe this book will help readers in designing, building, and operating holistic IoT solutions in a responsible and ethical manner. Great work Chitra and thank you very much for giving me an opportunity to write the foreword on such a wonderful topic! All the best!

— **Prashanth Southekal**
PhD, MBA, MS

Managing Principal at DBP Institute,
Professor at IE Business School,
Digital Transformation Strategist and
Best-Selling Author, Calgary, Alberta, Canada

Dedicated to

My Parents:
Asha Lele** and **G. G. Lele

*"Through thick and thin you are always by
my side. You both are the essence of
my life and spirit—My true pride."*

About the Author

Chitra Lele is a young software engineer, software solution architect, record-setting author, award-winning poet, and research scholar. She is a merit-holder and holds degrees in Software Engineering and Computer Management. She runs her software startup firm, Chitra Lele & Associates, which designs software solutions based on Ethically-Aligned Design principles. She is also the founder of 'Chitra Cares', a social transformation initiative dedicated to community building projects. Through her software projects, peace work, academic books, and social transformation initiatives, she strives to contribute to the greater good of the world.

Chitra has received more than 30 awards in the fields of Literature, Technology, Peace and Education. She has received more than 70 letters of commendation from world leaders and world organizations for her endless efforts in academic literature and peace promotion.

Chitra has regularly contributed scholarly articles, peace poems and research papers to reputed magazines, newspapers and journals worldwide. She is also an ardent creative artist.

Chitra's fields of software engineering, peace promotion and academic writing all are intertwined, and all these fields are very close to her heart. They complete the equation of her life and are an integral part of her DNA.

About the Reviewer

Dr. Ruchi Doshi is having more than 15 years of academic, research and software development experience in Asia, Europe and Africa. Currently she is working as a Research Professor at the Azteca University, Mexico and Adjunct Professor at the Jyoti Vidyapeeth Women's University, Jaipur, Rajasthan, India. She worked in the BlueCrest University College, Liberia, West Africa; BlueCrest University College, Ghana, Africa; Amity University, Rajasthan, India; Trimax IT Infrastructure & Services, Udaipur, India.

She is interested in the field of Machine Learning and Cloud computing framework development. She has published 20 research papers in peer-reviewed international journals and conferences; 3 Indian Patents; 3 books on Cloud Computing, Machine Learning, Mobile Cloud computing, Intelligent IoT Systems for Big Data Analysis and Mobile application development. She is Reviewer, Advisor, Ambassador and Editorial board member of various reputed International Journals and Conferences with IEEE, Springer and Elsevier. She is an active member in organizing many international seminars, workshops and conferences. She is nominated from the IEEE Headquarter, USA for the Chair, Women in Engineering (WIE) position in Liberia, West Africa.

– Dr. Ruchi Doshi
PhD, IEEE Senior Member

Founder Chair, IEEE Women in Engineering (WIE)
Liberia Research Professor,
Department of CSE Universidad Azteca, Mexico

Acknowledgements

I use this opportunity to express my heartfelt thanks to all those who supported me in one way or the other during the completion of my book project.

Special thanks to my exceptional Publishers, the BPB Publications team, for the valuable support provided throughout the entire process. The ceaseless cooperation by the team is greatly acknowledged.

What I have learned over the years comes as a result of being a daughter of wonderful parents, Asha Lele and G. G. Lele. They have been the motivation that has helped me to maintain laser-sharp focus on my goals. Thanks to them for their superb support and endless encouragement.

I owe my deepest gratitude to Prashanth Southekal Sir for writing the scholarly Foreword for my book. I tender my heartfelt thanks to Prashanth Sir for evincing keen interest in my book.

I offer my deep gratitude to the divine essence within me for bestowing on me the strength to follow my heart.

I owe my sincere gratitude to my company colleagues and my higher studies batch-mates who gave me the time and space to complete this book. Their ceaseless cooperation in adjusting to my software project work schedule, higher studies timetable and book writing schedule helped me to maintain balance between all these aspects.

Very special thanks must go to you all, my readers, for investing your time in reading this book.

Last but not least, I beg forgiveness of all those who have been with me over the course of my journey and whose names I have failed to mention. Your support and encouragement is deeply appreciated.

Preface

My book ‘Internet of Things (IoT) A Quick Start Guide' is a practical guide that demystifies the how, who, what, when, where, why, and what next dynamics of our increasingly “smart” and “connected” world driven by Internet of Things (IoT).

The IoT wave is heading for each and every domain. One can either meet it head on and surf high on this wave of transformation or one can turn one’s back and drown in it. The book begins with sharing specifics of IoT building blocks in terms of history, features, core concepts, software and hardware components, architectures, networks and protocols. It deals in depth with the perquisites, practices and procedures, and business potential generated by data from IoT devices. It deals with IoT security, interoperability and privacy issues, and how they are related to various aspects like trust levels, risk profiles, usability expectations, and so on. It focuses on applications, both major and minor, and also discuses novel use cases in various industries. Finally, it explains the current and future trends of IoT along with research findings and statistics.

The book is essential to enable all stakeholders to understand the importance of riding the wave of IoT in a responsible and successful manner. With the latest IoT technologies moving to their next stage of advancement, IoT will become more intuitive and convenient to use. This book offers practical guidance on how you can join the effort to build the wonder web of IoT that is as secure, safe, efficient and effective as possible.

My book believes in the concept of teach by example. All the tools needed to facilitate quick understanding of complex concepts are provided in this book:

1. Definition of key terms
2. Industry studies, research statistics
3. Spotlight sections

4. Questions for reflection
5. And much more

Through the 6 chapters in this book, you will learn the following aspects:

Chapter 1 introduces the history, features and core concepts of IoT. It then deals with the advantages and disadvantages of IoT. It also focuses on the main IoT processes right from data collection to analysis. The last subsection deals with software and hardware components.

Chapter 2 discusses IoT framework essentials and various frameworks. It also shares information on the various IoT networks and communication protocols. The last subsection deals with challenges and solutions.

Chapter 3 focuses on the perquisites, practices and procedures of IoT. It also explains the business potential generated by data from IoT devices and the various IoT solutions like Microsoft Azure and Amazon Web Services. Finally, it discusses the supporting components of IoT in terms of Metadata, Edge Computing and more.

Chapter 4 deals with security, privacy and interoperability dynamics and importance of security, privacy and interoperability measures. It then discusses in depth the various methods, tools and measures for improving security, privacy and interoperability. Finally, it focuses on the future direction of security, privacy and interoperability dynamics.

Chapter 5 explains in depth the main application areas and novel use cases of IoT, and also the various research findings and statistics related to them.

Chapter 6 helps to understand the main current trends of IoT and identify various trends that are going to rule the future horizon of IoT. It also shares more information on these aspects through research findings and statistics.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

https://rebrand.ly/811c36

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Table of Contents

Chapter 1
IoT: The Basic Dynamics

There are more connected devices in the world today than humans. The **Internet of Things** (**IoT**: we will be using this acronym from now onwards) through embedded devices facilitates seamless communication between people, processes, and devices; it involves adding digital sensors to every analog device in the physical world. IoT is a giant network of connected "*things*", which implies relationships between things-to-things, things-to-people and people-to-people. The Internet currently connects **people to people** (**P2P**), and this is Internet phase 1.

The next phase of the Internet is where IoT comes into play and will connect everyday devices to each other (M2M) and people to everyday devices (M2P). And this is what Cisco (it is an American multinational technology conglomerate) refers to as the Internet of Everything as it encompasses data, devices, people, and processes. IoT is making it fairly easy to directly integrate the real world into a computer-meditated reality. According to Gartner, 1 million IoT devices are going to be purchased and installed each hour in 2021.

According to Webopedia (it is an online dictionary and Internet search engine for information technology and computing definitions): "*The*

Internet of Things refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems."

The definition given by Investopedia (it is a group of editors, writers, product experts, developers, data scientists, analysts, and executives who are dedicated to financial education and empowerment) states: *"The Internet of Things (IoT) refers to a network comprised of physical objects capable of gathering and sharing electronic information. The Internet of Things includes a wide variety of "smart" devices, from industrial machines that transmit data about the production process to sensors that track information about the human body."*

Wikipedia (it is a multilingual online encyclopedia) defines IoT as: *"The internet of things (IoT) is the network of physical devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data."*

In common parlance: IoT means taking all the things in the world and connecting them to the Internet. IoT refers to the digital universe where it is about connecting any device to the Internet and to other connected devices, right from smart home devices to self-driving cars. This connectivity allows these devices to be online all the time to share data between them.

Spotlight

The investment in the IoT was approximately 157 billion US dollars in 2016. It is expected to reach 457 billion US dollars by the end of 2020. According to International Data Corporation (IDC is a market research company), IoT devices are expected to create over 90 zettabytes of data in 2025.

Structure

This chapter will cover the following topics:

- History, features and core concepts of IoT
- Advantages and disadvantages of IoT
- IoT processes
- IoT software and hardware

Objective

After studying this chapter, you will be able to:

- Understand the history and core concepts of IoT
- Identify the advantages and disadvantages of IoT
- Understand what are the various processes involved in IoT
- Identify the various software and hardware components of IoT setups

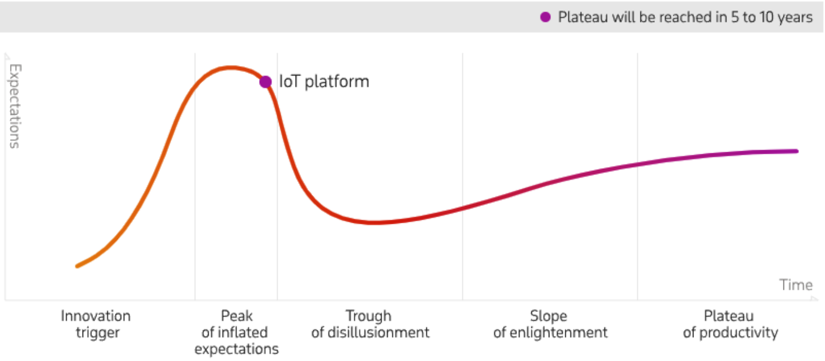
1.1 History of IoT—from toasters to cars

In the year 1970, the initial idea of connected devices was proposed; back then, it was called **pervasive computing** or **embedded Internet**. Thereafter, in the year 1990, *John Romkey,* along with his friend *Simon Hackett*, created the *Sunbeam Deluxe Automatic Radiant Control Smart Toaster* that could be turned on and off through the Internet; this was the first-ever smart IoT device. One year later, *University of Cambridge* scientists came up with the idea to use the first Web camera prototype to monitor the amount of coffee available in their computer laboratory's coffee pot.

In 1982, computer science students at the *Carnegie Melon University* had connected a Coca Cola vending machine to the Internet. They coded an application that would check the availability and temperature of the drink. They integrated micro switches into the system and used an early form of the Internet to check if the cooling device was keeping the drinks cold enough and if there were available cans.

In the year 1995, Siemens introduced the first cellular module built for M2M. In the year 1999, the actual term "*Internet of Things*" was used by *Kevin Ashton* during his work at Proctor & Gamble, and thereafter, it was officially recognized as a technology. *Kevin Ashton* opined **Radio Frequency Identification** (**RFID**) was a prerequisite for the Internet of Things. He concluded if all devices were "*tagged,*" computers could manage, track, and inventory them. The IoT concept was coined by a member of the radio frequency identification development community in the year 1999. Even though this term grabbed the interest of some P&G executives, the term Internet of Things did not get widespread attention for the next decade or so.

Later on, IoT was popularized through the famous press like the *Boston Globe*, the Guardian, and so on. In the year 2005, The *United Nation's International Telecommunications Union* published its first report on IoT. Three years later, IoT was born on a worldwide scale. During the period 2006–2008, IoT was recognized by the European Union, and the First European IoT conference was held. In 2008, a group of companies launched the IPSO alliance to promote the use of Internet Protocol in networks of "*smart objects*" and to enable the Internet of Things. The Internet of Things was originally thought of as extending the principles of the Internet as a network organization concept to physical things. In 2011, Gartner invented the famous "*hype-cycle for emerging technologies*" (refer to *figure 1.1*), including a new emerging phenomenon on their list: "*The Internet of Things*."

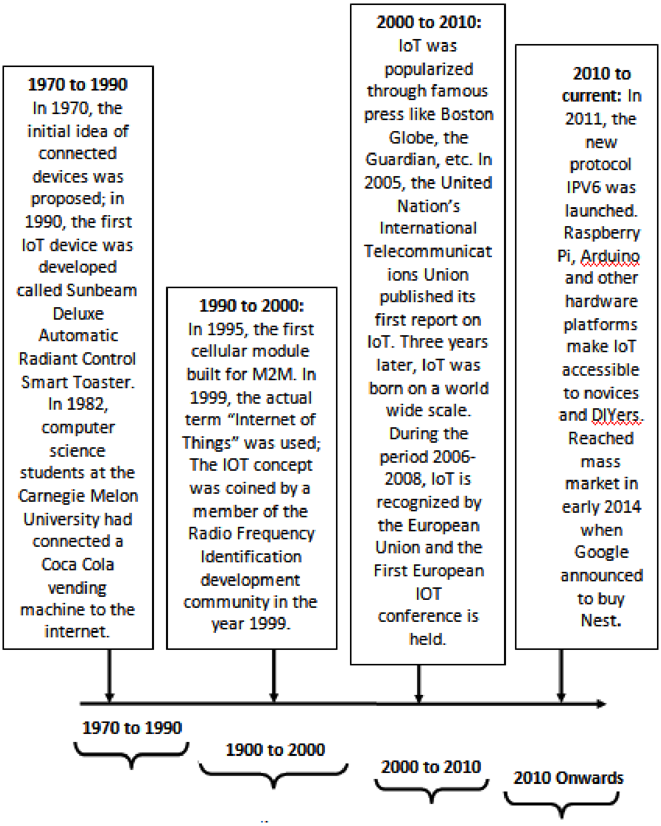


Data source: Gartner—5 trends emerge in the Gartner Hype Cycle for emerging technologies

***Figure 1.1**: Gartner hype cycle for emerging technologies*

In the book "*Emerging Technologies for Learning*," *David Becta* defines ubiquitous computing as "a vision of computing power 'invisibly' embedded in the world around us and accessed through intelligent interfaces: 'Its highest ideal is to make a computer so embedded, so fitting, so natural, that we use it without even thinking about it.'"

Figure 1.2 is a pictorial depiction of the history timeline of IoT.



1970 to 1990 In 1970, the initial idea of connected devices was proposed; in 1990, the first IoT device was developed called Sunbeam Deluxe Automatic Radiant Control Smart Toaster. In 1982, computer science students at the Carnegie Melon University had connected a Coca Cola vending machine to the internet.

1990 to 2000: In 1995, the first cellular module built for M2M. In 1999, the actual term "Internet of Things" was used; The IOT concept was coined by a member of the Radio Frequency Identification development community in the year 1999.

2000 to 2010: IoT was popularized through famous press like Boston Globe, the Guardian, etc. In 2005, the United Nation's International Telecommunications Union published its first report on IoT. Three years later, IoT was born on a world wide scale. During the period 2006-2008, IoT is recognized by the European Union and the First European IOT conference is held.

2010 to current: In 2011, the new protocol IPV6 was launched. Raspberry Pi, Arduino and other hardware platforms make IoT accessible to novices and DIYers. Reached mass market in early 2014 when Google announced to buy Nest.

Figure 1.2*: History of the Internet of Things*

In the year 2011, the new protocol, IPV6, was launched. The main function of IPv6 is to allow for more unique TCP/IP address identifiers to be created. This is one of the main reasons why IPv6 is such a critical component for IoT. Also, the increasing popularity of IoT hardware platforms grew immensely from this period onwards. Raspberry Pi, Arduino and other hardware platforms make IoT accessible to novices and DIYers that can help them to quickly develop IoT prototypes or projects.

It reached the mass market in early 2014 when Google announced to buy Nest for 3.2 US billion dollars. How are you reading my book right now? It might be on a desktop, on a smartphone, or any other device you are using, and it is most certainly connected to the Internet, which makes it an IoT device.

Spotlight
As TechCrunch (it is an American online publisher focusing on the tech industry) recently put it: “at this stage, there’s no putting the [Internet of Things] genie back in the bottle.”

IoT is bringing together a diverse set of players. It is estimated that global IoT spending will total 15 trillion US dollars in the 6 year period between 2019 and 2025, and IoT solutions have the potential to generate 4 to 11 trillion US dollars in economic value by the year 2025.

Table 1.1 provides us with an overview of statistics related to the various aspects of IoT.

IoT devices	Gartner anticipates that there will be 25 billion connected things by 2021 According to IDC, 75% of 56 billion connected devices worldwide are anticipated to be connected to an IoT platform by the year 2025
IoT use cases	66% of cities in the USA are making investments in smart city IoT technology. This includes intelligent traffic signals, smart meters and Wi-Fi kiosks 250 million connected cars will be present in 2020
IoT spending	The total business spending on IoT solutions by 2021 will reach 6 trillion US dollars Beyond 2021, it is expected that IoT spending will grow at 26.7% annually
IoT challenges	70% of IoT devices are vulnerable to security issues 75% of organizations will not benefit from the full potential of the IoT technology they are using, and this is due to the lack of data science specialists

IoT acquisitions	Cisco paid 1.4 billion US dollars to acquire IoT startup company Jasper Technologies SoftBank acquired ARM for a whopping 32 billion US dollars

***Table 1.1**: IoT statistics*

1.2 IoT concepts—needed for an increasingly interconnected world

We live in an increasingly interconnected world. An IoT device can be as small as a light bulb that can be switched on and off using a smartphone, or it can be as large as a driverless car equipped with dozens of sensors.

Without a doubt, these days, most organizations have become data-driven, and with IoT, this data is converted into actionable real-time insights. Also, IoT is related to three other main concepts: automatically, safely and with fewer efforts. According to **International Data Corporation** (**IDC**) (which is the premier global provider of market intelligence, advisory services), the global spending on IoT will exceed 1 trillion US dollars by 2022. The main aim of IoT is to make virtually everything smart with the help of technologies such as artificial intelligence, big data, and so on. The current data analytics have some limitations, but with IoT in the picture, they can be enhanced to provide an accurate picture.

All the collected data from the IoT devices need some kind of connectivity mechanism. And this mechanism is used to send data to some sort of a centralized hub like cloud infrastructure. These connectivity/communication mediums include Bluetooth, Wi-Fi, WAN, and so on.

Most IoT setups deal with the following protocol layers: perception layer that is responsible for sensing and gathering information about the environment from devices that includes various smart devices, sensors, controllers; network connectivity/edge computing that include wired and wireless networks and communication protocols, and it is responsible for connecting to other devices, servers, and so on, and it is also used for transmitting and processing sensor data; Information processing layer; and application layer deals with delivering application-specific services to the end-users.

Spotlight
IP-based addressing will no longer be suitable for the upcoming future involving a heavy proliferation of IoT. And this proliferation is going to be there in almost all aspects of life, right from smart healthcare to smart homes. IoT is about enabling devices to interact, contribute and collaborate.

Machine-to-machine (**M2M**), also called as **Machine Type Communication** (**MTC**), is the communications infrastructure of IoT. It handles the interaction of devices and machines that are connected to each other and to the Internet. M2M was first adopted in manufacturing and industrial setups. M2M is among the fastest-growing forms of communication in the marketplace as it enables large-scale implementation of IoT. M2M is the transfer of information from one device to another, whereas IoT is a broader term that refers to a network of connected devices that entails multi-level communication.

Machine-to-machine was initially a one-to-one connection whereby it linked one device to another. But due to today's explosion of mobile connectivity, data can now be more easily transmitted through a system of IP networks to a much wider range of devices. M2M can be embedded in software and hardware to connect devices. One M2M, the global partnership project and standardization body, was created to develop standards to enable IoT applications across different verticals to communicate in a smooth manner.

The emerging Industrial IoT (IIoT) gives rise to what is being called the next *industrial revolution*. Industry 4.0 and IoT are used almost interchangeably, but they are not synonymous. The fourth industrial revolution, or Industry 4.0, is closely linked with IoT. Industry 4.0 entails the use of automation and data exchange in manufacturing setups. It combines information technology with machine data communication between devices and machines. *Michael Kanellos,* spokesperson and analyst for OSIsoft (it is a manufacturer of application software for real-time data management), said, *"It is about using data as a driving force. The first wave involved mechanization and steam power; we were going beyond what you could do with human or animal labor. The second wave involved mass production. The third: robots and mechanization."*

The term Industrial Internet or Industry 4.0 goes beyond M2M since it not only deals with connections between devices but also includes human interfaces. It mainly focuses on manufacturing setups. Industrial Internet refers to the extension and use of IoT in industrial sectors and applications by making use of smart sensors and actuators to enhance industrial processes. And IoT goes beyond this aspect as it also includes dynamics beyond the industrial context to include other domains too.

IoT is affecting Industry 4.0 in a big way, and all thanks to the big data that is being generated through the IoT universe. For example, big data generated through IoT devices, sensors and other input points can be used for predictive analytics to help companies reduce their maintenance costs and relief the human resources, which can then invest their time and energy in a critical and creative task. IoT, along with big data, is reshaping how the world operates. By the year 2025, there will be more than 75.4 billion IoT devices worldwide.

Spotlight

IoT connectivity is helping the IoT universe grow. New enabling technologies for IoT networking, implies networks are no longer exclusively tied to major providers. Moreover, much of the current interaction with connected technology is more of a passive engagement, but with IoT, active engagement is becoming the norm.

The growth of the IoT is expected to go through the following stages of development. Passive involves RFID sensors, and so on; it constantly monitors the environment and offers the appropriate options to the users so they can take action. Active involves responding to sensor data. And then the next stage is the aware stage, whereby IoT can make choices based on data, and finally, the autonomous stage. Currently, IoT is in the early stage of development of the passive phase where data is being received from devices, objects, and so on, and then action is taken manually.

IoT provides a plethora of benefits like enhanced data collection and analytics, and hence, better insights and decision-making, which in turn leads to better customer engagement and customer-centricity. It helps to reduce human errors due to repetitive tasks and mundane activities. It helps to improve business processes and strategies. IoT, along with data analytics, can provide better and accurate actionable intelligence that can help to enhance business processes. With IoT, all things are interconnected, and due to this aspect, we can make the system more secure and efficient. And all these benefits lead to substantial cost savings and generate more revenue. Along with these benefits, IoT also has a downside: IoT setups are complex in nature, IoT is susceptible to a large spectrum of cyber-attack vectors.

As yet, there are no international standards of compatibility for IoT, and this makes it difficult for devices from different vendors and manufacturers to interface with each other. Moreover, with so many IoT devices connected to the Internet, there is an increase in the risk of data breach and the biggest disadvantage is that of losing control of life over to technology, and our dependency on technology is certainly increasing day by day.

1.3 IoT advantages and disadvantages—so many

Automation is the need of the hour, and this is where IoT comes into play. And due to this, IoT opens the door for new business opportunities and revenue streams. IoT provides seamless connectivity by offering the ability to operate multiple things from one device, for example, smart appliances, and this makes life easier. It also minimizes human efforts and human errors, as well as several of the aspects such as maintenance, remote support, and so on, are taken care of.

The machine-to-machine interaction provides better performance and time response. Due to its ability to give real-time results, IoT enables people to do critical activities and creative tasks. IoT helps to gather data, and the more significant the data and information is, the easier it is to make the most suitable decisions.

Due to IoT, a massive amount of data is collected easily and quickly. Once the IoT device is properly configured and implemented, it will automatically tackle this. It will gather data in terms like preferences and several other parameters, then store it in some centralized location or in the cloud storage for further use and processing.

Better and transparent communication is possible because of the interconnected nature of IoT. IoT helps devices communicate in a more efficient and effective manner.

As worldwide energy consumption is expected to grow by 40% over the next 25 years, energy-efficient solutions are the need of the hour, and this is where IoT comes into play. IoT setups and devices can save a lot of energy and reduce waste, and hence, reduce energy consumption costs. For example, an IoT system can detect variations in climate and make adjustments accordingly. As a result, it is helping the environment by saving energy and also saving money on bills in the process. IoT solutions offer a more stable and reliable source of power.

Spotlight

IoT can bring about a plethora of benefits for the customers, organizations, environment, and society, but as with any technology, there are always a set of disadvantages too.

On the one hand, IoT minimizes human effort; on the other hand, this leads to too much dependence on technology as we are not even willing to do small tasks, and this indicates we are getting handicapped with every new advancement in technology. With this dependence on technology increasing day by day, IoT devices will surely begin to dictate and control life in almost everything. And this will make people indolent.

Data security and information privacy is big issue with IoT. The more we entrust and rely on technology and its tools, there will be more likelihood of potentially negative scenarios in case this technology and its tools fail to deliver proper results. Industry research shows that users and consumers want security and privacy measure in their IoT devices, but that does not mean they will be willing to pay for it.

With so many devices connected to the Internet and interconnected to each other, cyber risk attack vectors increase, and there is every possibility that one's personal information and private data can be misused. Many companies do not have strong security measures and protocols in place. Moreover, an attack on IoT setups may bring real danger and damage to the real world because IoT is the bridge between the virtual world and the physical world; for example, app-connected cars can be hijacked. Even companies could make a lot of money from selling user's private information and personal data collected by their IoT devices without the consent or knowledge of the user. Such concerns make end-users and customers suspicious of such setups and devices; hence, they are not able to place their trust in these setups and devices.

On the one hand, organizations are moving ahead at full speed on the IoT highway and on the other hand, they are running far behind standards, protocols, and regulations. There are no universal standards for device and equipment compatibility yet, and this makes identifying, tagging and monitoring of devices a difficult task. Each organization develops its own proprietary solutions, and this adds to the compatibility level making it more difficult to integrate diverse devices and multiple systems. This compatibility issue, in turn, may lead to yet another problem of monopoly. This compatibility issue may force the users to buy and use devices from a specific manufacturer, which may create a monopoly in the market.

Designing and developing IoT setups requires skills and involves a high degree of complexity. And again, with the huge quantum of data generated from IoT devices, real-time analysis at times may not happen due to a lack of supporting technology and data infrastructure. As there are multiple vendor devices involved in a typical IoT setup, it requires interfacing and interoperability tests to be conducted before launching the IoT system for use, and this incurs heavy costs.

Moreover, interconnected IoT devices rely so much on the Internet that they cannot function without it. Without the Internet, the IoT devices will be rendered functionless; hence, making the end-users handicap as they do anything without these devices.

Looking at the IoT landscape from a socio-economic viewpoint, widespread adoption of IoT can cause mass unemployment of unskilled labor; unskilled workers are at a high risk of losing their jobs. Even if this technology offers us some advantages, it takes something back on a large scale as well as replaces mundane and repetitive jobs, but this means unemployment for low-income and less educated segments of society. Today, we are seeing a decline in jobs in various sectors where IoT, automation, and other functionalities are being implemented, and some examples include inventory evaluation, customer support, and so on.

IoT has an enormous impact on all aspects of life. To be able to become an effective player and be adopted on a mass scale, all IoT stakeholders will need to work on strategies of minimizing the impact of all the disadvantages.

Table 1.2 gives us a tabular recap of the various IoT advantages and disadvantages.

IoT advantages	• Automation • Better performance and time response • Minimized human efforts and human errors • Energy-efficient solutions • Enhanced data collection
IoT disadvantages	• Complexity • Security and privacy issues • Compatibility issues • Mass unemployment • Over dependency on technology

***Table 1.2**: IoT advantages and disadvantages*

1.4 IoT processes—from data collection to analysis

Devices with sensors and mini-computer processors are connected to an IoT platform, which collects and integrates data from the different devices and runs basic analytics on the same (both real-time and historical data) to provide actionable intelligence in terms of patterns, outliers, recommendations, and so on, and uses artificial intelligence and machine learning algorithms to do this. Essentially speaking, these IoT devices are mini-computers with machine learning support. These devices require basic storage and processing, which is usually provided by a microcontroller. Thereafter, this data is sent to a cloud setup, and this needs some form of connectivity medium like Wi-Fi, satellite network, WAN, and so on. Typically speaking, these devices are embedded devices. The embedded programs are often developed using programming languages such as Java, Python and C++.

In a typical, traditional setting, a heat sensor would display the pressure value on an analog or digital screen, and a person/persons would be monitoring it physically, or there could be an advanced setup where when the heating level goes beyond a threshold, an alarm would set off. In either case, the human element will need to be in proximity of the system and alarm to take appropriate action. In an

IoT setup, this sensor would be able to send a message to a decision engine that has rules within it to take the required action without human intervention. A decision tree helps businesses to make the right decisions. It helps to build appropriate workflows that facilitate to make easy yes/no decisions and also provide information on situations that need further analysis.

The next component in this process is that of connectivity. Now that we understand the role of devices with sensors, we now need to understand how they communicate with the decision engine. Various communication/connectivity protocols are used for providing wireless connectivity for IoT sensors; some examples are Bluetooth, cellular satellite, and so on, and the emergence of such protocols is due to the rapid increase in the number of sensors and data originating from these sensors. Once the receivers have received the data, they can send this data to the decision engines.

Another major component is the hyper decision framework. It is a set of rules built inside a rule engine that works at hyper speed in order to help organizations to make better and faster decisions. Its main focus areas are user experience, data, technology, business, security, and standards and regulations. This framework goes above and beyond the typical decision support system; it is more like a decision intelligence system facilitating better agility and visibility into the decision-making process, and this leads to hyper decisions.

Now that we have been able to send the data to the cloud let us try and understand what happens there in regards to IoT. Using the cloud is important for aggregating data and deriving insights from that data, and moreover, it provides scalability and smart capability. Devices and sensors collect data and perform some preliminary analytics, but most of the smart processing happens in the cloud. Processing could be simple or complex, and based on this, the user interface comes into play; this will help to provide the machine-to-people interface through the setup.

The end-user could be notified of an anomaly or a deviation through notification, e-mail, and other options. And based on this input, there could be two main possibilities, either the user may take an appropriate action to correct the deviance/anomaly, or the IoT setup could automatically make the necessary adjustment through pre-defined rules.

Figure 1.3 is a pictorial depiction of the IoT processes.

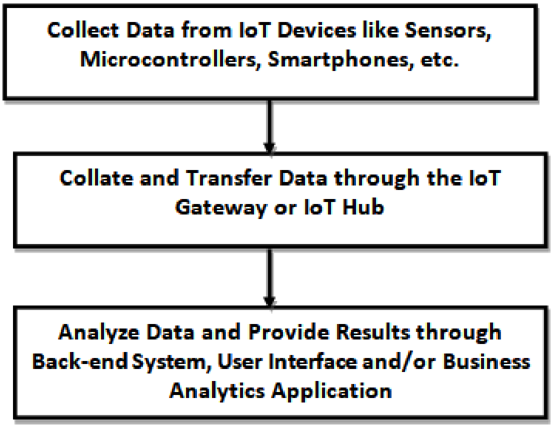

Collect Data from IoT Devices like Sensors, Microcontrollers, Smartphones, etc.
Collate and Transfer Data through the IoT Gateway or IoT Hub
Analyze Data and Provide Results through Back-end System, User Interface and/or Business Analytics Application

***Figure 1.3**: IoT Processes*

1.5 IoT software and hardware—application and process extension, sensors and more

European Organization of Telecommunications by Satellite S.A. (Eutelsat is a European intergovernmental organization; a satellite operator) in 2018 announced that it will launch 25 satellites to serve the IoT market, and such developments are definitely going to give a lot of traction to IoT. Eutelsat IoT first provides ubiquitous coverage which can reach objects with limited or no access to terrestrial networks.

The new AWS managed satellite service called "*AWS Ground Station*" is going to give a big boost to IoT; AWS IoT Greengrass aims to build market-specific IoT solutions. It currently has 12 antennae that are positioned around the globe with an aim to improve data sets by combining satellite data with IoT sensor data.

Most IoT devices consist of software and hardware components. IoT hardware is related to aspects like types of sensors, amount of data to be captured and transmitted, type of communication interface and frequency of data transmission. IoT software is related to aspects such as data collection, application and process extension, and much more. IoT addresses key areas of middleware, embedded systems, networking, and so on. These applications are responsible for collaboration with critical business systems.

IoT software is needed to tackle aspects such as real-time analytics, data collection, device integration, and many more aspects. The main software components are:

1. **Application and process extension**: These applications extend the reach of present software to reach out to a wider network. They support accurate data collection and better productivity.
2. **Data collection**: This software is about data acquisition, and it collects data from multiple devices like wearable health meters, security systems, and so on, and then transmits it to a central server. It uses specific protocols to connect sensors with real-time, machine-to-machine networks.

   Most IoT devices generate status data, which is raw data, processed later on for analysis purposes. Other types of data collected are automation data and location data. It can work both ways by collecting data from devices or sending out data to devices.
3. **Data processing**: This software deals with processing the huge amount of IoT data collected. It converts this raw data into something useful.
4. **Device integration**: This software ensures stable networking among the devices by managing applications and protocols of each device to facilitate communication. It helps to create and sustain the entire body / setup of the IoT solution / system.
5. **Real-time analytics**: With the explosion in the number of IoT devices across the world, there arises an urgent need to harness the power of data to produce actionable and meaningful insights. Traditional solutions allow after-the-fact, offline data mining and analysis and provide actionable insights after several days or weeks. This is no longer acceptable in a world where everything needs to happen in real-time. This is where real-time IoT analytics applications come into play. They take input data from several input points like devices, sensors, and so on and convert it into insights, actions and patterns for decision-making and analysis in real-time. This helps to achieve data aggregation, transmission and analysis.

Such applications provide the flexibility to run analytics in the cloud, at the Edge, or on a centralized server on the premises.

6. **Gateway**: An IoT gateway is software that facilitates IoT communication like device-to-cloud and device-to-device. It supports M2M. It serves as an intelligent access portal to give IoT devices access to the Internet. It translates communication among diverse IoT devices.

   It is a typical form of hardware having a software program on it to achieve this communication. It also performs data buffering and caching. It manages security features like network security, user access, and so on. It also does some level of pre-processing, cleansing and filtering of data. Apart from this, it also supports basic data analytics. Right from executing simple trigger-based rules to advanced capabilities of edge computing, IoT gateways are capable of performing a wide range of functions.

7. **Cloud**: The cloud and IoT share a complementary relationship; they are closely coupled. IoT generates massive amounts of data, and cloud computing provides a path for this data to travel. The cloud software completes the whole end-to-end IoT solution. There are several popular cloud service providers such as Cisco Cloud, Google Cloud, GE Predix, Microsoft Azure, and many more provide IoT platforms; they act as a sort of a front-end.

   Companies find it feasible to access these massive amounts of data through the cloud, and this provides economies of scale, especially for IoT startups. Using the cloud facilitates the factor of scalability. When there are endless sensors involved in IoT, having large amounts of computational power on each sensor would be extremely cost-intensive. Instead, data can be sent to the cloud from all these sensors and processed in the cloud.

   The cloud also allows developers to access IoT cloud computing on-demand through several options. It also provides better encryption protocols and security authentication for IoT.

Figure 1.4 is a pictorial depiction of the IoT software components.

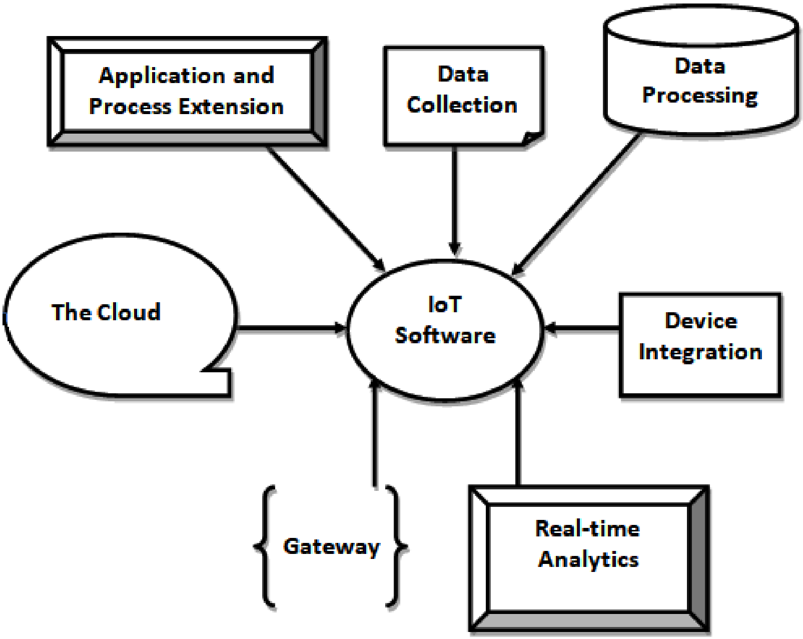


Figure 1.4*: IoT software*

IoT hardware is an equally important component of the IoT setup. The building blocks of IoT hardware are the device, sensors/ actuators, bridges, routing devices, communication interface, wearable devices, and other standard devices. The smartphone is the most used computing device in all spheres of life. Smartphones do play a big role in IoT as many IoT devices can be controlled through an app on a smartphone.

In today's smart setups, the smartphone plays a critical role, right from monitoring sensors to turning them off. First, it all started with a smartphone, and now with IoT, practically every device is soon to become smart in nature. Wearable devices such as smartwatches, activity trackers, and so on are an integral part of the IoT setup, and they facilitate great access and connectivity for better productivity.

IoT hardware platforms such as Particle Raspberry Pi, ESP8266, Intel Galileo, Banana Pi, and many more are an integral part of IoT applications. Most of the hardware development boards are microprocessors and microcontrollers, and some of them may have in-built sensors, and they offer a range of features integrated into them such as connectivity, developer tools, SDKs, and much more.

The most important hardware is a sensor. A sensor manages sensing through assorted active and passive measurement devices. Without sensors, there is no IoT data. It is used to measure so many factors and conditions, right from altitude to airflow and from water flow to pressure. Just as our senses allow us to perceive, interpret and make sense of the world, similarly, sensors allow machines, devices, and so on to make sense of the world and its environment. The component or thing may either be a device, machine, and so on, or a stand-alone thing. This device could either be a digital-first device, which connects with other devices (machine-to-machine) or a physical-first device, which has embedded circuitry on a sensor and it then connects to a specific endpoint like a monitoring platform or a dashboard. Devices may be stand-alone, or they can work in sync with other devices.

The data acquisition component/module deals with taking physical signals such as pressure, temperature, and so on from the "*thing*" and converting them into digital signals that can then be processed by a computer system. It is also responsible for functions noise removal, scaling, and conditional of incoming signals. It focuses on gathering and analyzing real-time data. This module consists of three essential elements—sensor, signal conditioning, and analog-to-digital converter. The analog-to-digital converter is responsible for analog to digital conversion—sampled signals are converted into digital form, and these signals can be analyzed, displayed, and stored in a computer.

The data processing module is the actual computer and the main unit, which deals with data storage, computing, local analytics, and many more functions. It plays a major role in converting raw data into something useful.

And the last hardware component is the communication module which is responsible for communication with the cloud and with third-party systems, both local or in the cloud.

Figure 1.5 is a pictorial depiction of the IoT hardware components.

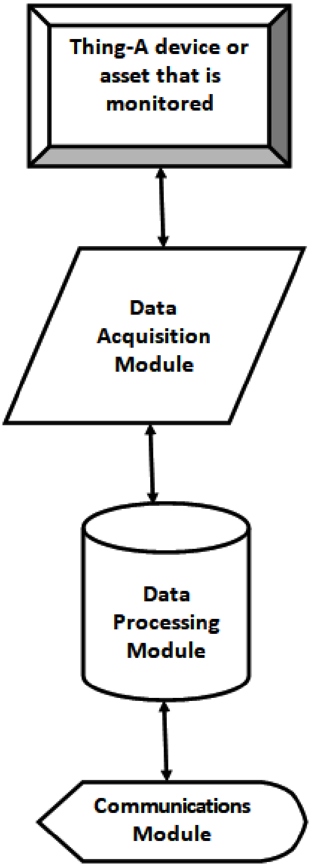


Figure 1.5: *IoT Hardware*

1.6 Conclusion

In this chapter, we have covered the basic dynamics and specifics of the building blocks of IoT in terms of definition, history, features, core concepts, advantages and disadvantages, processes, and software and hardware components so as to enable all stakeholders to understand the importance of riding the wave of IoT in a responsible and successful manner. This chapter sets the stage for the upcoming chapter that deals with important topics such as IoT architectures, networks, and protocols.

1.7 Questions for reflection

1. What business needs can be solved with IoT?
2. Which are some of sectors that use IoT?
3. What are the security concerns related to IoT?
4. What are the main components of IoT?
5. What does IoT stand for?
6. Give daily life examples of IoT?
7. How many IoT devices are expected to be connected to IoT by the year 2025?
8. What is the difference between IoT and IIoT?

Chapter 2

IoT—Nuts and Bolts of the Architecture

IoT architecture is made up of components, frameworks, networks, and protocols that are used to cater to the three main players of the architecture: the device layer or the client-side, the gateway layer or the operators on the server-side, and the platform layer or a pathway for connecting client-side and server-side. Although every IoT system is unique, the foundational framework is almost the same. The device layer consists of all the smart devices that are connected to the system. The gateway layer sits between the device layer and the platform layer. The platform layer consists of edge and cloud-based or physical data centers.

A typical IoT architecture consists of devices or objects connected to the Internet called as *"things"* and with the help of their embedded sensors and actuators, they are able to sense the environment around them and collect information that is then passed on to gateways. The next stage is that of IoT data acquisition setups and gateways that collect a huge amount of unprocessed data, which then is pre-processed so that it is ready for analysis. The third layer contains edge computing devices responsible for further processing and enhanced analysis. Thereafter, the data is transferred to data centers which can be local or in the cloud. This is where the data is stored, processed, and analyzed in-depth for decision making, actionable insights, and so on. The IoT architecture, no doubt, has come a long way and will need to march on further to minimize all the problems related to fragmentation and building a more standardized and integrated future filled with more scalable and secure IoT systems.

Spotlight
The core elements that make IoT architecture successful are availability, maintainability, scalability, and cost-effectiveness.

Structure

This chapter will cover the following topics:

- IoT framework essentials and various frameworks
- IoT platforms and models
- IoT communication protocols
- IoT networks
- Challenges and solutions

Objective

After studying this chapter, you will be able to:

- Understand the key components/essentials of IoT framework/ecosystem
- Identify the major IoT platforms and models
- Identify the various IoT networks and their strengths and weaknesses
- Understand the major IoT communication protocols
- Pinpoint the challenges and solutions of IoT systems

2.1 Framework—key component of the ecosystem

We have discussed the dynamics of IoT architecture/ecosystem (refer to *figure 2.1*) in the previous section. Now in this section, we will deal with the key component of IoT—the IoT framework essentials.

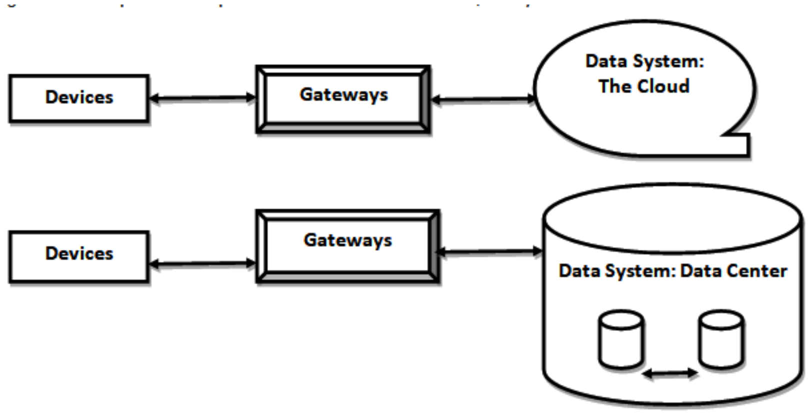


***Figure 2.1**: The IoT architecture/ecosystem*

IoT frameworks are a key component of an IoT ecosystem and services. This ecosystem and services consist of several programs related to security, analytics, middleware, connectivity, software and hardware, and so on. IoT Frameworks help developers, vendors, and manufacturers to develop products and services in a decreased time period. The main aim of IoT frameworks is to make the aspect of data transmission seamless and to provide a standard way of implementing the services.

Most IoT frameworks solve different aspects of the total IoT ecosystem. There is not one single comprehensive framework available till date. And also, integration is not possible due to several loopholes. Currently, the IoT framework landscape is quite fragmented.

Spotlight
Overcoming fragmentation is about IoT organizations overcoming the silo mode and expanding their operational footprint in order to carry out smooth IoT deployment. It is about expanding through open-source frameworks that facilitate collaboration among IoT solution providers.

Figure 2.2 is a pictorial depiction of the IoT framework essentials.

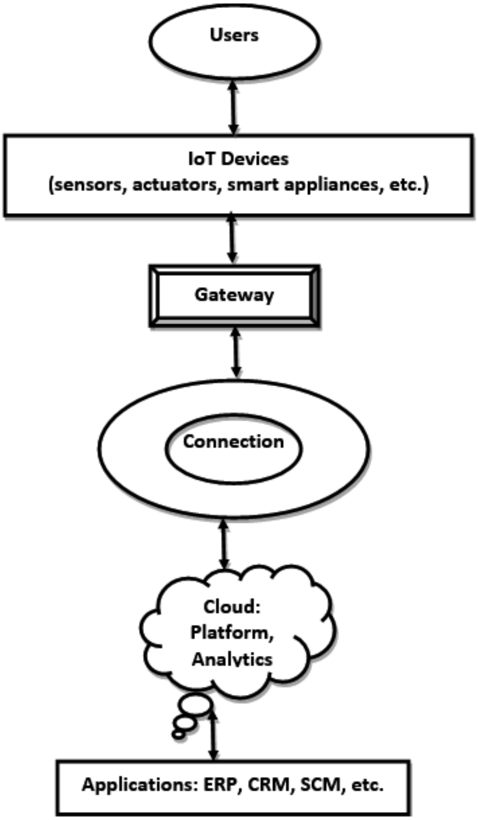

Users
IoT Devices
(sensors, actuators, smart appliances, etc.)
Gateway
Connection
Cloud:
Platform,
Analytics
Applications: ERP, CRM, SCM, etc.

***Figure 2.2**: IoT Framework Essentials*

The main components of an IoT framework are users, software applications, hardware devices, cloud applications, and communication channels. Some of the common IoT Frameworks are Salesforce, Hewlett Packard Enterprise, Cisco IoT Cloud Connect, IBM Watson, and ThingWorx.

- **ThingWorx**: It is one of the earliest IoT software platforms designed to build and deploy smart IoT applications as it provides end-to-end, scalable, and flexible application design, runtime, and intelligent environments. With the help of pre-built widgets and extensions, ThingWorx facilitates the rapid developing and deploying of IoT applications. It facilitates the development lifecycle in one centralized place, which helps to quickly connect devices, analyze data, and build, deploy and extend solutions.

It provides advantages like drill down to details on a one device level and provides features that help to bring about improved customer experience and optimized business processes. It provides a user-friendly interface to set up IoT systems and also facilitates integrated machine learning. It requires very little programming.

IoT devices are represented by software objects, properties, and data are included in the representation. Users can then use the objects to build applications that can track and control devices. Users can also build dynamic dashboards, apply business logic, and incorporate applications from third parties.

When it comes to managing highly complex systems or installing edge systems in a custom platform, ThingWorx does not perform that well.

- **Salesforce thunder**: It is optimized for IoT setups, and it is a massively scalable real-time event processing and rules engine. It is designed to capture, filter, and respond to events in real-time, and it does this in coordination with the Salesforce IoT cloud.

  It is based on open-source tools of the likes of Apache Cassandra (a highly scalable distributed database management), Apache Kafka (a messaging system that can handle a massive volume of data), Apache Storm (big data and event processing platform in real-time), and Apache Spark (distributed large-scale data processing framework for both batch and streaming data).

  Its pros include technology optimization, easy and interactive user interface designs, low-code environment, improved data collection, and real-time event processing. Its cons include flexibility limitation and security loopholes.

- **Oracle IoT**: Provides reliable and secure communication between IoT devices and the cloud, real-time analytic tools, integration of IoT applications with existing applications, and high-speed messaging where end-users can receive real-time notification directly on their devices.

  Oracle states: *"Oracle Internet of Things (IoT) Cloud Service is a managed Platform-as-a-Service (PaaS) offering that helps you make* *critical business decisions and strategies by allowing you to connect your devices to the cloud, analyze data, and alert messages from those devices in real time, and integrate your data with enterprise applications, web services, or with other Oracle Cloud Services, such as Oracle Business Intelligence Cloud Service."*

- **Hewlett Packard Enterprise**: It transforms IoT data into insights in an efficient manner. It lets the customers capture, analyze and act upon data in a seamless manner from the edge to the cloud. It is capable of supporting several verticals such as retail, manufacturing, and so on.
- **Cisco IoT cloud connect**: It is a popular, award-winning IoT platform that offers extensive IoT technologies. Cisco IoT platform is known as the platform with the least connectivity problems and great security support. This platform has received numerous awards in its field. It is a cloud-based software suite and provides a complete solution for mobile operators to provide top-class IoT experiences.

  It also supports IIoT. It can perform advanced data analysis along with proper operational safety measures needed by large enterprises. It provides flexible deployment options for devices. It facilitates faster and better decision-making and distributed intelligence and control.
- **Amazon Web services IoT**: It is one of the much-preferred **Platform-as-a-Service** (**PaaS**), and it can provide reliable and secure support for billions of devices and trillions of messages, and also can process and route these messages to endpoints and to other devices. It provides a well-rounded, secure communication between sensors, devices, and so on and the AWS cloud. It offers IoT services from the edge to the cloud. It facilitates the collection of data from multiple devices and stores, computes and analyzes the same.

  One can also create applications that facilitate the users to control the sensors, devices, and so on, from their computers, smartphones, and so on. It makes it easy-to-use services such as AWS CloudTrail, Amazon QucikSight, Alexa Voice Service, and so on to build IoT applications. It allows developers to develop their own SDK or use an open-source.
- **IBM Watson**: It provides robust security, rich developer resources, visual dashboards, and so on to build enterprise

IoT. With IBM cloud, organizations can scale and adapt quickly to changing business needs. It also helps to manage and integrate IoT data into asset-based data structures. It helps to parse, filter, and transform device and performance data in a quick manner.

It has the ability to handle a large quantity of data, process untapped data, and provide improvised customer service. And it provides data insights in a simple and intuitive manner. It uses standard protocols, and this allows for the efficient exchange of data to and from devices in real-time.

- **Eclipse Kapua**: It is a modular, extensible, integrated framework and it is built around Java/OSGi based Kura API container and aggregation platform for M2M applications. It began as an open-source incubator project under the Eclipse IoT Workgroup.

  It handles the connectivity for IoT devices and gateways through a number of different protocols such as MQTT, HTTP, and so on. It provides an application container, ready-to-use protocols, and Web-based visual data flow programming to acquire data from the field, process it at the edge, and publish it to IoT cloud platforms through protocols such as MQTT, HTTP, and so on.

- **GE Predix**: It began as a tool for General Electric's internal IoT, and now it caters to several industrial IoT applications; it is a software **platform-as-a-service** (**PaaS**). This platform is scalable and secure and provides industrial-grade analytics for performance management and operations optimization.

  It offers inexpensive developer kits that save the developers a lot of time by taking care of all the main functionalities such as establishing the connection, transmission of environmental data from devices, sensors, and so on. It has partnered with Microsoft Azure; hence, GE Predix is able to offer a host of advanced features such as advanced data visualization, AI, and so on.

Spotlight
The main factors that make an IoT framework successful are interfacing, interoperability among various devices, and value-added services.

2.2 Platforms and models—API-oriented, SOA-based

Technavio (it is a leading market research company with global coverage) has predicted that the global API-as-a-service market will reach 965 million US dollars by 2020. **Application Programming Interface** (**API**) allows developers to build context-based applications that can interact with the real world. IoT faces integration issues, and APIs provide a solution to minimize these issues considerably by providing a streamlined data pipeline. All main IoT providers such as Amazon, Google, Azure, and many more provide both HTTP and MQTT APIs to access their services.

API is a set of protocols, routines, and tools used for building software applications. APIs are tightly linked with IoT setups. In the case of IoT setups, these APIs help developers to access the functionality of a sensor/device. APIs are the points of interaction between a device and another device, or the Internet or several others components. APIs can be accessible to authorized users only, or they can be open to the public (not requiring any registration) as well. To facilitate the smooth functioning of IoT, we need **representational state transfer** (**REST**) (is a set of rules to build a web API) APIs for every device. They normally use methods of HTTP to perform different actions; actions such as POST, GET, and so on, which then can be mapped to database operations such as CREATE, SELECT, and so on.

REST APIs provide a unified architectural setup that helps to integrate heterogeneous services and applications in an efficient manner allowing IoT organizations and developers to focus on services and applications interactions versus the services and applications themselves.

With the help of the unified architecture of REST APIs, a single app can use software written with multiple programming languages. It helps to bring multiple services together for an IoT setup and allows them to interact in a standard, well-understood manner. APIs have the capability of developing built-in security to protect IoT devices and their data.

REST APIs make it easier for developers and programmers to work with connected devices without having to worry about the intricacies, and this makes IoT more accessible to developers and programmers in a consistent, scalable, and secure manner. REST is resource-based instead of action-based.

Spotlight
Just as HTML provided the standardization that helped the Internet to expand, in a similar manner, APIs are becoming the defacto standard for IoT application networks and setups. APIs are a sure-shot way of realizing the full potential of IoT.

According to IBM, *"In the years to come, the power and importance of APIs will be at the forefront of the conversation around enabling—and more important—monetizing the 'internet of things.'"*. The APIs work as data interfaces/pipelines to send the data to the cloud and retrieve the metrics, recommendations, and so on. Quite a few apps work in the standalone mode, but otherwise, the provider does all the main work in the cloud.

There are numerous API platforms already in place both for consumer and industrial IoT, but the problem of fragmentation is affecting them as there are issues with interacting and interoperability of IoT setups. The API market is expected to grow as more and more get into the IoT space. The main disadvantage or pain point of IoT is fragmentation which creates challenges. The best way forward is that service providers to start working on solutions that facilitate unifying the silos. *Figure 2.3* is a pictorial depiction of the application programming interface.

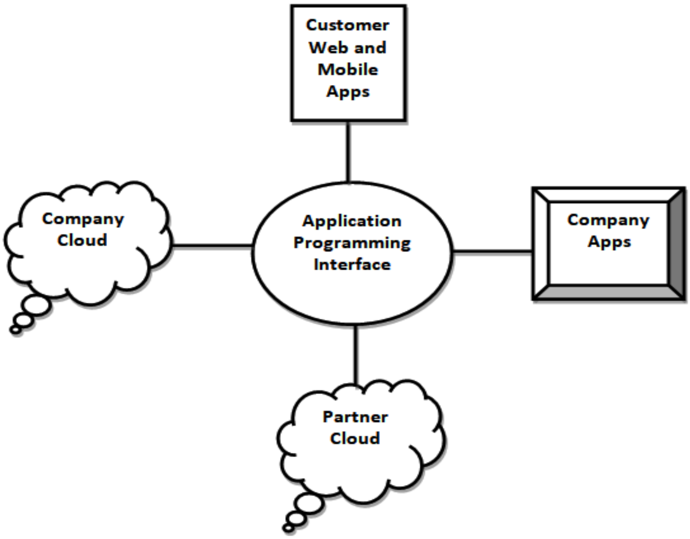

Customer Web and Mobile Apps
Company Cloud
Application Programming Interface
Company Apps
Partner Cloud

Figure 2.3: *Application programming interface*

Service-oriented architecture (**SOA**) is an agile software architecture model that consists of services, messages, operations, and processes, which together enable the development of new business applications.

Service-oriented architecture is a widely used design pattern. In a service-oriented model, the main aim is to start with how the IoT application should interact with the outside world in contrast to the technical aspects of how IoT works in the traditional model. Each interaction is independent of each and every other interaction.

SOA enables the development of new applications and facilitates applications integration architecture in an organization. It is based upon the use of services such as REST Web services. Services can be delivered as a composite service or as an individual service. A service is a function that is self-contained and does not depend on the state or context of other services. Its main aim is to be independent of technologies, vendors, and so on. SOA provides location transparency and better information flow, but it is not suitable for GUI-based functionality.

There are two major components of SOA—service provider: it is the maintainer of the service/s and the organization that makes available one or more services for others to use. The provider can publish the service/s in a registry which contains information such as nature of services, fees for the service, and so on, and the second component is that of service consumer: it can locate the service metadata in the registry and develop the required client components to bind and use the service.

As they are loosely coupled, SOA components can be changed with minimal impact on other components. Hence, scalability and reusability are not much of a headache. If IoT devices are visible on an open network, then cybercriminals, hackers, and so on can easily compromise their security. But with SOA, enterprises can place these devices in a private subnet, which is well protected and can be accessed only by the IoT services.

SOA services help to balance the load when devices are hit with multiple requests. SOA helps to harmonize the various devices and also insulate the various applications and systems from the fact that different devices, sensors, and so on operate differently. As SOA services present a harmonious view of the various components involved; thus, any changes in the components or how they behave will not affect the programming logic.

Spotlight

APIs can be thought of as a service, and SOA, as the architecture that allows the service to operate.

Figure 2.4 is a pictorial depiction of service-oriented architecture.

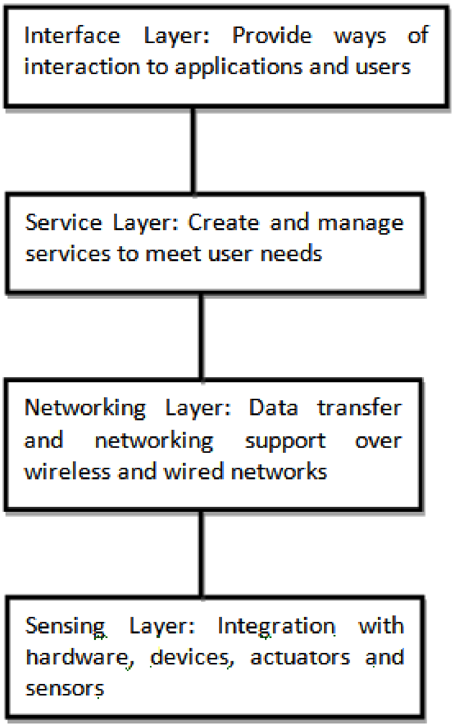

Interface Layer: Provide ways of interaction to applications and users
Service Layer: Create and manage services to meet user needs
Networking Layer: Data transfer and networking support over wireless and wired networks
Sensing Layer: Integration with hardware, devices, actuators and sensors

***Figure 2.4**: Service-oriented architecture*

2.3 Networks—options for transmitting data

There are several types of networks for IoT. Each network has its strengths and weaknesses based on the various network criteria like bandwidth, interoperability, security, range, and so on.

- **Wired and short-range wireless**: It does not allow a realistic operation on battery, is not well adapted to an industrial environment, and does not offer global scope (limited in scope). Using wireless or wired depends mostly on the application involved and others factors such as security, space consideration, economic implications, and so on.

- **Cellular (3G/4G/5G)**: It offers reliable communication but has high power needs, expensive equipment, a large footprint, and operational cost. 2G and 3G networks are likely to be shut down in the coming years. Though 4G coverage is currently the best around the world, it still has some flaws like higher power consumption, higher module cost, and so on.

  2G and 3G networks are slower than 4G. Several nations and companies have and/or are in the process of shutting down 2G and 3G networks to free up frequencies for the new technologies in favor of the new **Narrowband Internet of Things** (**NB-IoT**) service based on 4G, and this NB-IoT guard band uses a dedicated bandwidth at 180 kHz that is assigned just for IoT applications. Although cellular is not viable for the majority of IoT applications and use cases, it does fit well in certain use cases such as fleet management, traffic routing, and so on. 5G is the next-gen cellular network that offers ultra-low latency and high-speed mobility.

  The cellular IoT market is expected to grow from 1.26 billion US dollars in 2015 to 5.31 billion US dollars by 2022.

- **Low power wide area network (LPWAN) or low-power network (LPN)**: Provides long-range communication on small, inexpensive batteries, optimized to communicate for very small data rates, and supports large-scale IoT networks in vast industrial and commercial premises. It is a broad term used to refer to a variety of technologies used to connect sensors and devices, and so on to the Internet without the use of traditional cellular or Wi-Fi. The main players are the **long-range wireless area network** (**LoRaWAN**) and SigFox. Both these provide advantages like relatively low-cost chipsets and low power requirements. Other options include Weightless, NB-IoT, and RPMA.

  LPWAN sends and receives small packets of information at infrequent intervals. Messages sent over LPWAN need to be simple and small. Because of these attributes, these messages can be communicated over the required distance without needing a large power source. It can only send small blocks of data at a low rate, and therefore, LPWAN is best suited for use cases that do not require high bandwidth and are not time-sensitive.

Data packets that are transmitted over LPWAN sometimes are not received by the gateway, and this is called **packet loss**. This can be handled by adding additional gateways to the network or sending multiple messages, but these solutions result in higher costs and more power consumption, respectively.

Spotlight
There is no perfect networking solution for IoT. Hybrid solutions are viable solutions where the benefits of one solution help to overcome the disadvantages of the other.

2.4 Communication protocols—from Wi-Fi to Bluetooth

Some of the major IoT protocols include Wi-Fi, Radio, Bluetooth, and so on and they cater to and meet the specific functional requirement of an IoT system. IoT solutions involving wireless sensor networks, machine-to-machine, and so on require communication protocols. There are several protocols for physical and network access.

- **Wi-Fi**: It is based on the **Institute of Electrical and Electronics Engineers** (**IEEE**) 802.11 family of standards. It has become an indispensable part of our lives as it uses a wide range of infrastructure components and offers quick data transfers speeding up to hundreds of megabits per second. It has the ability to handle huge amounts of data transfers. It facilitates Internet access to devices that are within the range of about 66 feet from the access point.

  When one accesses Wi-Fi, one is connecting to a wireless router that allows one's Wi-Fi-compatible devices to communicate and interface with the Internet. A series of RF development kits designed for building Wi-Fi-based applications are also available.

  The deployment is easy, universal smartphone compatibility is possible, and the device cost is low in Wi-Fi setups, but the range for communication between devices using Wi-Fi is approximately much higher than Bluetooth. Wi-Fi is most suited for IoT applications that do not have to worry about power drain, for example, in-home automation IoT systems, whereas, for other types, LPWAN or Bluetooth works better. Wi-Fi offers a range of hundreds of megabits per second, and this may be too power-consuming for many IoT applications.

Wi-Fi 6 (the next generation of Wi-Fi) brings about a greatly enhanced network bandwidth, and this, in turn, helps to improve data throughput per user in congested environments.

- **Near field communication (NFC)**: It provides simple and safe communication between devices and enables devices to share information at a distance that is less than 4 cm. It facilitates easy-to-tap-and-go communication, and there is no lengthy handshake involved. By embedding NFC tags in unconnected, unpowered devices, objects, and so on, one can make them IoT-driven smart systems. Some examples of NFC are transport ticketing, contactless mobile payments, and so on. It involves an initiator and a target device.

  There are two modes—**active mode**: in this mode of communication, both devices alternately generate an RF signal on which the data is carried. And both devices have power supplies. **Passive mode**: the initiator device provides a carrier field, and the target device answers by modulating the existing field through the load modulation technique to transfer the data back to the primary device or initiator.

- **Radio frequency (RF)**: It is the easiest form of communication protocol between devices, and it is in the range extending from around 3 kHz to 300 GHz. Protocols such as ZWave, ZigBee, and so on (primarily used for home automation for products such as sensors, controllers) use a low-power RF radio embedded in systems and devices.

  RF radiates from an antenna on the transmitter end and is then received by an antenna on the receiver end. The actual data being carried is modulated on one end, and it is transmitted over the air. Then the data is demodulated on the other end. The signal propagation characteristics are determined by various aspects such as amplitude, wavelength, and frequency. RF is mainly used in large deployment setups where a large number of devices are needed to be managed locally and centrally.

- **Bluetooth**: It is used for exchanging data between devices over short distances using short-wavelength UHF radio waves. There are three main kinds of Bluetooth: Classic Bluetooth, which is battery draining, Bluetooth 4.0 or **Bluetooth low energy** (**BLE**), and iBeacon. In contrast to Classic Bluetooth, BLE is designed to provide significantly extended range mode and lower power consumption. Hence, it is suitable for many industrial IoT applications.

  As several IoT systems involve small devices and sensors, BLE has become the more common protocol of the two. iBeacon is a hardware transmitter by Google—a class of Bluetooth low energy devices that broadcast their identifier to nearby portable electronic devices. The new Bluetooth low-energy or Bluetooth Smart is an important protocol for IoT applications; it has been designed to offer significantly reduced power consumption. iBeacon is a simplified communication protocol based on Bluetooth technology that Apple uses.

  On the one hand, Bluetooth is a widely used technology as it makes using services easier and it facilitates better management of permission configuration, security measures, and so on, but on the other hand, keeping pace with changing hardware capabilities becomes cumbersome.

- **Zigbee**: It is one of the most trusted standard wireless protocols, and it is majorly used in industrial settings. It is the full-stack solution for a majority of large smart home ecosystem providers. It provides long battery life and a low latency rate.

  It is a product from Zigbee Alliance based on the IEEE Standards Association's 802.15 specifications. It operates in the **industrial, scientific, and medical** (**ISM**) radio bands.

  Data is usually sent through a mid-range distance of 10 to 100 meters, but ZigBee uses its mesh network to significantly extend this distance. The latest version of ZigBee 3.0 is the unification of the various previous wireless standards into a single standard.

2.5 Challenges and solutions—ups and downs

The challenges faced by the IoT systems are very different from their traditional counterparts because the number and complexity of endpoints, applications, and so on involved are higher. Inmarsat (a British satellite telecommunications company that offers global mobile services) stated that 24% find connectivity issues as one of the biggest challenges in IoT deployment.

As per findings by *McKinsey* (it is an American management consulting firm), 40% to 60% of the total value lies in our ability to achieve interoperability between different IoT systems. Data connectivity can be an IoT implementation challenge. The more components there are in the system, the more complex and confused it gets for the users. Identifying the physical devices and understanding the associated compatibility issues before undertaking the IoT implementation is highly recommended.

Problems such as connectivity, implementation, interoperability, and so on need a robust ecosystem, global standards, and security protocols are much needed. In order to drive greater adoption and usage of smart devices by the mainstream population, the IoT onboarding process must be simple, seamless, and personalized. Organizations have taken notice of this consumer preference for self-service and are upgrading their current **support of things** (**SoT**) customer support models. Many organizations are also working on providing AI-driven self-service IoT solutions, visual assistants, virtual assistants, and so on.

There is a lack of trust to exchange data, information, and knowledge. There is a lack of trust in the existing data exchange platforms. Given the fact that a large amount of IoT data is stored in the cloud, it is likely that cloud platforms are one of the main targets of cybercriminals. Factors such as encryption, firewalls, and so on are needed to protect the IoT system from attacks. Also, the IoT ecosystem needs overlay agent-less, agnostic protection to monitor the traffic of the devices. One can also reduce the vulnerability of IoT devices through measures such as two-factor authentication, digital certificate, and many more.

2.6 Conclusion

In this chapter, we dealt with important topics such as the various IoT architectures, networks, protocols, and challenges and solutions. This knowledge is essential for facilitating proper interaction and interconnection with the IoT devices, sensors, setups, and so on. This chapter sets the stage for the upcoming chapter that deals with the IoT data management strategy and its critical components.

2.7 Questions for reflection

1. What type of endpoints do we need to support IoT solutions?
2. What are some of the major IoT protocols?
3. What are the benefits of APIs?
4. What are some of the challenges of IoT systems?
5. Which factors determine the strengths and weaknesses of a network?
6. What measures need to be taken to ensure an IoT project's success?

Chapter 3 Data Management Strategy

IoT systems generate a huge amount of data, but not all this data is needed or used for improving the business of an organization; this is where a well-thought data management strategy comes into play. A comprehensive data management strategy saves a lot of time and energy for organizations, which they then can use for tackling higher-impact tasks.

According to a recent report published by *Machina Research* (it is the world's leading provider of strategic advice on the newly emerging M2M, IoT, and Big Data markets), "*The significance of the Internet of Things is not that more and more devices, people and systems are 'connected' with one another. It is that the data generated from these 'things' is shared, processed, analyzed and acted upon through new and innovative applications, applying completely new analysis methods and within significantly altered timeframes. The Internet of Things will drive big data, providing more information, from many different sources, in real-time, and allow us to gain completely new perspectives on the environments around us.*"

Spotlight
In the past, data was considered as a by-product of a business process or any other process for that matter, but in the current era, data is the new oil, which essentially means everything in business and in life revolves around data.

The value derived from data is directly proportional to the volume of data. Volume creates value, and in order to tap into and harvest benefits from this value, organizations need to have a robust data management strategy and infrastructure in place to be able to handle huge volumes in order to gleam actionable insights from it. The data coming in from a few connected devices may be manageable, but storage can become an issue as more devices come online, and adding more storage is not the solution. If organizations really want the data that they collect to work for them, then they have to understand how to manage it with the help of a scalable data management strategy.

To handle the data effectively and generate revenue streams from it and gain quick access to metrics, a data management strategy is needed. It is a formal, comprehensive approach that consists of components, policies, practices, and so on for preserving and enhancing the aspects of data shareability, communication, security, quality, and access across an organization.

Structure

This chapter will cover the following topics:

- Practices and procedures of data management
- Business potential generated by data from IoT devices
- IoT solutions such as Microsoft Azure, Amazon Web Services
- Metadata, Edge computing, and more

Objective

After studying this chapter, you will be able to:

- Understand the prerequisites of data and its dynamics
- Identify the benefits of a data management strategy

- Understand what is an IoT data pipeline and which procedures are needed to build it
- Identify the business potential generated by IoT data
- Define the best practices needed for IoT data management
- Pinpoint the main players that provide IoT solutions
- Describe the supporting components of IoT ecosystem

3.1 Prerequisites—data and its dynamics

Before beginning the data collection process, organizations will need to identify their business needs and objectives and then will need to understand which type of data they will require and how much data storage they own, and these will fulfill their business needs and objectives. Business leaders need to analyze how different data sets can correlate to one another to use available data efficiently and minimize storage requirements.

Additionally, developers and business leaders need to collaborate to figure out how collected data can be optimized and integrated with enterprise systems. They can also use this data to conduct predictive analytics in terms of product or asset value. Insights from both users and device behaviors and patterns help organizations to carry out predictive analytics and pinpoint areas where the users need further training and the product/device/equipment needs enhancements; this scenario is highly pertinent to industrial IoT.

The sheer size of IoT data and the volume of traffic make the data management strategy a critical component of IoT. The IoT data management can be made robust only when it takes care of the following questions:

- What are you going to do with your data?
- Which types of data will be needed?
- How much data are you sending and transmitting to the cloud?
- How long are you going to keep this data?

- How do different data sets correlate to one another?
- Can the existing infrastructure handle large volumes of data?
- What data must be recorded before and after the fact to prove that the right decision/predication/recommendation was made?
- Will archival of data be needed?
- Which platform should be used to manage the gathered data?

The best way to develop a robust data management strategy is to first make sure that your existing data is well stored, well managed, and well secured. Thereafter, in-depth analysis, POC, and pilot studies are needed (based on questions shared before). Data streaming from a few connected devices may be manageable. Storage can become an issue as more devices come online, and this is where a proper data management strategy comes into play, as it enables businesses to discover usage patterns from this deluge of data. An efficient data management strategy should be able to handle data drift or schema drift.

As data is coming from several IoT devices and systems, it is bound to change over time, and this is where it is important that your data management strategy can address this data drift without interrupting the actual data management process. Data drift is the sum of undocumented and unexpected changes to data semantics, structure, and so on. This is where a data management strategy comes to the rescue; it helps to manage this uncertainty by facilitating organizations to tap into the new opportunities generated by data drift (rather than falling prey to corrupt data). Schema drift occurs when the sources often change metadata on the fly; columns, fields, and types can be modified, added, or deleted on the fly. A data management strategy is the solution as it can streamline this process by setting some clear rules in terms of defining sources that have mutable fields, types, and so on, defining dynamic transformation parameters, and so on.

Organizations need to carefully analyze several aspects of their data management strategy such as human resources, security measures, infrastructural resources, data requirements, and so on. By analyzing these requirements, businesses can allocate sufficient monetary resources for their projects. All the teams, such as sales, marketing, and so on, need to be trained properly so as to facilitate them to use the data efficiently and effectively.

Spotlight
Data management helps in collecting field data both during the launch and post-launch of various IoT products and systems. This helps with improved iterations and continuous improvements.

An optimized data management strategy will aim to filter out erroneous data coming from the IoT systems and also be able to enhance and enrich the data, both structured and unstructured, with metadata to facilitate better data analysis.

Data architecture deals with the logical structure of the data components, subcomponents, integration, and connectivity. It also provides a standard common business vocabulary for all stakeholders to understand. And this will be managed through tools such as Big Data, BI tools, Analytics tools, master data management, and more.

Organizations that deal with complex data insights and analytics can use the cloud for plugging in their IoT applications as the cloud provides a more secure IoT data architecture and development studio.

Both data and metadata are critical components of IoT systems. Metadata is data about data, and it makes it easy to organize and catalog IoT data; it provides data in context. Metadata helps devices, systems, and so on with what information to use, when to use and how to use it. Metadata helps to protect legacy hardware and software. As IoT evolves and new devices come into play, metadata can help to archive and protect the future accessibility of legacy hardware and software by ensuring that new hardware and software can still communicate with their legacy counterparts, and this also helps to overcome interoperability issues.

Given all these aspects of the data management strategy, still, the current strategies and infrastructure setups will need to be fine-tuned and overhauled in order to optimize the uses of IoT data. The data management strategy also depends on the choice of platform. The platform should be able to optimize data storage and provide a better **return on investment** (**ROI**).

3.2 Benefits—from real-time insights to resource efficiency

Data is a very strategic asset for any organization, and it is critical to process and analyze this data to be able to get the right insights and information at the right time to the right people so that they can use it to arrive at optimized outcomes. And for this to happen, a comprehensive data management strategy is needed, and this strategy, if implemented properly, can bring about the following benefits:

- A typical IoT system consists of several devices. Although each of them separately might work well but when working as a system, they can behave in unexpected ways. It is not merely about collecting data from individual devices. The transferring, storing, and managing of data is necessary as it enables organizations to identify and resolve problems early on in the entire workflow in order to improve the overall performance level. Moreover, data management enables organizations to localize all important data and offers a general access point, which minimizes data movement (less data needs to be moved around, archived, or restored).
- A well-thought-out data management strategy helps to make businesses agile and helps businesses to gain real-time operational insights; it helps to understand data requirements and usage patterns of users. All these aspects can help organizations to understand how user behavior can affect the performance of their systems and products, and accordingly, they can fine-tune them. It helps to create the best-connected products, devices, and so on; it helps in product optimization. This strategy also helps to measure performance metrics.
- A robust strategy provides real-time monitoring in terms of the status of the processes and also gives out alerts in case any issues arise during the processes. Organizations need not rely on blind guesstimates anymore as they have real-time updates, and this helps them both in maintaining customer behavioral patterns and engagement history and in bringing about resource efficiency in terms of saving up on time, cost, and efforts.

- A comprehensive data management strategy can help in offering personalization to the customers. Analytics combined with machine learning and deep learning algorithms, organizations can predict customer needs, usage patterns, and so on, and in turn, use these findings to offer personalized customer experiences. According to research findings, 80% of customers are more likely to purchase products and services when organizations provide personalized experiences.

- A proper data management strategy aids in discoverability, this, in turn, leads to enhanced data quality, and it does this by ensuring there are standardization, completeness, and consistency of data.

- A great strategy helps in better predictive maintenance, especially for the manufacturing sector. It allows companies and their workers to see exactly how their machines are performing in real-time and alert them to any issues that need their immediate attention. IoT data is essential for understanding the projected wear and tear of assets and planning for maintenance and repairs accordingly. With the help of real-time monitoring, organizations can confirm whether end-users are operating their devices, products, and so on differently than anticipated. A study done by Deloitte (it is an industry-leading audit, consulting, tax, and advisory services firm) found that predictive maintenance can reduce the time required to plan maintenance by 20–50%, increase equipment uptime and availability by 10–20%, and reduce overall maintenance costs by 5–10%. An effective strategy helps to enhance product design and development (and hence end-user experience) by providing the means to understand and use metrics and patterns in order to pinpoint improvement areas in existing product versions. The strategy also allows to get better insights into how users engage with the IoT devices, products, and so on. Volume creates value, and as the volume of IoT data grows, it acquires data gravity. And this is where a sustainable strategy comes into the picture as it helps other systems and applications to use this data to generate value out of the data and to generate actionable intelligence. These systems and applications, in turn, generate even more data volume and hence gravity, and with a stable, scalable data system, organizations can glean actionable insights from this massive stream of data.

Figure 3.1 is a pictorial depiction of the various benefits derived from IoT data management strategy.

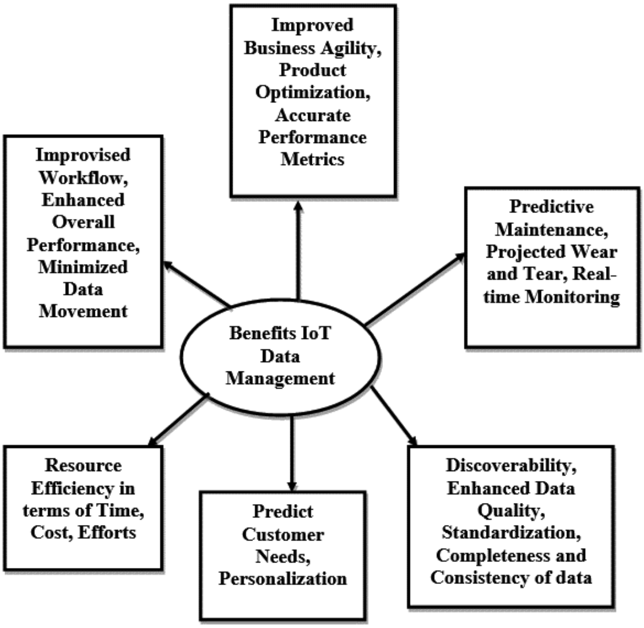

Improved Business Agility, Product Optimization, Accurate Performance Metrics
Improvised Workflow, Enhanced Overall Performance, Minimized Data Movement
Predictive Maintenance, Projected Wear and Tear, Real-time Monitoring
Benefits IoT Data Management
Resource Efficiency in terms of Time, Cost, Efforts
Predict Customer Needs, Personalization
Discoverability, Enhanced Data Quality, Standardization, Completeness and Consistency of data

***Figure 3.1**: IoT Data management benefits*

3.3 Procedures—building the IoT data pipeline

To take full advantage of the available data for real-time data analytics, an organization must adopt a strategy that encompasses the following key aspects of IoT data management; it is called an IoT data pipeline. It is a technology stack that involves multidisciplinary approaches, experts, tools, and so on for handling data in terms of collection, aggregation, transformation, and analysis. It is always wise for companies to spend quality time in researching vendors, protocols, platforms, and tools before making big choices and decisions related to the IoT data pipeline.

The previous versions of a data pipeline were about moving data from relational databases/data sources into a data warehouse; it was about dealing with structured data. Modern-day data pipelines can not only handle both structured and unstructured data from a wide spectrum of data sources (message queues, devices, apps, and so on) but are also dynamic in nature as they deal with the issues of processing and speed. Choosing the right tools needed for streamlining the IoT pipeline in order to match needs is critical for both short- and long-term success.

It is about what kind of data to collect, how to collect it, and from where to collect it, and thereafter all these following procedures help to combine, parse, validate, load, and more this data in ways that help organizations to use it for their benefits.

1. **Ingestion**: It is the first step in building the IoT data pipeline, and it is the backbone of the analytics architecture, wherein it involves moving unstructured data from where it has originated coming in at different speeds and formats (data sources could be databases, spreadsheets, and more) into a system where it can be stored, processed and analyzed. Data must be ingested before it can be digested. It can happen through the creation of new data values, data captured through devices, and more, and this ingestion process can be done in various modes such as continuous, real-time, batch, and so on.

   Data is prioritized and categorized, individual files are validated, and then routing data items to the correct destination occurs. And all these aspects make data flow smoothly through the entire IoT data pipeline.

   It involves procuring data from sources such as devices, data file uploads, web logs, and so on, and then transporting them into a data store, data warehouse, and others for further processing. With so much of data coming in, it needs to be ingested in a streamlined manner, either in batches or in real-time/stream processing. For batch processing, it is done based on a schedule or on activation of a certain condition. In real-time processing, data is sourced, processed, and loaded as soon it is created by the ingestion layer.

2. **Integration**: The IoT setup generates and transmits a huge amount of data that requires a stable and reliable infrastructure to handle this deluge of data. In traditional integration of the extract, transform, and load model, data is obtained from one framework. But in IoT, there are several frameworks involved. Hence, the new model of integration is about subscribe,

transform, and publish. Here, the integration supports a data feed from the gadgets, implements business rationale against the approaching data, provides enrichment, and afterward distributes the outcome to an enterprise framework.

For companies where the volume of data increases at breakneck speed, integrating data coming from various data sources at the edge becomes a must-have in the pipeline. It is to do with real-time processing of operational data, secure integration within an IoT setup so as to enable organizations to harvest, share and manage data across the whole IoT network.

3. **Storage**: According to the research firm Mordor Intelligence's "*IoT Data Management Market–Growth, Trends and Forecast (2020-2025)*" report, "*Organizations average 30 percent data growth year-over-year as a result of their rapidly expanding IoT infrastructure*." These statistics clearly show that organizations cannot merely rely on the cloud due to several bottlenecks such as cyber-attacks, latency, and so on.

   Moreover, organizations also need to categorize data into what data is needed and what data is not needed. Organizations will need to keep their data closer to the devices, at the edge, especially when a large volume of data has to be tackled. All these implications need to be taken into consideration in order to store a large amount of data efficiently.

   A data lake is also a good option for storage, but several factors need to be studied before using this option. Proper data lake management and stream processing measures need to be in place, or else just dumping data into a data lake without proper management can lead to a data swamp. For long-term analytics, investment in a data warehouse is a prudent choice. All these aspects need to be able to answer questions such as how structured and/or unstructured data will be stored, how will the data be kept secure, and so on.

Another critical aspect of data storage is archival. Archival is the copying of data to a place where it is stored, in case it is needed again in an active production environment; it protects older data that is not needed for everyday operations.

4. **Prepare**: The advantages of IoT data can only be realized when proper data preparation approaches are in place. Organizations must provide their teams with proper data preparation platforms that can tackle the large volume and complexity of IoT data, as well as understand how this data will be used with other sources across the organization. By adopting intelligent data preparation solutions, the complex universe of IoT and big data can be made manageable.

5. **Discover**: This sub-phase helps to pinpoint potentially useful data along with the relevant information about the data (metadata). It also captures the current state of the data lifecycle, dependent business processes, and so on.

6. **Analytics and advanced analytics**: For both real-time and historical data is another critical component for having an optimized data management strategy. IoT systems and data remain intrinsically linked together. No matter how sophisticated or self-driven an Enterprise Business Intelligence system is, business stakeholders and users can never extract any value from their analytics or advanced analytics systems unless the data they are using is clean, well-governed, value-oriented, and secure. This is the stage where data is translated into value.

Figure 3.2 is a pictorial depiction of the procedures needed to build the IoT data pipeline.

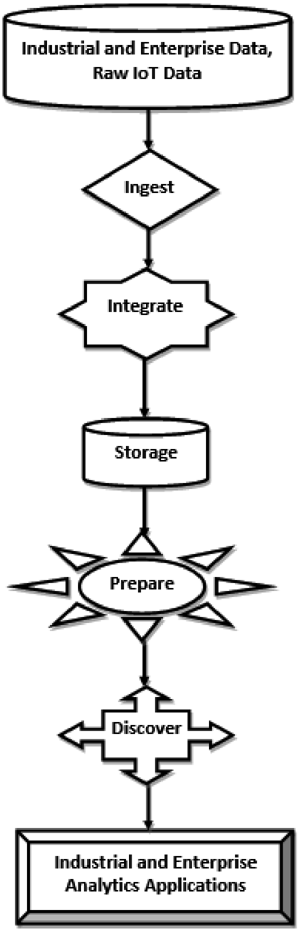


***Figure 3.2**: Building the data pipeline procedures*

Spotlight
Analytics and advanced analytics tools allow organizations to make effective use of their data sets by helping to study various sets of data, managing large volumes of data to derive relevant patterns, statistics, trends, and so on, helping organizations to gain insights into customer preferences, expectations, and more, which then can be used to generate revenue streams and make improvements in products, devices, services, and so on.

3.4 Practices—from business goals to data protection

Business goals such as enhancing sales efficiency, creating customer loyalty, and so on are the starting point for any organization. Using data to meet various business goals is quite common as a practice. This helps organizations to identify the most important data sets and decide on how they need to be dealt with and what technology will be needed to do this. Smaller, simpler, and more stable data sets are the key to success.

Another key practice is data governance. The main aim of data governance is to provide concrete answers to how an organization can determine and prioritize the benefits of data while mitigating the risks associated with it. It deals with what data can be used in what scenarios and by whom.

To ensure data quality, organizations must follow certain data management best practices. Or else, they could end up with redundant, ad-hoc, stale data that result in high costs, wastage of time and efforts, and so on.

With access to more data, it is easier to quickly determine which data will best predict an outcome; hence, simplifying this data is a good practice. Also, this data needs to be scrubbed to improve its quality, and this is why a proper data management strategy is a must. This enriched data, in turn, helps to have optimized practices related to analytics and advanced analytics. And all this can be made seamless with the help of metadata management as it streamlines so many aspects of the data management strategy, such as faster cycle time, enhanced data preparation, and so on.

Organizations need to check and clean data before it is used to derive any predictions, metrics, trends, and so on. All redundancies need to be taken care of. No wonder, these days, metadata management is moving from "*nice to have*" to "*must-have*" components on the data management agenda.

Scalability is another important best practice. The maximum scale-out of the IoT applications of an organization in terms of locations needs to be properly defined; only then training, infrastructure, personnel, and resources can be made available.

As per the study conducted by Unit 42 and Palo Alto Networks (a security consulting organization that provides resources to create an intelligence-driven, response-ready organization), a striking 83% of medical imaging devices run unsupported (i.e., insecure) operating systems. Such research findings indicate IoT setups are highly vulnerable to cyber-attacks. Solid practices such as access management, network segmentation, authentication, standard public and private encryption, patching updates through a remote mechanism, and so on are needed to keep a tab on new vulnerabilities and ensure that all data points are kept secure.

Moreover, with the **General Data Protection Regulation** (**GDPR)** (is the core regulation in the **European Union** (**EU**) law on data protection and privacy) being introduced in the EU, and other nations are likely to follow suit in the near future; hence, it is crucial for organizations to follow all protocols, standards, and guidelines to ensure the data privacy and information security. It is wise to have some sort of a data protection strategy in terms of physical security, encryption, firewall, access control, and so on for how to handle potential breaches and cyber-attacks. Organizations also need to incorporate best practices published by the IoT Trust Framework, an initiative set up by the **Online Trust Alliance** (**OTA**). The OTA, in turn, is an initiative of the Internet Society and is tasked with providing advice for security best practices and increasing consumer confidence in the information technology domain.

Spotlight
These best practices are needed to achieve several goals such as data privacy, disaster recovery, data management across diverse data tiers, and so on. These practices help to correctly prepare, manage and store data, which in turn helps an organization to optimize this data and harness its power in order to achieve its business goals.

3.5 Business potential generated by data from IoT devices

The number of businesses that use IoT technologies has increased from 13% in 2014 to about 25% today. IoT data is a powerful economic driver as IoT systems cover most areas of everyday life and business. Here are the major areas of business potential and opportunities generated by data derived from IoT devices, sensors, and systems.

For organizations to be able to tap into the business potential generated by IoT data, they will need to build a scalable, secure, and agile data supply chain that can quickly gather, integrate and transform data from a variety of data sources.

- **Business opportunities**: IoT data helps to uncover new business opportunities. Due to the ubiquitous nature of digital devices, a large amount of data can be acquired. And such data can enhance the operations of sectors such as retail, logistics, medical care, and so on. Smart IoT setups help organizations to position themselves as potential business partner in the marketplace, and this also creates a favorable impression on investors and customers.
- **New capabilities**: New capabilities provided by IoT can help to predict accurately and act on IoT data collected from a variety of sources. Such accurate predictions can be used to fine-tune operations and processes in order to provide value-added services.
- **Personalization**: IoT and personalization are two sides of the same coin. As the IoT devices, sensors, and so on gathering more data from the customers, they will quickly learn the customers' likes, preferences, and dislikes and tailor their products and services to meet these parameters; hence, enhanced personalization.
- **Convenience**: An increase in connectivity means a decrease in the amount of time normally spent performing the same tasks.
- **DataOps**: Can automate data provisioning through self-service options, including processing tools such as automated data masking and obfuscation to fully integrate data into workflows for added protection and without compromising on the speed.
- **Improved monitoring**: A large variety of devices is connected to the Internet and exchange data through sensors day in, day out. This data without analysis and monitoring capabilities is useless, and this is where IoT comes into play.
- **Increased customer interaction and retention**: IoT and all its functionalities provide new ways and opportunities to increase the level of dialog and interaction with customers.

IoT helps to pinpoint data anomalies in the data collection process, which can help organizations to create appropriate response mechanisms so as to retain customers.

- IoT data can help organizations to lower their costs, improve their operational efficiency and optimize their workflows. The whole gamut of IoT devices can provide real-time data that can proactively advise of their status so organizations can schedule the maintenance before it can affect production or operation.
- IoT data analytics derived from the game-changing combination of IoT and Big Data has the potential to bring about big value and benefits. This combination is already proving its value in sectors such as manufacturing, healthcare, and so on. Data analytics insights can help to spark innovation of new products and services, facilitate scalability and growth in new markets, pinpoint and correct parameters for quality optimization, identify future trends, and many more. This duo allows organizations to analyze all types of data sets using automated tools.

Even at this current state of the IoT domain development, the advantages of IoT solutions are quite impressive and game-changing.

Figure 3.3 is a pictorial depiction of the business potential generated by IoT data.

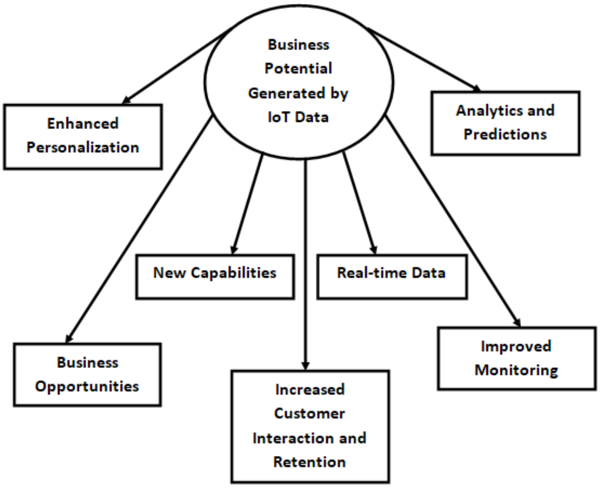

Business Potential Generated by IoT Data
Enhanced Personalization
Analytics and Predictions
New Capabilities
Real-time Data
Business Opportunities
Increased Customer Interaction and Retention
Improved Monitoring

***Figure 3.3**: Business potential generated by IoT data*

3.6 IoT solutions: AWS and Azure

Microsoft and AWS are industry players when it comes to complete IoT solutions framework and infrastructure that provide a plethora of benefits right from maximum asset utilization to real-time analytics. They provide a range of IoT offerings.

Microsoft Azure helps to build, scale and sustain IoT solutions in a highly secure manner through its three main components: IoT Central, IoT Edge, and IoT Hub. These three components help to present the most important data analytics insights to organizations in order to meet the industry needs.

- The central component is the IoT **Software as a Service** (**SaaS**) platform that builds enterprise-grade IoT applications on a secure, reliable, and scalable infrastructure. Its web user interface lets organizations to connect devices and manage a plethora of devices and their data.
- The Edge is a fully managed service that provides a simplified, cost-effective solution with low latency for Edge IoT dynamics, including analytics, image recognition, event processing, and much more. It is built on the hub.
- The Hub provides a **Platform-as-a-Services** (**PaaS**) cloud-hosted backend solution to connect, monitor, and control virtually any IoT device. It establishes simple, secure, and bidirectional communication between IoT devices and the cloud in a cost-effective manner.

  AWS IoT is an Amazon Web Services platform that gathers and analyzes data from IoT devices and connects that data to AWS cloud applications. Each device is represented as a device shadow. A device shadow maintains an identity and the last known state of a device and provides a channel to send and receive messages. Here are the main components of the AWS IoT solution:
- The AWS IoT Core forms the backbone/heart for IoT solutions suite. It connects devices to the cloud and with each other in a secure manner. It coordinates with other AWS services and components like Greengrass and IoT Analytics. It provides authentication and encryption at all points of connection.

- The Amazon FreeRTOS component is a free open source IoT-connected operating system for micro-controller-based edge devices. This is where most of the IoT data is generated. It is s an extension of the open-source FreeRTOS kernel.
- The AWS Greengrass is an open-source edge runtime and cloud service that extends IoT functionality to the edge. It uses the serverless programming model; hence, organizations can easily code, execute and test lambda code in the cloud and install them on a Greengrass core device. It provides near real-time response due to local; execution.
- The AWS IoT Device Defender is responsible for auditing the policies related to the IoT devices and monitoring all devices for anomaly detection and also for initiating corrective measures.
- The AWS IoT Rules specify what to do when a rule is triggered. It defines a rule/query and one or more actions to take when a message is received from a device, and then accordingly, the rules engine carries out the action/s.
- The AWS IoT Analytics is a fully managed sophisticated analytics component that easily analyzes huge volumes of IoT data. It can run analytics on massive volumes of IoT data without having to worry about all the complexities involved. It has advanced components such as Amazon SageMaker, Amazon QuickSight, and Jupyter Notebook that provide incredible insights. AWS IoT Analytics has templates to build predictive maintenance models.

3.7 Supporting components—metadata, edge computing, and more

Apart from the usual devices and data generated by these devices, metadata is yet another critical component of IoT setups in terms of data management. Metadata is a set of data that analyzes, labels, categorizes, and describes data itself and it makes it easy to organize data; it is about bringing structure to unstructured data/content.

Metadata ensures that we will be able to find data, utilize it, and also be able to preserve and re-use it in the future. It contains information about all the devices, sensors, things, and so on connected to the IoT platform. Metadata makes a data set truly valuable as it associates relevance and context to it.

Metadata represents elements such as the ID of a device, date manufactured, model, serial number, and so on. On the one hand, IoT is about connecting devices, sensors, and so on, and on the other hand, metadata is about ensuring that these connected components are working properly. Data needs to have a proper context to provide business value, and this context is provided by the metadata.

Metadata is helpful in protecting old and legacy software and hardware. Metadata can archive and protect the future accessibility of devices, thereby ensuring that new devices can still communicate with legacy devices.

With the help of metadata, a device can quickly identify a new device that tries to connect to it by looking up its metadata. Once the new device has been identified, the first device will be able to find a suitable communication protocol that is supported by both devices to exchange data. Therefore, metadata that stores all the attributes of devices, sensors, and so on is able to help IoT setups deal with the problem of interoperability.

Digital 2.0 technologies such as Machine Language, Artificial Intelligence, and so on are needed to apply the apt metadata parameters to data in order to describe data accurately in a context-aware manner. This is where **enterprise content management** (**ECM**) solutions come into play. ECM and IoT platforms enabled by Digital 2.0 technologies can easily identify any new device with the help of its metadata. Once this is done, the device can then be connected to any other devices, and data can be exchanged. Metadata can even be added to this exchanged data in order for the devices to process this data in a faster manner.

ECM helps IoT organizations to create new revenue streams throughout the content lifecycle. Moreover, it is important for organizations to remember that ECM is a versatile solution; its scope goes beyond content management to include other areas such as compliance, collaboration, security, and continuity. The rapid evolution of the technology landscape has interesting implications for the IoT ECM duo in terms of convergence of various stakeholders and new opportunities in areas such as data cloud, wearables, enterprise systems, and many more.

Spotlight
The marriage of IoT and ECM will lead to the growth of more and more connected enterprises, and this combination will enhance the capabilities of such enterprises to manage and analyze unstructured, structured data scenarios. This combination will lead to the development and deployment of novel use cases.

Edge computing is one step ahead of the cloud. Gartner (it is a technology research and consulting company) defines edge computing as *"a part of a distributed computing topology in which information processing is located close to the edge—where things and people produce or consume that information."* It is computing that is done at or near the source of the data in terms of content collection, processing, and delivery (whereas the cloud involves multiple data centers). The main aim of edge computing is to reduce network congestion and latency by keeping the traffic local. Making the entire edge computing infrastructure intelligent is where technologies such as IoT, AI, and more, come into the picture. In turn, edge computing and its advantages act as a cost-effective enabling factor for implementing new IoT use cases and initiatives. More and more new applications of IoT arising on the tech horizon continue to drive edge computing as it provides real-time computing power and reduces bandwidth requirements to a considerable degree.

The main reason why the edge has become so popular is because of its "*intelligent*" aspect, which opens up a whole new set of opportunities. The advantages of switching from "*dumb*" to "*intelligent*" edge computing architectures include reduction in cost and increase in functionality, agility, usability, scalability, and flexibility.

IoT gateway platforms are needed to centralize and preprocess the data derived from IoT devices/sensors at the edge level. In the case of edge computing, IoT analysis and response to findings becomes faster as all this is done where a data source or physical IoT device or sensor actually exists. Such platforms provide an interoperable, secure, compatible, and scalable channel for remote device management, as they have several features such as device authentication, data preprocessing, edge analytics, fault detection, timely diagnostics, and so on. The new generation of gateways is far superior and intelligent. Some of the popular platforms include Azure, AWS, and so on.

IoT benefits from having computing power closer to where a data source exists. In order for IoT data to be analyzed quickly so it can be used for rapid decision making, it needs to be analyzed at the edge, rather than transferring it back to a central location before it can be analyzed. An IoT device is a physical object that is connected to the Internet and is the source of the data being generated. An edge device is where the data is collected and processed.

IoT and edge computing can bring about a lot of advantages such as reduced data exposure, faster mitigation response, lesser security breaches, reduced bandwidth bottleneck, lesser network load, optimized performance, enhanced security measures, and so on. The biggest advantage of edge computing for IoT business applications is business continuity. As edge computing and its operations are distributed, in case some component breaks down, businesses can still continue with their operations, and in the meanwhile, the broken component can be fixed.

Apart from the main components of IoT, these supporting components are the glue that holds the entire IoT ecosystem together. Each one comes with a fair degree of interdependence on the other building blocks too in order to put up a brilliant IoT show. It is all about managing the dynamic data lifecycle from inception to disposal and everything in between. And this indicates the fact that organizations should always be on the lookout for newer, optimized ecosystems that will help them to keep pace with all the breakneck developments.

3.8 Conclusion

In this chapter, we discussed the deeper dynamics of IoT data management strategy so as to reduce the impact of cyber risk vectors. It covered topics such as practices and procedures, business potential generated data from IoT devices, analytics in terms of Microsoft Azure and Amazon Web Services, and metadata, edge computing, and more. This chapter sets the stage for the upcoming chapter that covers critical topics such as various IoT security, interoperability, and privacy issues and how they are related to various aspects such as trust levels, risk profiles, usability expectations, and so on.

3.9 Questions for reflection

1. Why is IoT data management important?
2. What is an IoT data pipeline?
3. Identify some of the best practices of data management?
4. Describe the different components of IoT data management?
5. What is a data recovery plan/strategy?
6. What are the challenges involved in designing a security framework?
7. What will be the expected rate of data growth over the next five years?
8. Which industries can benefit from IoT data?

Chapter 4

IoT Security, Privacy and Interoperability: What, Why, How, and What Next

IoT security and privacy are about a set of best practices, protocols, techniques, methods, and tools of protection that keeps IoT projects, resources, and solutions safe and secure and makes sure that the integrity, availability, and confidentiality of IoT projects and solutions is kept intact by minimizing the degree of impact of cyberterrorism and cybercrime.

Spotlight
IoT systems and devices not only pose a major security concern but also a major privacy concern, as these systems and devices collect a lot of personal data such as user location, user identity, and so on. Day by day, IoT is saturating the environment with smart things; hence, with more risks too.

IoT interoperability is the ability of components, devices, systems, applications, and networks to operate in conjunction (regardless of their technical or manufacturer specifications) in order to have seamless, coordinated, and secure connectivity and communication. For this workflow to be glitch-free, security and privacy are a must-have. Only then interoperability can improve the delivery of the right data at the right time to the right resources. IoT interoperability is closely linked to security vulnerabilities.

In an independent survey from IOActive (it is known for reporting high severity security vulnerabilities in a variety of products), it was found that nearly half (47%) of all respondents distrust the security in IoT devices. In a comprehensive study conducted by *Forescout Research Labs* (it is an industry leader in providing an active defense for the Enterprise of Things) where it analyzed data from over 8 million devices, it was found that smart buildings, medical devices, networking equipment, and VoIP phones represent the riskiest IoT device groups and 6 of the top 10 riskiest IoT device types fall into the categories of medical devices and networking equipment.

An example of a very malicious attack was the WannaCry ransomware attack on the **National Health Service** (**NHS**) (is the umbrella term for the publicly funded healthcare systems of the United Kingdom) in May 2017, which affected MRI scanners, operation theatre equipment, and so on, thereby putting many lives at risk. Apart from this, this attack caused a great deal of financial loss to the NHS; a total of £92 million through services lost during the attack and IT costs in the aftermath. Such attacks show that cybercriminals, through their malicious means, can initiate malicious instructions to endanger a patient's life.

A 2019 survey done by the Internet Society in countries such as the UK, France, and the USA revealed that 63% of consumers find connected devices "*creepy*." This goes to show that IoT security is a critical component of the IoT ecosystem. According to Gartner (it is a technology research and consulting company, over 80% of organizations have implemented IoT devices, whereas 20% have detected IoT security attacks within the last three years.

According to the survey conducted by the **Economist Intelligence Unit** (**EIU**) (which is the research and analysis division of Economist Group providing forecasting and advisory services through research and analysis) on 1,600 consumers in eight countries, it showed that 92% of global consumers want to control the types of personal information that organizations automatically collect about them. The same percentage wants to increase punishments for organizations that violate consumer privacy.

As IoT becomes more ubiquitous, nearly every sensor, device, and so on will have the ability to interact with other components and the Internet to some degree or the other. If best practices related to security and privacy are not implemented properly, then authorized customers/users can face a gamut of issues such as intruders gaining access to IoT sensors, devices, perform unauthorized surveillance and monitoring, and hence, harassment, and so on.

Spotlight
According to McKinsey & Company (it is a management consulting firm that advises on strategic management to corporations, governments, and other organizations), "Interoperability has the potential to unlock more than $4 trillion per year in potential economic impact from IoT use by 2025."

Structure

This chapter will cover the following topics:

- What are security, privacy, and interoperability
- Importance of security, privacy, and interoperability measures
- Methods, tools, and measures for improving security, privacy, and interoperability
- Future direction of security, privacy, and interoperability dynamics

Objective

After studying this chapter, you will be able to:

- Apply the concepts of security, privacy, and interoperability
- Pinpoint the gaps in the current security, privacy, and interoperability frameworks and then use the measures mentioned in this chapter to close these gaps
- Understand what are the possible future developments that can occur in the security, privacy, and interoperability dynamics

4.1 Measures and their importance

Experts at Seagate (it provides consumers and businesses with data storage solutions to create, share, and preserve digital content) and

International Data Corporation (it is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets) predicts that by 2025, IoT will produce an insane amount of data that is predicted to grow to 79.4 zettabytes.

Spotlight
Security and privacy, at times, are contradictory to interoperability. Gartner identified interoperability as one of the top three challenges preventing IoT from reaching its full potential. But when more organizations begin to incorporate more and more security and privacy measures, they are able to offer more interoperable systems. All these three aspects need to be dealt with early on in the project/device life cycle.

Existing interoperability frameworks have more to do with corporate concentration and monopoly over data; the big giants have more control over data than the users who actually own the data, and these big players generally only pretend to act as stewards of user security privacy. New interoperability frameworks that are user-centric in nature need to be introduced that support more legally protected data. Such new frameworks have the potential to improve the privacy of users and give more power to users to determine when, how, where, and by whom their data can be used.

There is a thin line between the balance of interoperability and privacy; too much of interoperability can disrupt this balance as there will be new ways and interfaces of sharing user data, and hence, more privacy risks will arise. Optimized interoperability opens up space for developing privacy policies that are democratically designed and implemented for the users.

Figure 4.1 is a pictorial depiction of a generic IoT security and privacy model.

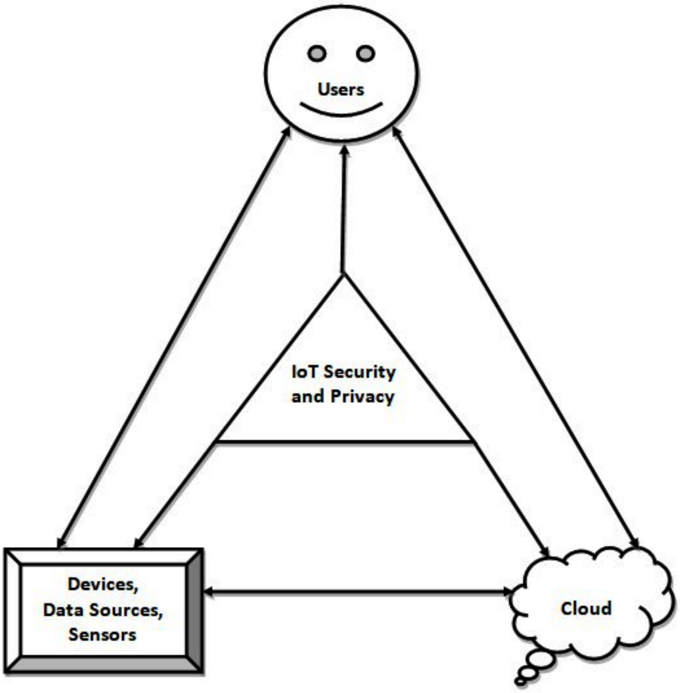


***Figure 4.1**: Generic IoT security and privacy model*

In a typical generic model of IoT security and privacy, as shown in *figure 4.1*, there are only a few layers of protection; these will not be able to deal with cutting-edge scenarios of attack/disruption. New layers like edge and fog need to be developed and added to this generic model, and existing layers of cloud, data sources, cloud, and users need to be enhanced and fine-tuned in order to boost the maturity and robustness of IoT security and privacy. Edge and fog measures are needed to bring about multi-faceted secure authentication and visibility. As devices move from centralized architectures to the far ends of a network, traditional security and privacy measures can become less relevant; hence, edge- and fog-related measures are needed. *Figure 4.2* includes additional layers of the IoT security and privacy model.

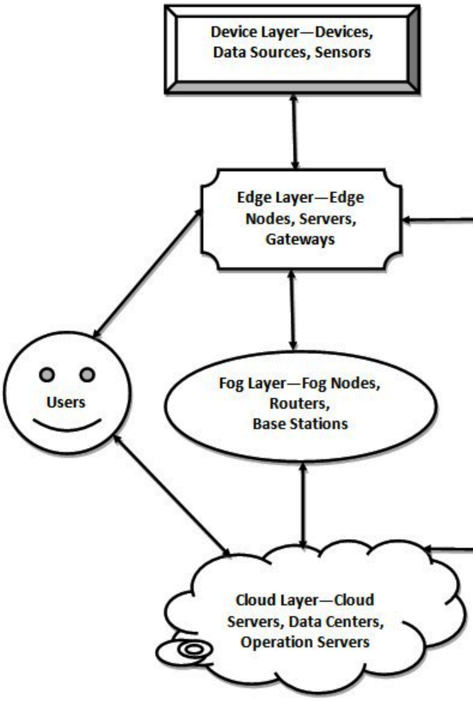

Device Layer—Devices, Data Sources, Sensors
Edge Layer—Edge Nodes, Servers, Gateways
Users
Fog Layer—Fog Nodes, Routers, Base Stations
Cloud Layer—Cloud Servers, Data Centers, Operation Servers

***Figure 4.2**: Upgraded IoT security and privacy model*

As no single technology can deliver a complete, end-to-end IoT solution on its own, this leads to a lacuna of having a uniform code of security and privacy. The interoperability of devices is not only limited in terms of functionality but also in terms of security and privacy measures. The core aspects of interoperability, such as networking, connectivity, and so on, are not adequately supported by security and privacy measures.

Many IoT devices like sensors are designed and development for deployment on a massive scale; hence, they open the door to the large attack surface. Such scenarios need to be dealt with utmost care and caution. Attack surface refers to the vulnerabilities in an IoT system that can be exploited by cybercriminals. Apart from of IoT devices, other aspects of the IoT system that are susceptible include APIs, web interfaces, cloud interfaces, mobile interfaces, and more. Currently, we are grappling with highly orchestrated cybercrimes, which are increasing in scale and scope day by day.

It is observed many IoT devices send data in clear text rather than in an encrypted form. Such a data exchange format is highly susceptible to attacks. Hence, it is of utmost importance to build up the trust factor in IoT solutions. Moreover, IoT devices, actuators, sensors, and so on generate a huge amount of data and hence more entry points for cybercriminals and attackers. As per the findings of the Federal Trade Commission report *"Internet of Things: Privacy & Security in a Connected World,"* fewer than 10,000 households can generate 150 million discrete data points every day. This creates more entry points for cybercriminals and hackers and leaves sensitive data vulnerable to severe attacks.

There are no standard security frameworks and privacy policy checklists available for IoT organizations to follow. Another important aspect that needs to be taken care of is that of increasing user awareness around these aspects.

Attackers and hackers can literally use unprotected devices, sensors, and so on to hack an office, a home, or any other setup or perform corporate spying. As IoT security and privacy breaches can lead to a direct loss of life; hence, protection related to it is a little different than the traditional systems of security and privacy protection. IoT systems and devices transcend the traditional network perimeter; they are all over the place. IoT devices do not operate in isolation; they are linked to the Internet, smartphones, the cloud, and so on. All these interfaces, most of the time, provide insecure setups.

Building trust in IoT-connected devices is very critical as this trust level directly impacts the perceptions of customers towards IoT. Trust is a critical component to realize the full potential of the IoT. Apart from building trust around factors such as social impact, environmental impact, and many more, IoT needs to focus on security, privacy, and interoperability too.

AT&T's (it is a leading telecommunications company and the largest provider of mobile telephone services in the USA) Cybersecurity Insights Report surveyed more than 5,000 organizations across the globe and found that 85% of enterprises are in the process of or intend to deploy IoT devices. Yet a mere 10% of those surveyed feel confident that they could secure those devices against hackers. Such studies and surveys show a low degree of IoT-security-driven solutions. It cannot be an afterthought, or else there will be such a deep impact in terms of financial, legal, practical, and business will aspects of the corporate world. Unprotected systems can easily help cybercriminals to profile, track, identify, and then harass users.

Spotlight
IoT business cases have wide spectrum applications, and due to this fact, the cybercriminals who attack these kinds of setups have unique motivations and methods for their attacks. Hence, critical setups such as nuclear plants, power grids, hospitals, and others, are highly susceptible to such malicious attacks because of the high potential loss of life involved. Such risks make it all the more important for organizations to take the aspect of security and privacy very seriously.

5G technology (the fifth-generation wireless technology that focuses on delivering higher multi-gigabits-per-second peak data speeds) plays a critical role in the IoT dynamics and its interconnectivity aspect. 5G operates on short-wavelength, which requires major infrastructural changes in terms of more towers and stations to cover the same area than other wireless technologies. This new setup opens up new doors for threats and breaches, and it is essential for the IoT industry to understand this new spectrum of security risks and implement potential solutions in regards to the 5G dynamics.

Hardware-level security is very important as most cybercriminals and hackers often buy IoT devices and then reverse engineer them to study their attack entry points and vulnerabilities and what kind of sensitive data can be tampered with. It is also useful because software can be easily compromised with malicious code injection. Apart from per-device security, complete network solutions are a major added benefit.

Furthermore, there is no proper global ecosystem or international standards and regulations as far as IoT security and privacy measures are concerned. This lack of universal IoT security and privacy standards facilitates IoT organizations, manufacturers, and vendors to overlook project, device, user, and consumer security and privacy measures.

Cybercriminals and hackers can compromise all kinds of cameras and change their settings, or they can access motion sensors embedded in smart devices to steal digital data. In 2016, a botnet called *Mirai* used IoT devices to launch distributed denial-of-service (DDoS is one of the most powerful attacks on resources; it overloads the servers, applications, networks, and so on by flooding them with malicious requests) attacks against organizations such as OVH (it is cloud computing company which offers VPS, dedicated servers and other web services), DynDNS provider and several others. This was the first time ever in the history of the IoT landscape where devices were used as a means of attack propagation.

After the Mirai attack, several new-generation malware has come into existence. Some examples include Mozi botnet, Muhstik botnet, HEH botnet, Reaper botnet, Xbash botnet, and so on. IoT botnet is a malware that targets a group of smart devices, servers, appliances, Internet-connected devices, and routers that have fallen into the hands of miscreants and used by them to launch DDoS attacks.

Worm wars are a big menace running amok across the IoT threat landscape. The growing number of IoT botnet malware families and their variants, if not handled in a prudent, proactive manner, will continue to develop and implement more complex malware, which will be extremely difficult to take down.

Privacy, transparency, control, and trust go hand in hand. Users are ready to share and disclose their personal data with organizations, vendors, and third parties, only when they trust and feel assured that it will not fall in the wrong hands. Users need to be informed about when and how their data is collected, and where it has gone, and for how long it will be kept. Users need to be given control over the data they share. This means they should be able to activate and mute devices in their home, office, or on their bodies and also be able to control who can access and analyze this data.

Privacy policies need to be shared with the users upfront. But again, there is a downside to this aspect of policies, most users do not read the privacy policies, and even if they try to read, they fail to understand the policy terms and conditions as the language used is legal jargon, which is unintelligible to the average user. Moreover, extra care should be taken to deal with business scenarios for which user data is collected and used when users have no choice as there is no opt-out option. Such examples include business scenarios like smart meters.

Merely device interoperability will not work to unlock the complete value potential of IoT; rather, it is data interoperability that will do this magic. As per industry experts, up to 60% of the value that IoT systems hold is currently locked by a lack of data interoperability.

The sooner data interoperability comes to its completion, the sooner the IoT will value be unleashed.

Security, privacy, and interoperability need to go hand in hand—only then transparent user-oriented/centric interfaces and systems can be developed and implemented. With the increase in more open infrastructure, where external sources of data are closely tied into organizational processes to bring better interoperability, security and privacy measures must upgrade themselves as well in order to match up with these new interoperability frameworks.

Table 4.1 gives a tabular recap of IoT security issues, privacy issues, and interoperability issues.

Security issues	Privacy issues	Interoperability issues
No standard comprehensive security frameworks.	No standard comprehensive privacy checklists.	Non-uniformity of interoperability protocols.
Lack of trust from the customers.	Lack of trust from the customers.	Lack of trust from the customers.
The core aspects of interoperability, such as networking, connectivity, and so on, are not adequately supported by security and privacy measures.	The core aspects of interoperability, such as networking, connectivity, and so on, are not adequately supported by security and privacy measures.	Existing interoperability frameworks are more to do with corporate concentration and monopoly over data; hence, they give rise to more security threats and privacy risks.
Security and privacy breaches can lead to a direct loss of life.	Security and privacy breaches can lead to a direct loss of life.	Interoperability can lead to user's losing control over their data and hence its security and privacy.

Table 4.1*: IoT security, privacy, and interoperability challenges*

All these aspects and concerns (hopefully) should drive better comprehensive, well-thought-out laws and regulations.

4.2 How—methods, tools, and measures

Introducing IoT security during the design phase is of utmost importance; including this critical component from the ground up is of utmost importance. To begin with, IoT organizations need to educate their employees and users on how to manage and change default passwords and subsequent ones based on standard industry digital identity guidelines in order to minimize malware, device spoofing, ransomware, brute force, impersonation, and hacking. Changes should not allow the use of weak passwords, and hard-coded and embedded credentials need to be avoided. Biometric authentication, two-factor authentication, and many more can make sure that only authorized users can access resources. This action should be implemented for each of their IoT devices. In 2020, ZDNet (it is a business technology news website) shared how a hacker published a list of Telnet credentials for 515,000 IoT devices, routers, and servers. This password dump was obtained by using preset default usernames and passwords.

Zero trust approaches are needed to improve the trust level of customers. Such approaches require that security starts with the user, and all the plethora of tools, measures, and methods discussed in this chapter need to be implemented right from device identification to proactive monitoring. Continuous network monitoring is a must, and micro-segmenting devices into proper zones are required to reduce the attack blast radius. Each segment/zone will have its own users, roles, access control lists, and responsibilities.

Zero trust is based on the principles of granular access policies, continuous monitoring, never trust, always verify, and the least number of privileges. Zero trust is not about one-time security; it is a continuous, dynamic phenomenon. Zero trust emphasizes on the tenet of "*all devices matter*", and hence, developing a comprehensive risk profile of all devices is critical. It is always wise to isolate data and networks from existing systems in order to reduce the impact of an attack.

As far as interoperability is concerned, organizations need to test their devices across all modes of operation, specifically, how security and privacy measures are used in terms of their degree of effective implementation; as interoperability is a fragmented environment, severe security loopholes can occur. When it comes to privacy and interoperability, competitive compatibility is a critical component; competitive compatibility means the smaller players can interoperate with bigger players without having to seek their permission or break laws or negotiate with them on lopsided terms and conditions. There is a thin line regarding the balance between compatibility and privacy, and when this balance is thrown off, i.e., when user data is misused, organizations should either use legal mandates to shut down the interoperability interface or limit its services by revoking API keys or they can also remove it completely.

For added security and privacy, the passwords can be protected by a password vault. In addition, the passwords need to be changed on a timely basis. Organizations need to include security and privacy measures as a part of their business agenda. Users also need to use a trusted **virtual private network** (**VPN**) (which is used for transmitting sensitive data through a strongly encrypted tunnel), which helps to secure the data transmitted on their public or home Wi-Fi.

Access control frameworks and policies like **role-based access control** (**RBAC)** (is a security strategy approach where organizations grant their employees varying levels of access based on their roles and responsibilities) mandatory control access (MAC is a security approach of limiting access to resources based on user clearance level and data confidentiality) and **access control list** (**ACL)** (is a set of rules that grant or deny access to certain digital environments; ACL is a network traffic filter that can control incoming or outgoing traffic need to be in place in order to ensure that only valid users are allowed to access the IoT devices, especially when devices are operating in a distributed setting, directly connected to the Internet.

There are four main types of interoperability: semantic, legal, syntactical, and semantic. Semantic interoperability deals with the interpretation of data; it is about deriving meaning from structured data in a contextual manner. Legal interoperability deals with laws, agreements, and policies needed to facilitate the seamless exchange of data. Syntactical interoperability deals with well-defined syntax and formats for the data that is exchanged. Semantic interoperability is about ensuring systems interact with each other in an unambiguous manner.

Up-gradation of skills, user guidelines, training workshops, orientation sessions, and regular newsletters need to be carried out by organizations to ensure that both their employees and end-users are well abreast of the latest trends, patterns, and threats of the IoT landscape. Moreover, organizations should work on ways of incorporating automated secure updates and patches in their IoT devices.

Security and privacy measures, tools, methods, and protocols need to be incorporated throughout each and every stage of the development of devices. The principle of "*Privacy by Design*" needs to be incorporated in the IoT landscape, which is currently a missing component in most organizations. Moreover, enabling anywhere anytime access to only critical functions needs to be allowed. Users should disconnect devices when they are not needed, and they should never leave their smart devices unattended in public places and crowded spaces, and should also turn off Bluetooth and Wi-Fi as many times organizations allow automatic sharing of data with other users sharing the same space.

Organizations need to provide transparency in their privacy policies, and this can be made possible when users demand for this. In fact, the best practice for this aspect has a three-tiered approach, a layered approach: machine-readable policy, user-readable policy, and legal policy. When companies collect user data, they must take responsibility for protecting their users and their data or else they should not collect the data at all. The IoT ecosystem needs to have legal terms and conditions for organizations as well so that they are legally bound to fulfill all the promises they make to the customers.

A simple summary for the users to understand is what the user-readable policy is all about. When it comes to legal policy, it is the actual legal code used by lawyers and judges. The code understood by technologies, applications, and search engines is the machine-readable format that they interpret to access only the data that the users allow. This multi-layered approach is a must-have for developing a comprehensive IoT security and privacy ecosystem.

Spotlight

Many times, IoT systems and organizations sell user data to various third parties, thereby violating security and privacy rights and also regulatory and legal compliance terms and conditions. In such cases, strict legal action should be taken against such organizations, but in reality, there is no such system of check and control in place.

Public key infrastructure authentication (**PKI**) and cloud security are also needed to handle the large surface of security threats associated with IoT setups. PKI is a security framework that uses certificates and a pair of keys to carry out asymmetric encryption and decryption of confidential data. PKI offers secure encryption and decryption of communication over the Internet using digital certificates; this is particularly helpful to have secure transactions in case of clear text communication.

Proprietary encryption protocols need to be avoided, and instead, organizations need to implement standard protocols such as Transport Layer Security, OS4I, Zigbee, Secure Sockets Layer, and so on.

The virtual private network is a great method to minimize the incidence of compromise of devices, especially smart home-based devices. By enabling the connection to these devices through a VPN, hackers can be prevented from accessing a user's personal data such as phone, credit card information, address, and so on.

Several IoT devices have outdated operating systems running on them. Such devices need to be prevented from connecting with the outside world, outside of the premises of organizations. Not all these devices are high-end in nature; hence, it is difficult to integrate them with sophisticated security protection software. Most IoT devices are single-purpose systems built with low processing power. Organizations need to upgrade such IoT devices or completely replace them with the latest ones that have the computing power, memory, and speed to integrate with security software.

In order to minimize attacks through vendor systems, it is wise for organizations to set a limit on the number of vendors. Internal employees should be trained to keep a tab on vendor systems and remote access solutions. Vendors and manufacturers need to issue patches for new vulnerabilities and share them with their users, and users, in turn, need to visit the website of manufactures and vendors on a regular basis to download and apply these patches.

Networks are highly susceptible to a huge spectrum of cyber risks as they consist of both digital devices and physical assets, leading to not only user privacy breaches but also loss of intellectual property and trade secrets. And this leads to more number of access/entry points; open ports can be used to launch **denial-of-service** (**DoS**) attacks. Hence, point-to-point management of such entry points/

ports is of utmost importance. Port management methods such as intrusion detection, firewalls, port forwarding, and so on are critical for keeping IoT networks intact. Whenever ports are not in use, it is always wise to deactivate them.

Application programming interface (API) (is a set of functions and procedures that allows two applications to talk to each other) measures such as certificates, quotas, and tokens are a great way to secure IoT devices. For example, API-as-a-service is a great example. Quite a few organizations host their APIs on internal servers, and this approach is not fool-proof, especially when organizations do not give much attention to the security and privacy aspects. Hacked or broken APIs can lead to malicious cyber-attacks on data transfer and services associated with APIs. More secure options like API gateways and API-as-a-service help to authenticate traffic as well as control and analyze how the APIs are used.

Organizations need to store as much data as possible on the device itself and only send absolutely necessary data over the network or to the cloud. Whenever data is not needed, organizations need to stop gathering it.

IoT Forensics deals with the complete investigation process of crimes related to IoT; it is done with the identification, collection, assessment, and analysis, documenting and reporting digital evidence collected from various sources in a cyber-crime event. It helps to pinpoint compromises and provides root cause analysis to organizations, vendors, suppliers, and manufacturers, which enhances the security and privacy aspects of data protection.

Network Access Control (**NAC**) is a centralized solution that consists of a network switch and wireless assimilations and is designed to enhance security and privacy measures for business network protection. NAC helps to monitor and detect devices through optimized inventory management and pinpoints problematic connections within the network. A comprehensive NAC solution is able to identify all devices that are connected to a network and also manages to profile these devices to ensure that they are not compromised.

Having multi-layer security at both the software and hardware levels will go a long way in minimizing the impact of botnets. Network-level security is also a must-have, especially in cases where device-level protection is not possible. IoT devices should be connected in an environment where firewalls are present. Whenever the back-end services communicate with an IoT device, organizations should implement measures that will be able to differentiate between a valid endpoint and a clone by forcing the endpoint to authenticate itself.

Cryptography is a powerful way of tackling many of the IoT security and privacy concerns. Integrity, accessibility, and confidentiality of sensitive data and device firmware can be maintained by end-to-end encrypting and decrypting it and thereby help to prevent malicious forms of attacks such as man-in-the-middle attacks, corporate spying, and many more. It should be made an integral component of IoT devices and projects. A digital signature generated by a cryptographic algorithm is an added layer of protection.

There are several advancements in cryptography, and one of the main ones is lightweight cryptography which has a smaller footprint, and hence, better operational efficiency. Industry experts endorse this type as it works well for IoT devices as many of these devices operate in a constrained environment in terms of low processing power and low storage capacity. Lightweight cryptography is all about combining minimum computing power devices with a reasonably advanced level of security.

Organizations and users should protect IoT devices in secure spaces, probably coupled with intrusion detection alarm systems. Organizations should ensure that devices have a strong fail open mechanism. Organizations need to have built-in remote monitoring and device locking in case an attack occurs. Organizations should select commercial providers who can provide automated and/or default-on responses to attacks.

There is an urgent need to spread awareness of cybersecurity industry standards and best practices to enable all the stakeholders such as service providers, governance agencies, device developers, and so on to enhance the adoption rate of IoT worldwide.

Table 4.2 provides a tabular recap of methods, tools, and measures and their short description for enhancing IoT security, privacy, and interoperability.

Methods, tools, and more	Short description
Privacy by design	Security and privacy measures, tools, methods, and protocols need to be incorporated throughout each and every stage of the development of devices.
Password protection	IoT organizations need to educate their employees and users on how to manage and change default passwords and subsequent ones based on standard industry digital identity guidelines in order to minimize malware, device spoofing, ransomware, brute forcing, impersonation, and hacking.
Zero trust approaches	Such approaches are needed to improve the trust level of customers. Such approaches require that security starts with the user.
Competitive compatibility	It means the smaller players can interoperate with bigger players without having to seek their permission or break laws or negotiate with them on lopsided terms and conditions.
Access control frameworks and policies	It is a network traffic filter that can control incoming or outgoing traffic need to be in place in order to ensure that only valid users are allowed to access the IoT devices, especially when devices are operating in a distributed setting, directly connected to the Internet.
A layered approach towards transparency	The best practice for this aspect has a three-tiered approach, a layered approach: machine-readable policy, user-readable policy, and legal policy.
Public key infrastructure authentication	It is a security framework that uses certificates and a pair of keys to carry out asymmetric encryption and decryption of confidential data.

Methods, tools, and more	Short description
Virtual private network	It is a great method to minimize the incidence of compromise of devices, especially smart home-based devices
Network Access Control	It helps to monitor and detect devices through optimized inventory management and pinpoints problematic connections within the network.
IoT Forensics	IoT Forensics deals with the complete investigation process of crimes related to IoT; it is done with the identification, collection, assessment, and analysis, documenting, and reporting of digital evidence collected from various sources in a cyber-crime event.
Cryptography	It is a powerful way of tackling many of the IoT security and privacy concerns. Integrity, accessibility, and confidentiality of sensitive data and device firmware can be maintained by end-to-end encrypting and decrypting it and thereby help to prevent malicious forms of attacks such as man-in-the-middle attacks, corporate spying, and many more.
Awareness of cybersecurity industry standards and best practices	This is necessary to facilitate all the stakeholders such as service providers, governance agencies, device developers, and so on to enhance the adoption rate of IoT worldwide.

***Table 4.2**: Methods, tools, and measures*

Spotlight

Security, privacy, and interoperability are not to be treated as elements that receive attention only at a particular point in time, but rather they need to evolve themselves day in, day out, as the involved organizations, devices, users, and systems do the same. Future-proofing IoT systems need to become the standard for IoT security, privacy, and interoperability.

4.3 What next—future direction

Currently, there are no global standards in terms of security and privacy frameworks and architectures. It is imperative for the IoT industry to begin work on developing comprehensive frameworks and architectures that will accommodate the deeper dynamics of the vast spectrum of stakeholders (users, tech companies, consumers, research experts, government bodies, devices, interfaces, hardware, software, operating systems, cybersecurity specialists, and antivirus companies) One of the main areas that will need a lot of research work is that of reducing mitigation time from days to hours to minutes to maybe even immediate; this will certainly be a viable future direction to take.

Protocol layers and IoT need to go hand in hand as IoT is susceptible to attacks at all layers, right from perception layer to application layer to service layer. There is a need to introduce and integrate security and privacy mechanisms at all these levels in terms of identity management systems, trust management hubs, enhanced protocols, and much more. Organizations will need to continue to work with vendors to limit the collected data to the bare minimum of what the vendor needs to operate their service; these stakeholders will need to be more transparent with their business models and focus more on using them for user data security and privacy (and not merely focusing on monetizing data).

Digital 2.0 technologies such as **Artificial Intelligence** (**AI**), Blockchain, **Machine Learning** (**ML**), and so on will be used more and more for bringing about real-time security management. Blockchain and IoT integration is a trend to watch out for as this integration will bring about tremendous improvement in security management. Blockchain combined with hardware-driven security gives the dual advantage of not only protecting users from malicious attacks but also giving data ownership back to users. Blockchain gives the users the choice to keep their data completely private or share it with other users or allow organizations to use it.

With quantum computing gaining momentum, organizations are likely to explore quantum solutions for security, privacy, and interoperability. Organizations also need to study how to deal with quantum encryption and decryption as it involves complex dynamics, which, if not comprehended completely, could potentially jeopardize many aspects of IoT security, privacy, and interoperability.

Dealing with the escalating threats will require new approaches and new technologies. Digital 2.0 technologies help to provide water-tight threat intelligence, big IoT data analytics, prediction, and protection in real-time. These technologies are about predicting an attack based on past historical data and patterns and then providing a viable solution accordingly; they are about using intrusion detection systems based on predictive analytics. For network security, ML can effectively monitor incoming and outgoing traffic to pinpoint traffic that does not fall within the established security and privacy guidelines in order to protect both the inner and outer perimeters. Moreover, as IoT devices have low storage capacity and processing power, ML can provide lightweight, less resource-demanding endpoint protection.

Although AI and ML solutions can work independently without the intervention of humans, it is still wise that some degree of intervention by humans is there; this will make the solutions more balanced. AI and ML need to be an integral part of IoT systems and not an add-on feature. This is necessary as only then organizations will be able to secure their endpoints in an optimized manner.

Spotlight
IoT stakeholders will have to realize the importance of ethics policies in all aspects: security, privacy, and interoperability.

Interoperability is all about dealing with distributed devices, but currently, the IoT interoperability standards are not comprehensive enough to handle such a dynamic. Going forward, the current centralized interoperability testing system will need to be replaced as it does not really serve the purpose, and IoT organizations will need to research on and build distributed interoperability testing systems.

Organizations and the industry will begin to focus more on protocol translation and standardization platforms that will be able to translate legacy protocols in order to communicate with proprietary IoT systems. The future focus will be all about developing the capability to communicate with an evolving protocol stack.

Given the current trajectory of IoT, context-based service composition on the fly could be a possibility, which means complex services could be added to the devices in a dynamic fashion, and this is one area that IoT interoperability experts will need to study thoroughly. Constant research regarding emerging threats will also be needed.

Going forward, standardization in terms of shared understanding of security, privacy, and interoperability dynamics is something that organizations will tend to focus on more and more. Moreover, changing governance structures will be needed to be handled by involving each and every stakeholder for building collaborative interoperable solutions. No one can operate in a silo mode. Although organizations such as Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI), Indian Standard Development Organization (SDO) OneM2M, and so on are working on this aspect at global, national, and regional levels, yet there is no universal organization established. There could be a huge possibility of such an organization coming into existence. Such a shared accountability and responsibility setup established by all stakeholders is the key to securing the future of the IoT space.

As organizations continue to perform intensive study and research the newer cyber risks arising on the technology horizon in general and on the IoT horizon in particular, they will slowly and steadily increase their acceptance and adoption index for bringing about transformative changes in their security, privacy, and interoperability frameworks. More research in the field of AI and ML is likely to be the order of the day in the near future as they have given promising proof points that demonstrate the value of their importance as an emerging IoT security solution.

Threat modeling, which is yet to be adopted on a mass scale in the IoT industry, is likely to become a major component in security and privacy frameworks for bringing about better situational awareness and more maturity. Threat modeling is a quantitative method of risk management, which helps to determine how a company would perform before a real attack occurs. It is about early pinpointing and fixing of unique potential problems and identifying resources/connections/assets that may require additional security and privacy. Automation is an important aspect to be used in order to enhance organizational security and privacy maturity, and situational awareness. It is essential for establishing a stable trust boundary with the users and for saving money and efforts by solving problems before releasing software and carrying out costly code rewriting.

More and more research work is likely to occur in the field of IoT Forensics. The industry will need to take this one step further by upgrading the existing IoT Forensics principles to state-of-the-art, adaptable forensics frameworks in order to ensure that they are capable of handling this at all levels in a multi-faceted way: device, cloud, network. There also needs to be work done on the IoT forensics tools, hardware, and software that are both affordable and reliable in their results.

IoT Forensics experts will have to develop new skills in order to keep pace or rather be one or more steps ahead in the game. They will need to indulge in extensive research and knowledge-sharing in order to thwart future attempts of weaponizing IoT devices, and this will be possible only when players and stakeholders come from a breadth of expertise and geographic spread.

Figure 4.3 is a pictorial depiction of the future direction of IoT security, privacy, and interoperability.

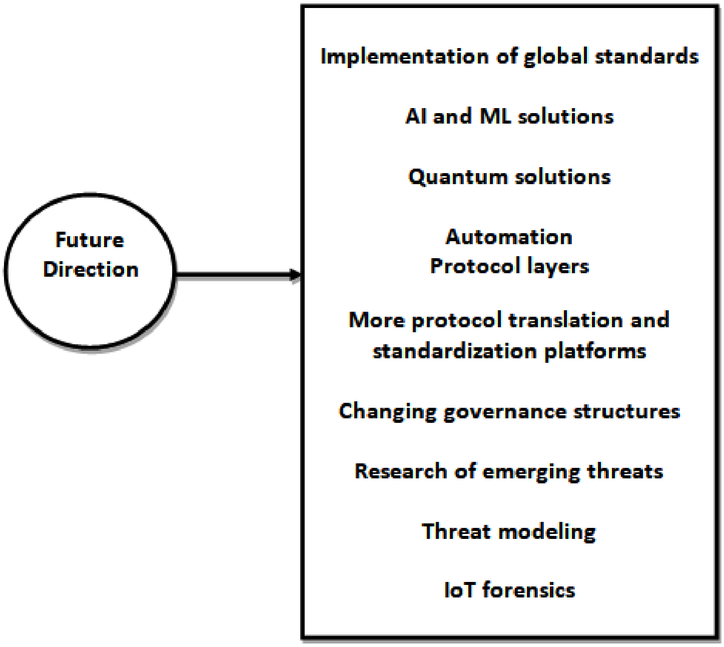

Future Direction
Implementation of global standards
AI and ML solutions
Quantum solutions
Automation
Protocol layers
More protocol translation and standardization platforms
Changing governance structures
Research of emerging threats
Threat modeling
IoT forensics

***Figure 4.3**: What next for IoT security, privacy, and interoperability*

Spotlight
The future direction will need to be all about the tenet “secure the devices now, secure the smart era of IoT business for the future”.

In essence, as the IoT domain begins to outnumber humans, it will be beyond humans alone to deal with attacks; we will need to seek help from the machines to protect themselves. The IoT domain needs to make sure that future IoT devices/systems, including smart grids, smart homes, and smart cities, are safe and secure, and care about people's privacy is given prime importance—only then new business models and additional revenue streams can be created and implemented successfully.

4.4 Conclusion

In this chapter, we covered IoT security, interoperability, and privacy issues and how they are related to various aspects such as trust levels, risk profiles, usability expectations, and much more. After reading this chapter, the readers will have gained a deep understanding of the concepts of security, privacy, and interoperability, pinpoint the gaps in the current security, privacy, and interoperability frameworks, and then use the measures mentioned in this chapter to close these gaps and be able to understand what are the possible future developments that can occur in the security, privacy, and interoperability dynamics. This chapter sets the stage for the upcoming one wherein we deal with IoT applications and use cases.

4.5 Questions for reflection

1. What needs to be done in terms of interoperability, security, and privacy in order to meet the needs of a scaling business?
2. Why interoperability is important in IoT?
3. What can be done to build autonomous and self-adapting systems in terms of security, privacy, and interoperability?
4. Describe the different components of security, privacy, and interoperability management?
5. How should organizations protect the privacy of their users with increasingly vulnerable devices, sensors, and so on?
6. How do the current developments in IoT impact the future of threat modeling?
7. What are the existing remedial measures for security management?

CHAPTER 5
Applications and Use Cases

In recent years, digital transformation in terms of IoT has emerged as a key growth driver in several business domains. Application domains have been presented by both the industry and academia. According to Libelium 2015 report, it lists 61 applications for IoT in a number of domains using different sensor boards. Of course, this number has increased over the next five years exponentially.

As per the findings shared by Meola in 2016, the application of sensors in the automotive sector has been one of the largest growth areas. In recent years, there has been a dramatic increase in investment in IoT research and development. Monitoring and controlling operational data in real-time help businesses to improve performance by tracking progress in real-time. All these statistics show that with IoT, the future is now.

Six of the top ten IoT use cases today, ranked by adoption, aim at making operations and processes intelligent and intuitive. IoT use cases help businesses to test out their product or service ideas in terms of whether they are able to tap into real-time context data to drive better decision-making, optimize the workforce, maximize returns, improve quality, and so on.

Structure

In this chapter, we will cover the following topics:

- The main application areas of IoT
- Novel use cases of IoT
- Various research study findings and statistics

Objective

After reading this chapter, you will be able to:

- Understand the main application areas of IoT
- Identify various novel use cases of IoT
- Study the various statistics related to the main application areas and use cases of IoT
- Figure out more options related to IoT applications and use cases

5.1 Applications of IoT

Combined with other technologies such as artificial intelligence, machine learning, and many more, IoT revolutionizes the way we go about and carry out our businesses. A survey conducted by KRC Research (it is a full service global public opinion research consultancy and a member of the Interpublic Group of companies) in the UK, USA, Japan, and Germany, these early adopters of IoT revealed which devices are customers more likely to use in the upcoming years. *Figure 5.1* shows the results of this survey.

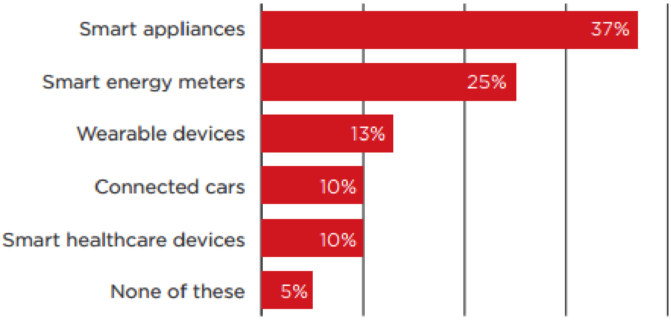


***Figure 5.1**: Devices that customers are most likely to use in the coming years (Source: GSMA Report)*

Spotlight

The current wave of IoT connectivity is going smartphones, computers, and so on; it is going towards smart homes, connected cars, smart cities, and many more domains. Both business applications and personal applications of IoT are growing at an exponential rate.

Table 5.1 shares information on the various IoT domains and their application areas.

IoT domain	Application areas
Industry	Healthcare, supply chain, marketing, retail, transport, agriculture, and many more
Wearables	Smart clothing, Smartwatches, Disability management, and many more
Environment	Disaster alert, smart water management, smart energy management, air pollution control, and many more
Society	Smart city, smart grid, smart home, smart building, smart surveillance, smart waste management, and many more
Vehicle	Vehicle condition monitoring, autonomous vehicles, driverless cars, and many more
Maintenance	Asset/machine condition monitoring, predictive analytics, anomaly detection, and many more
Media and entertainment	Content delivery, content personalization, targeted advertising, and many more
Healthcare	Health monitoring and reporting, alert systems, location service, and many more

***Table 5.1**: IoT domains and their application areas*

Table 5.2 presents the various IoT domains and their top players.

IoT domain	Top players
Autonomous vehicles	Toyota, Volvo, Tesla, Nissan, and Uber
Industrial IoT	PTC, Intel, IBM, Texas Instruments, and SAP
Data management and security	Cisco, Arm, and Calsoft,
Healthcare	CitrusBits, RisingMax, Mindbowser, and HQSoftware Lab
Retail	Qliktag, Swirl, Wise Shelf, and Gimbal
Logistics	Maersk, Dash, Chariot, and GE
Smart setups (homes, offices, grids, and so on)	Awair, RapidSOS, Helium Systems, and Notion
Predictive maintenance management	IBM, Siemens, SAP, GE, Uptake, Microsoft, Oracle, and AT&T

***Table 5.2**: Top players in various IoT domains*

IoT has numerous applications areas, and we will explore the main ones in this section.

- **Autonomous vehicles, driverless cars**: There are a large number of sensors within such vehicles to collect a wide variety of data, right from tire pressure to engine operation. Because it is human lives (and other life forms too) on the roads that we are dealing with, we need to ensure the technology has all of that it takes to ensure better safety, reliability, and precision for the passengers and pedestrians. McKinsey Global Institute (its focus is on helping leaders in the commercial, public, and social sectors develop a deeper understanding of the evolution of the global economy) predicts massive value growth for IoT—11.1 trillion US dollars annually by the year 2025.

  IoT devices, sensors, and radar lasers collect data related to the path, traffic, and how to navigate around any obstacles.

All of this data is shared between connected cars, and this data is sent to the cloud to be analyzed in order to handle all the automation dynamics such as predictive modeling, traffic congestion control, obstacle avoidance, and so on effectively. Some of the main players in this space are Ford, Honda, Uber, and Volvo.

According to Fortune (it is an American multinational business magazine), fully autonomous vehicles will not noticeably hit the market until about 2020, but it is predicted that by 2040, 95% (or 96.3 million) of new vehicles sold will be driverless.

Current driverless cars and other vehicles can only allow partial autonomy under certain predefined operating conditions. The progress of technologies involved in making autonomous vehicles also impacts the emergence of smart cities.

- **Smart cities**: Similar to smart homes, cities are now using IoT devices for various aspects of running the city. IoT systems collect data on water usage, waste management, traffic management, pollution, and so on. With the help of IoT data collection and analysis in real-time, cities will be able to make smarter decisions on where improvements are needed and which gaps need to be closed.

  The growth in demand for IoT-enabled homes and offices will lead to the development of more and more smart cities. Combining IoT devices and data with a city's infrastructure can lead to a plethora of benefits such as a decrease in traffic congestion, reduction in pollution, improvement in air quality, smart garbage collection, better urban security, and so on.

  As cities become more dependent on digital support systems, they will also become more vulnerable to cyber-attacks. Hence, smart city solutions require high-level security measures, and this is one area where IoT companies will need to gear up their efforts.

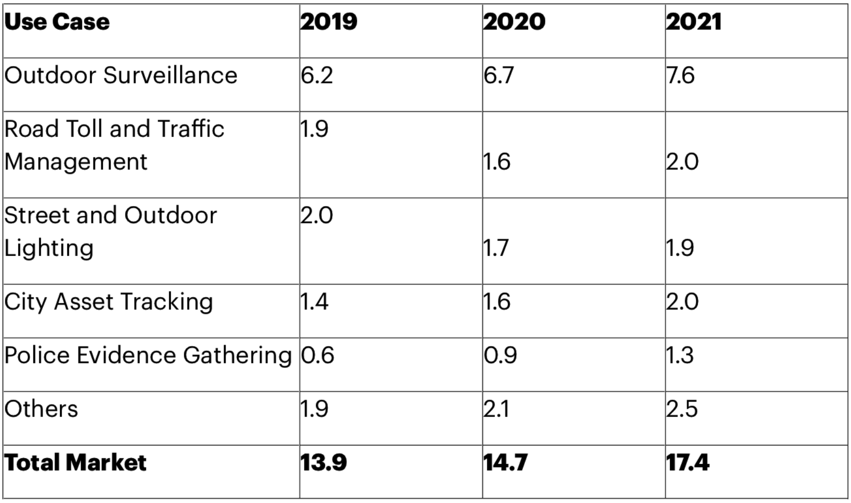
  Moreover, in recent years, the size of cities in terms of their population has been growing at a fast pace due to the migration of people from remote areas and villages to cities in search of better opportunities. As this migration continues, cities will need to optimize their existing infrastructure in order to keep up with the increasing population. Thus, smart cities supported by IoT-enabled applications and initiatives will start to become the norm.

According to IoT Analytics (it is a leading global provider of market insights and strategic business intelligence for IoT, AI, Cloud, Edge, and Industry 4.0), smart cities are prioritizing IoT technologies in a number of interesting ways. The research study focused on decision-makers from some of the world's leading smart cities. It categorized how leaders were using IoT to curb urban inefficiencies and improve the quality of life. The study found that the following areas were the top priorities (*percentages shown are the percentage of included smart cities that have deployed use cases as part of a smart city initiative*) for city governments:

- Connected public transport (74%)
- Traffic monitoring and management (72%)
- Water level/flood monitoring (72%)
- Video surveillance and analytics (72%)
- Connected streetlights (68%)
- Weather monitoring (68%)
- Air quality/pollution monitoring (68%)
- Smart metering–water (66%)
- Fire/smoke detection (66%)
- Water quality monitoring (64%)

Smart cities are directly linked to smart grids. Municipalities and cities are becoming increasingly aware of how important it is to get electricity from renewable sources, and supporting all this energy generated from renewable methods requires the smart grid.

Table 5.3 shows the estimates shared in a study conducted by Gartner that reveals the top five government IoT applications and revenue generated by each use case for the years 2019, 2020, and 2021.



Use Case	2019	2020	2021
Outdoor Surveillance	6.2	6.7	7.6
Road Toll and Traffic Management	1.9	1.6	2.0
Street and Outdoor Lighting	2.0	1.7	1.9
City Asset Tracking	1.4	1.6	2.0
Police Evidence Gathering	0.6	0.9	1.3
Others	1.9	2.1	2.5
Total Market	**13.9**	**14.7**	**17.4**

Table 5.3*: Top five government IoT applications and revenue generated (in US dollars) for several applications areas of smart cities Source: Gartner*

- **Smart homes and offices**: One of the most practical applications of IoT is smart homes. They take convenience, comfort, control, and security to the next level of performance, thereby enabling enhanced home security. Research indicates that more than 60,000 people currently search for the term "*Smart Home*" each month. Experts predict that homes will become as common as smartphones. Some of the major players in this space include Ring and Nest. There has been significant growth in the demand for smart home devices such as smart locks, personal home assistants, and many more. Some of the main players in this area are Haier, Nest, and Philips.

  IoT solutions for smart homes can help homeowners to track various temperature factors such as air quality, humidity, and so on, and also track how much electricity each device uses. All such factors can lead to better energy resources management.

  In addition to growth in consumer adoption of smart solutions driven by IoT, there has also been a surge in demand for offices. A report by British Land (it is one of the largest property development and investment companies in the UK) and Worktech Academy (it is the world's leading knowledge platform and member network exploring the future of work and workplace) of over 1000 workers, nearly a third of whom were decision-makers, found that 88% of respondents expressed a wish to control their work environment better.

- **Health**: Remote health monitoring via connected devices can save lives in the event of an emergency like an asthma attack or heart failure. With the help of protocols such as ZigBee, Wi-Fi, and so on, the healthcare industry is revolutionizing the ways in which it identifies and treats diseases. These protocols and Digital 2.0 technologies will take healthcare solutions, end-to-end connectivity, and facilities to the next level of performance. IoT-enabled healthcare devices are about creating systems of precision and providing real-time information that could save lives.

  A significant area of application involving the use of smart home setups, with the help of IoT dynamics, will let patients (especially elderly people) monitor and care in an immediate, independent setup. This area of application is called **ambient assisted living** (**AAL**). AAL systems deal with developing context-awareness based on sensor data and observations to gain information about the current situation.

  AAL aims to go beyond mere observation of one's living and working conditions. Research in this area majorly focuses on human–machine interaction via prompts in terms of prompting the user to perform the next step in a sequence of actions/emergencies.

  Sudden changes in heart rate, blood pressure, and so on can be monitored and notified to the end-users through health monitoring devices and apps such as microcontrollers, display systems, and many more, thereby allowing them to take necessary action on time.

  Industry research shows that demand for specific IoT-enabled health applications such as remote monitoring and digital diagnostics is increasing day by day. It is about providing pocket-friendly solutions for both the patients and healthcare professionals.

  Figure 5.2 is a pictorial depiction of a typical IoT healthcare system workflow.

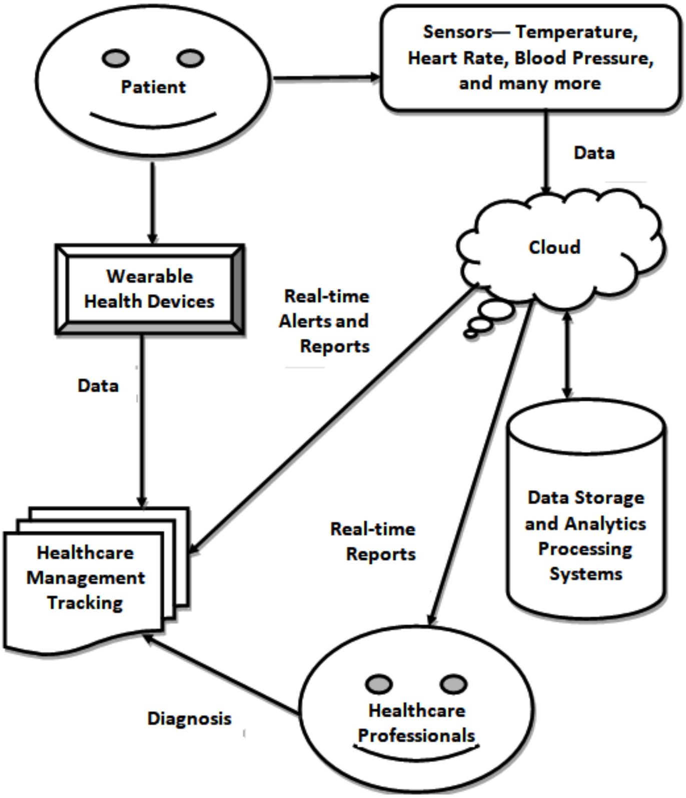

Patient
Sensors— Temperature, Heart Rate, Blood Pressure, and many more
Data
Cloud
Wearable Health Devices
Real-time Alerts and Reports
Data
Data Storage and Analytics Processing Systems
Healthcare Management Tracking
Real-time Reports
Diagnosis
Healthcare Professionals

Figure 5.2: A typical IoT healthcare system workflow

- **Predictive maintenance management**: The combination of specialized maintenance management and IoT devices, sensors, and so on, maintenance management can enhance various aspects of products in terms of functionality, health, availability, utilization, performance, and reliability. IoT-enabled setups are about preemptive forecasting and planning to avoid unexpected breakdowns. It is about smart machines with proactive maintenance based on data gathered from data analytics systems, machine learning algorithms, and so on.

  Especially in asset-intensive organizations, IoT can lead to huge cost savings and cut down on unplanned downtime. Gartner estimates that through 2022, decision automation in the form of predictive maintenance will generate the highest business value for organizations with heavy assets.

IoT-based predictive maintenance management enables more efficient use of existing resources and assets by providing the features to predict failures and reduce maintenance issues. Hence, this leads to increased asset utilization and an uninterrupted flow of mission-critical processes. It can detect issues before they become occur by providing early warning signs.

Another important aspect is ring-fencing. IoT-enabled systems can ring-fence them to make sure that high-value assets are protected from theft and removal.

According to a report by PwC (it is a multinational professional services network of firms), on average, predictive maintenance in factories could:

  - Reduce costs by 12%
  - Improve uptime by 9%
  - Reduce safety, health, environmental, and quality risks by 14%
  - Extend the lifetime of an aging asset by 20%

- **Industry 4.0**: Fourth industrial revolution and IoT are meant to improve the performance and outcome of each phase of the manufacturing process through optimized decision-making, lean manufacturing, and so on. It is about bringing in agility.

  Industrial automation, simulations, robots, and so on is a huge part of the combination of Industry 4.0 and IoT. Right inventory management to quality control can be optimized through industrial automation for delivering better customer experiences, higher return on investment, and enhanced performance.

  According to a PWC survey, 72% of manufacturers are increasing their digitization efforts, investing 907 US billion per year–roughly 5% of revenue–toward smart factories and connectivity. This shows that the industry players are beginning to realize through the combination of IoT and Industry 4.0 that it would be possible to not only improve operational efficiency but also to generate new ways of adding value to their customers.

- **Wearables**: They are electronic smart devices that are physically worn by individuals in order to track, analyze, and transmit personal data. These "*smart*" IoT devices can track biometric data from heart rate to sleep patterns and are also becoming popular consumer technologies in the gaming and fashion industries. In recent years, wearables have experienced an explosive demand in markets all over the world. Some of the main application areas are medical, entertainment, and fitness.

  Wearables can be used for identification and security purpose. Biometric capabilities such as face recognition or fingerprint activation help to improve security. Health and fitness wearables can offer biometric measurements such as body temperature, heart rate, and many more.

  Research shows that people use wearables mainly to accomplish "*legacy tasks*" or tasks that can be done without complex technologies. The healthcare domain is witnessing the biggest benefit from wearable technology.

- **Inventory and logistics management**: With large numbers of warehouses, distribution centers, and shipments, and increased inventory, IoT technologies bring about a plethora of benefits such as damage detection, accurate inventory control, enhanced freight management, and so on. Touchless data collection and tracking helps to bring about error-free workflows and processes.

  In the world of online shopping, customers need to have their orders delivered within days or sometimes even within hours. Today it is essential for companies to ensure that their customers have real-time accurate information of an item's availability and expected delivery date.

  With the help of actionable insights derived from the analysis of real-time data about the quantity and the location of the items, organizations and manufacturers can lower the amount of inventory on hand while meeting the needs of the customers waiting at the other end of the supply chain.

  IoT solutions like smart storage bins and shelves, companies can capture usage patterns and trends based on data of stock levels shared by these solutions. IoT-enabled weather tracking devices help companies to link forecasted weather conditions to route schedules, thereby enabling them to make better delivery decisions.

As per the survey done by Kenco (it is a logistics provider), 56% of supply chain professionals are currently or planning to invest in sensors/IoT, up from 42% in 2017.

- **Smart grid**: It is the next-gen energy system. Digiteum (it is a custom software development company that designs and develops digital systems for SMB and enterprise clients) defines it as follows: "*It's an electricity network that consists of a system of infrastructural, hardware and software solutions that enable two-way communication between all system parts and participants and provide efficient power generation and distribution in the supply chain.*"

  Smart grid solutions and devices, such as routers, radio modules, sensors, and so on, allow cities to improve energy usage, prepare for disasters, save on electricity, and also, they enable power authorities to restore power after a blackout in a quick manner.

- **Retail**: IoT dynamics have enhanced the consumer experience management cycle in the retail domain by tracking assets, customer satisfaction, and so on. Moreover, the pandemic crisis has made many retail organizations rethink their business strategies in order to ride the wave of the IoT era.

  IoT can help track and analyze shopping mall traffic so that shops and stores can make the necessary adjustments in order to streamline customer inflow and enhance customer shopping experiences while reducing overhead and cutting down on logistical and merchandising expenses.

  Retailers can update their products in real-time and also keep track of misplaced or lost merchandise with the help of IoT devices like sensors and actuators built-in on the shelves.

  A sensor-enabled shopping cart helps retailers to understand their customers' shopping patterns and inside-the-store journey, facilitate faster checkout, and so on. This, in turn, helps them to grow their businesses. By placing sensors on assets like shopping baskets and carts, retailers can track their location and receive alerts if they are stolen or damaged.

The demand-aware warehouse is another important functionality using components like warehouse automation and robotics, which are driven by online and in-store shopping customer demands. IoT allows retailers to monitor sales opportunities in real-time and track missed sales.

IoT-enable smart shelves help to solve aspects of tracking misplaced items or keeping track of out-of-stock items, which helps to reduce manual labor. Smart shelves with RFID and sensors can help in theft detection.

IoT tracking solutions help to determine if the products and materials are safe, track them and ensure that they are delivered on time and transported in ideal conditions. All these aspects help retailers optimize their supply chain management, transportation dynamics, and logistics. These solutions can also help track ambient conditions such as air quality, humidity, and so on through environmental sensors, inside cargo containers, in-store space, or delivery vehicles to protect perishable goods.

- **Media and entertainment**: The combination of IoT and AR can bring 3D immersive digital content to the customers, and moreover, IoT technologies can help companies understand the emerging needs and preferences of the customers, thereby providing an edge for the media and entertainment companies to be able to reach a wider audience through the use of granular insights to build targeted ads and context-driven content.

  IoT systems can also be developed with features like age-based content filtering, simplified media/content sharing, and so on. With a large amount of IoT data at their disposal, companies can capitalize on the same to create personalized content, offers, and so on for their audiences.

  Wearable devices fitted with sensors can also help companies to determine what number of people, who noticed a particular advert on a particular medium, and how many of these translated into conversions.

Figure 5.3 is a pictorial depiction of the global IoT market share by sub-sector.

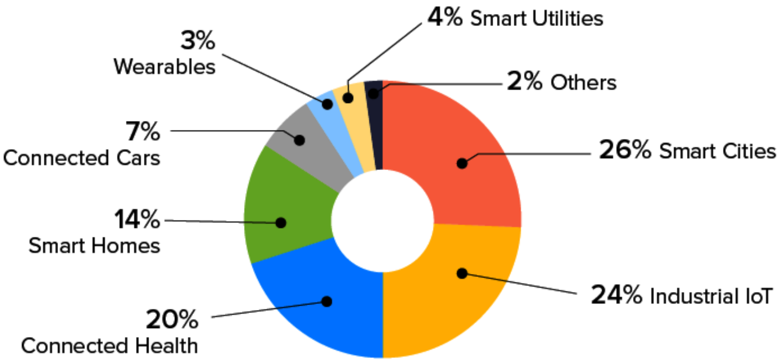


***Figure 5.3**: Global IoT market share by sub-sector*
Source: GlobalEnabler Analytics

5.2 Novel use cases

As per the IoT use case adoption report by IoT Analytics (it is a leading global provider of market insights and strategic business intelligence for IoT, AI, Cloud, Edge, and Industry 4.0), in 2021, the average large manufacturing, healthcare, automotive, retail, or energy company has rolled out eight different IoT use cases. In October 2020, the H2020 project named IntellIOT, funded by the European Commission, was launched. The project runs until September 2023, and its main aim is to support the development of novel intelligent, human-centered, and trustworthy IoT use cases in specific sectors like agriculture, healthcare, and so on.

Table 5.4 shows IoT uses cases with the most investment in recent times.

Use case domain	Investment (in US dollars)
Manufacturing operations	100
Production asset management	44.2
Smart home	44.1
Freight monitoring	41.7

***Table 5.4**: IoT uses case with the most investment in recent times*

According to the IoT Use Case Adoption Report 2021, IoT adoption is set to accelerate in 2022, driven by smart operations use cases with a high **return on investment** (**ROI**) and by IoT projects in **Asia-Pacific** (**APAC**) region. Other fascinating findings in this report are: the average large company is planning to invest into nine different IoT use cases in the next two years; use cases that focus on improving operations and assets are on the rise; and the average large company in Europe or North America indicated plans to invest strongly into seven different IoT use cases in the next two years, whereas companies in APAC plan to invest into 13 different IoT use cases.

A. **Daylight harvesting**: Connected lighting helps daylight harvesting systems; they are able to save electrical power. By tracking parameters like daily usage through IoT-enabled systems can improve a city's ability to stay green.

B. **Local trust zones**: Certain use cases require security, throughput, and so on at levels that are not feasible to deliver on a wider scale over a dedicated network.

C. **Drones for search and rescue operations**: Ongoing and future research is all about drone-based and sensor-based technology to help rescue humans and animals in dangerous situations. Apart from this critical area, drones are also gaining momentum in the e-commerce domain, oil rig companies, and so on.

D. **Industry 4.0**: Right from visual inspection to marketing and to green manufacturing, IoT will begin to play a more important role in the upcoming years. For example, in-store contextual marketing will be one of the fastest-growing cross-industry IoT use cases and obviously will play a major role in retail as well.

E. **Workplace analytics**: such analytics will be able to improve the return on investment and optimize the operations, but to fully realize this, companies will need to implement vast IoT systems and gather data over long durations before these analytics offer accurate and actionable insights.

As IoT analytics solutions continue to connect and harness the collective intelligence of employees, they are creating much more than an office setup; they are creating a community of collective intelligence. Through the proper use of IoT, organizations will be able to leverage their greatest asset—their employees.

F. **Freight monitoring**: Digitizing and analyzing assets through IoT can bring about a plethora of benefits, right from the reduction of risks to process standardization. Freight management is rapidly growing, and hence, the traditional track-and-trace solutions will not be able to keep up with this pace. This is where IoT-driven solutions come into play.

   With the current fragmentized solutions with limited visibility into real-time events, the introduction of IoT use cases can lead to a smart solution with enhanced real-time data gathering, data processing, and data analytics capabilities.

G. **Augmented reality (AR) and virtual reality (VR)**: Be it entertainment, gaming, or any other domain, AR and VR are gaining traction to create customized immersive experiences. AR and VR with IoT can enhance a whole range of business processes right from real-time training and instruction to modeling and simulating performance prior to manufacturing.

   According to a *Software.org* (it is an independent and nonpartisan international research organization to help policymakers and the broader public better understand the impact of software on our lives, our economy, and our society) report, adding the AR dimension to IoT expands its potential. For instance, in retail, AR can bridge the gap between online and offline, providing the customer with the best of both worlds.

   IoT is about taking traditional augmented reality systems to visualize to the next level—transforming them into smart, intuitive, and interactive AR. IoT and VR can bring about various types of collaborative solutions as they both share the concept of merging physical and digital worlds. The combination of these three technologies can add a whole new level of dimension, personality, and performance to the concept of smart communities, smart campuses, smart events, and smart cities.

Figure 5.4 is a pictorial depiction of a typical IoT AR/VR application workflow used in gaming, entertainment, and so on.

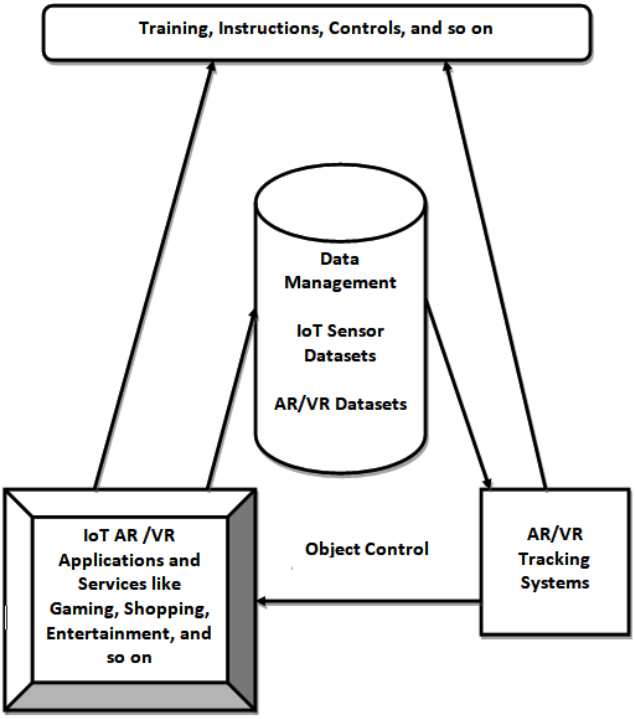

Training, Instructions, Controls, and so on
Data Management
IoT Sensor Datasets
AR/VR Datasets
IoT AR /VR Applications and Services like Gaming, Shopping, Entertainment, and so on
Object Control
AR/VR Tracking Systems

***Figure 5.4**: A Typical IoT AR/VR application workflow used in gaming, entertainment, and so on*

H. **Safety and hygiene**: IoT devices and technologies allow organizations to monitor the physical health of employees and monitor environmental conditions and equipment and machinery conditions, and thereafter the data collected can be used to design occupational health and safety strategies and to limit employee exposure to potential risks, structural failures, and accidents.

IoT devices with geolocation features can provide an asset or employee's exact location in real-time, which is needed to carry out a successful rescue operation.

I. **Parking**: In several metro cities, parking is a big problem. With IoT systems, such issues can be minimized. Sensors connected to parking lots can keep track of parker care, and data is sent to the cloud periodically, and then the analyzed data can be accessed by vehicle owners to check for vacant parking lots.

J. **Cobots**: The combination of IoT and Digital 2.0 technologies such as machine learning, artificial intelligence, and so on, robots (both consumer and industrial) will become more prevalent in our lives. As these technologies advance, the capabilities of robots will also advance. They will be able to perform for even more complex and dangerous tasks, and this is where cobots come into the picture; the next wave of IoT automation.

   A cobot is a robot that operates in close collaboration with autonomous systems and human beings. Cobots are conceptually different from today's typical robots. As the name suggests, these robots are designed to be collaborative, and they will work in close proximity to human beings and autonomous systems.

K. **Telepresence**: Telepresence is made possible due to the cutting-edge combination of IoT, and virtual reality has made; it is a set of technologies that enables a person to perform actions in a remote or virtual location as if physically present in that setup. Major players in this space include Cisco, VGo Communications, and iRobot.

   Current and future use cases in this field are focusing more and more on building multimodal telepresence devices and systems.

L. **Benchmarking**: Enhanced benchmarking solutions are a trend that is picking up pace. Data integration and aggregation helps to build structured benchmarking and standardization.

M. **Twinning**: Twinning or a digital twin is a digital representation of a physical device, object, process, or service that is used to run simulations before the actual device, object, process, or service is built and deployed. IoT is the backbone of twinning; both combined together can help in gauging future performance and possible failure.

   Let us take the example of car automation and maintenance to explain how IoT and digital twins are interrelated. A digital twin uses data from connected IoT sensors in the car to tell its story all the way through its complete lifecycle. And with IoT data, we are able to keep track of this asset and its performance and health. By connecting this data to its digital twin, companies and manufacturers will then have a full view into their asset is doing.

N. **Trash collection**: The data generated, collected and analyzed can be used to optimize collection practices, pest control techniques, and collection routes. Optimizing routes also leads to less truck emissions and traffic congestion.

Spotlight

None of these use cases can be fully successful in isolation because IoT is becoming the norm—all-pervasive. Developments in one domain impact others. It is about coexistence in order for all these use cases to reach their full potential.

Figure 5.5 is a pictorial depiction of the various novel use cases of IoT.

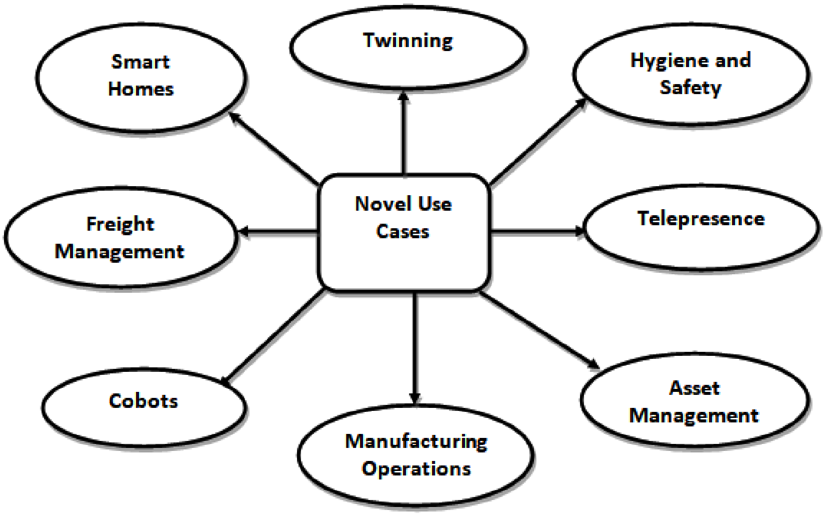


Figure 5.5*: Novel use cases*

5.3 Conclusion

In this chapter, we covered the main application areas of IoT like smart cities, healthcare, and so on. We have also discussed certain novel uses cases of IoT that are likely to pick up the pace and grow into full-fledged applications in the near future. This chapter sets the stage for the final chapter of the book that deals with important topics such as current scenarios, top future trends, and some final words.

5.4 Questions for reflection

1. How can we prepare for the advancements in IoT technologies?
2. What is meant by a smart grid?
3. Which IoT use cases are likely to improve the return on investment?
4. What is the difference between IoT and IIoT?
5. Have you worked on any IoT use cases, and what were your learnings and findings?
6. How does IoT influence the development of smart cities?
7. Which industries can benefit from IoT?

Chapter 6
Current and Future Trends

Distributed and dynamic digital interactions carried out by IoT have been the central theme throughout a crisis-stricken world in 2020. This current trend of IoT that involves a wide spectrum of domains has surely helped the world in crisis to fight it off by continuing to connect, live, communicate, work, and collaborate.

Fortune Business Insights report states that IoT technology holds important potential in the ICT segment, with the worldwide market valued at 190 US billion dollars in the year 2018 and hitting 1.1 trillion US billion dollars by the year 2026. IDC reports that on the global market, Industrial IoT spending is going to surpass the consumer IoT domain.

As the IoT devices and systems extend from everyday household objects to advanced industrial tools, each and every person will eventually have access to all these trends. To maintain or rather to add pace to the trends, organizations will have to adapt quickly to maintain their momentum to remain competitive.

Structure

This chapter will cover the following topics:

- Current trends of IoT
- Future trends of IoT

Objective

After studying this chapter, you will be able to:

- Understand the main current trends of IoT
- Identify various trends that are going to rule the future horizon of IoT
- Learn more about these aspects through research findings and statistics

6.1 Current trends

Combined with emerging Digital 2.0 technologies such as AI, cloud computing, and so on, IoT is able to minimize costs, optimize customer experiences, enhance operational efficiency, and many more. The current trends of IoT reflect all these benefits in full-spectrum through their various applications.

Table 6.1 presents the highlights of various domain-wise current trends of IoT.

Domains	Trends and Developments
Security	In 2021, we witnessed an increase in security-centric smart IoT devices, sensors, and gadgets. With the rise of distributed work setups and work-from-home dynamics, a new spectrum of cyber risks has opened up, and for handling this new spectrum, organizations now are already in the processing of IoT-enabled security measures and strategies to bridge this gap.

Manufacturing	Enhanced shop floor operations, end-to-end solutions, and product-as-a-service business models are some of the key trends that show the growing influence of IoT in the manufacturing domain.
Edge	The combination of IoT and edge computing is helping to overcome the downside of cloud solutions in terms of network congestion and latency issues. The remarkable improvement in connectivity has triggered a new investment in infrastructure, especially edge architecture.
AI	A recent Tech Trend survey by SADA Systems (it is a premier cloud solutions provider specializing in technology consulting, IT services, application development, and managed services) states that IoT and AI are the popular technologies currently in use today. It also found that AI and IoT are the top technologies companies are investing in most to increase efficiency and provide a competitive advantage.
Healthcare	AI-based patient monitoring tools, delivering healthcare courses through a combination of IoT, augmented reality, and virtual reality, remote patient monitoring have become popular in the recent past due to the global crisis.
Blockchain	The development of the combination of Blockchain and IoT is fast becoming an integral part of the agenda of businesses as it provides a more flexible and secure environment for IoT devices.
Data Analytics	Digital 2.0-driven analytics systems are getting more advanced with the help of IoT. With the ongoing IoT advancements, these data analytics systems are able to not only study the various data sources but they also aid in rapid data processing and decision-making.

***Table 6.1**: Highlights of current trends*

Let us have a look at the top current trends that bring about all a gamut of benefits.

- **Security**: With the threats landscape changing each day, IoT solutions are expected to focus more and more on security measures and protocols to meet the complicated challenges in the coming years. Moreover, with the rise of distributed work setups and work-from-home dynamics, a new spectrum of cyber risks has opened up, and for handling this new spectrum, organizations now are already in the processing of developing advanced IoT-enabled security measures and strategies to bridge this gap.

  With the increasing number of interlinked devices, extra and enhanced security measures and mechanisms are becoming the order of the day. In the ongoing period, we are likely to see an increase in security-centric IoT devices and solutions.

- **Healthcare**: Many exciting developments have taken place in the healthcare domain—all thanks to the global crisis. AI-based patient monitoring tools to collect and treat the patient based on real-time reports are already becoming popular.

  IoT, in combination with AR and VR, is witnessing adoption in medical institutions and universities for delivering health care courses. Remote monitoring has fastly become a cost-effective tool that offers high-quality treatment to patients who live in far-off areas or are elderly people.

  Organizations are already developing initiatives around the wellness in terms of team-building events, retreats, and so on. The employer-provided wellness apps are a relatively new concept, and this trend is picking up a good pace.

  These plug-and-play apps, systems, and platforms are able to offer enhanced versions of traditional medical devices and treatment modalities.

- **Blockchain technology**: IoT devices are very susceptible to cyber-attacks and security. This is where Blockchain, a game-changing online distributed ledger technology, comes into play. The development of the combination of Blockchain and IoT is fast becoming an integral part of the agenda of businesses as it provides a more flexible and secure environment for IoT devices.

Using Blockchain to store IoT data adds another layer of security. This duo is already bringing about transformation in supply chain management as Blockchain provides a shared ledger and smart contract for the various suppliers, distributors, and customers, thereby minimizing the involvement of manual processes. This whole dynamic helps to reduce bureaucratic layers and improves trust levels.

- **AI and IoT**: The dynamic duo of AI and IoT, "*Artificial IoT*" is about resource and process optimization. The combination and integration of AI, smart devices, and other Digital 2.0 technologies will continue to contribute to improving the overall security of IoT solutions. Moreover, more and more industry players are in the process of joining the bandwagon of developing artificial IoT solutions.

  A recent Tech Trend survey by SADA Systems (it is a premier cloud solutions provider specializing in technology consulting, IT services, application development, and managed services) states that IoT and AI are the popular technologies currently in use today. It also found that AI and IoT are the top technologies companies are investing in most to increase efficiency and provide a competitive advantage.

  The AI-IoT duo has already started to redefine the future of automation. According to experts, in the near future, over 80% of IoT initiatives will use AI.

- **Enhanced data analytics**: Digital 2.0-driven analytics systems are getting more advanced with the help of IoT. With the ongoing IoT advancements, these data analytics systems are able to not only study the various data sources but they also aid in rapid data processing and decision-making.

  Hyper personalization gives products and services a human touch. Currently, organizations are slowly and steadily tapping into the various dynamics of this field using enhanced data analytics solutions driven by IoT. Smart home setups are a sector where hyper-personalization is becoming more popular.

- **Emerging use cases**: Novel use cases are bound to emerge at a fast pace. Presently, IoT apps surround smart homes, smart grids, wearable, smart cities, industrial settings, and so on. With the rise of newer versions of IoT technologies in the coming days, the reach of IoT will cover more business domains, assets, processes, and settings.

- **Edge computing**: The combination of IoT and edge computing is well way underway. It will become more prevalent in the upcoming years, and this will help to overcome the downside of cloud solutions in terms of network congestion and latency issues. The remarkable improvement in connectivity has triggered new investment in infrastructure, especially edge architecture.

- **IoT app testing**: As time progresses, the future of IoT app testing will continue to grow. It is already pervading all aspects of life in one way or another through enhanced wearables, sensors, connected devices, and so on.

- **Manufacturing**: As per the findings of the annual survey conducted by Bsquare (it is an Internet of Things systems software provider, technology distributor, and system integrator), 86% of manufacturing enterprises have adopted different forms of IoT to enhance shop floor operations. This goes to show the growing influence of IoT in the manufacturing domain.

  IoT helps the manufacturing sector to build end-to-end solutions. It also helps to build a product-as-a-service business model, which gives organizations a chance to generate new revenue streams and also have the ability to quickly roll out multiple versions of products to see what works best and to optimize the same to meet customer requirements.

  Figure 6.1 shows the pivotal moments in IoT market evolution right up to the year 2020 (Source: IDC)

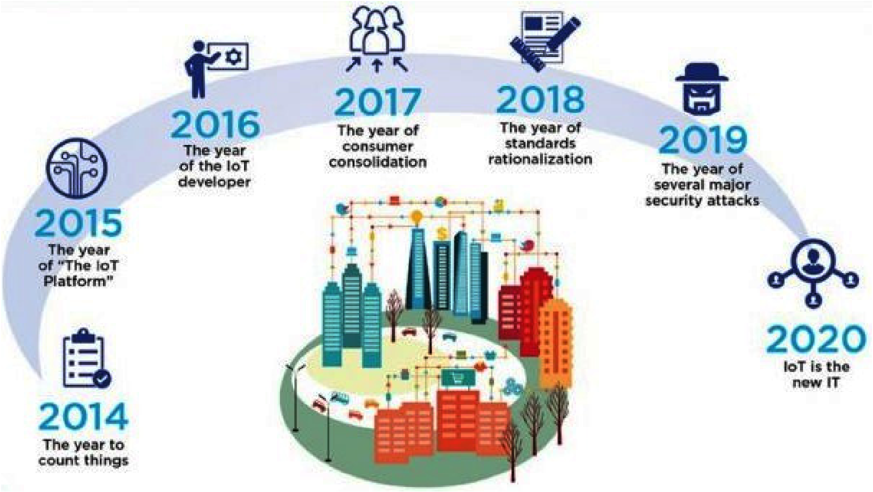

2014
The year to count things
2015
The year of "The IoT Platform"
2016
The year of the IoT developer
2017
The year of consumer consolidation
2018
The year of standards rationalization
2019
The year of several major security attacks
2020
IoT is the new IT

***Figure 6.1**: Pivotal moments in IoT market evolution right up to the year 2020 (Source: IDC)*

Spotlight
Slowly and steadily, IoT is being driven by business goals and by not by mere technology trends. This, in turn, is leading to the creation of more use cases around business goals and impacting the way of carrying out business processes and tasks.

6.2 Future trends

As per Statista (it is a company specializing in market and consumer data), the projected global IoT spending is valued at over 1.1 trillion US dollars and has been steadily growing. As per Mckinsey (it is a management consulting firm), around 40% of the value IoT generates will come from developing countries. Fortune Business Insights projects that the IoT market size, which was 250.72 billion US dollars in 2019, will top 1.4 trillion US dollars.

Figure 6.2 is a pictorial depiction of the top future trends of IoT.

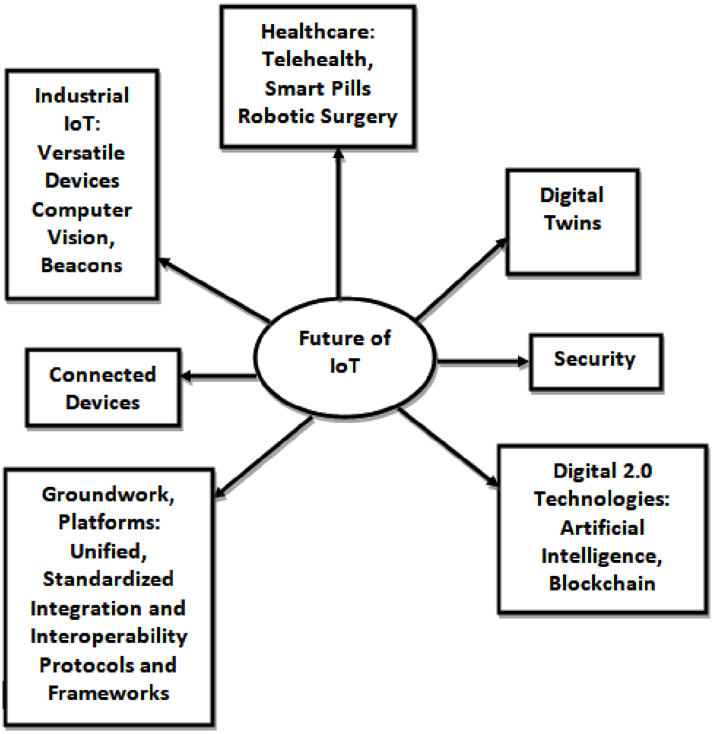

Healthcare: Telehealth, Smart Pills Robotic Surgery
Industrial IoT: Versatile Devices Computer Vision, Beacons
Digital Twins
Future of IoT
Connected Devices
Security
Groundwork, Platforms: Unified, Standardized Integration and Interoperability Protocols and Frameworks
Digital 2.0 Technologies: Artificial Intelligence, Blockchain

Figure 6.2*: Top future trends of IoT*

Table 6.2 presents the future statistics related to various IoT domains.

Domains	Statistics
IIoT	IIoT market is expected to grow from 76.7 billion US dollars in 2021 to 106.1 billion US dollars by 2026.

Domains	Statistics
Healthcare	Recent forecasts from the US Census Bureau report that by 2025, 1.2 billion people will be elderly. This fact indicates the population's future needs for health care wearables, the demand for which will be higher than ever. The healthcare industry is projected to increase revenue by more than 135 billion US dollars by 2025. Allied Market Research reported that the global share of IoT in the health care market would reach 332.672 billion US dollars by 2027, with a CAGR of 13.20% from 2020 to 2027. Zion Market Research (it creates futuristic, cutting edge, informative reports ranging from industry reports, company reports to country reports) estimates that the global IoT medical devices market is going to have a CAGR of 15.27% between 2019 and 2025.
Artificial intelligence	The global AI in the IoT market is expected to grow at a CAGR of 27.3% during the forecast period 2021–2026.
Consumer IoT	The consumer IoT market is estimated to reach 142 billion US dollars by 2026 at a CAGR of 17%. The Smart Home IoT market will grow to 53.45 billion US dollars by 2022.
Cellular IoT	The number of cellular IoT connections is expected to reach 3.5 billion US dollars in 2023.
Edge	According to recent estimates, the global edge computing market has been projected to grow to 9 billion US dollars by 2024.

Domains	Statistics
Big Data Analytics	As per TechJury (it is a platform that provides detailed, unbiased reviews of business software solutions, latest tech industry news, buying guides, and comparisons), 103 billion US dollars is the projected value of the big data analytics market by 2023. Forbes (it features articles on technology, finance, science, industry, investing, and marketing) predicts that more than 150 zettabytes or 150 trillion gigabytes of real-time data will need analysis by 2025.

***Table 6.2**: Future of IoT statistics*

As we continue into the year 2022 and beyond, the following set of IoT trends are going to accelerate growth in all spheres of life leading into the near future.

- **Connected devices**: They will grow at an exponential rate many times fold than the current rate due to triggering factors like global pandemics and the emergence of cutting-edge technologies such as AI, 5G, smarter hardware, and so on; this will enable richer data-driven experiences.

  Moreover, connected devices are bound to see improvement in their remote access functionalities. Given the fact that in the period 2020–2021, the world witnessed several new ways of doing business and leading life, such as remote work, remote healthcare, and so on, organizations are bound to capitalize on this trend.

- **Healthcare**: The duo of healthcare and IoT provides the ability to constantly monitor patient health parameters and metrics outside of typical medical tests and appointments (refer to *figure 6.3*). This trend will pick up pace in the next five years or so. The use of drones will see a huge growth rate in the upcoming years.

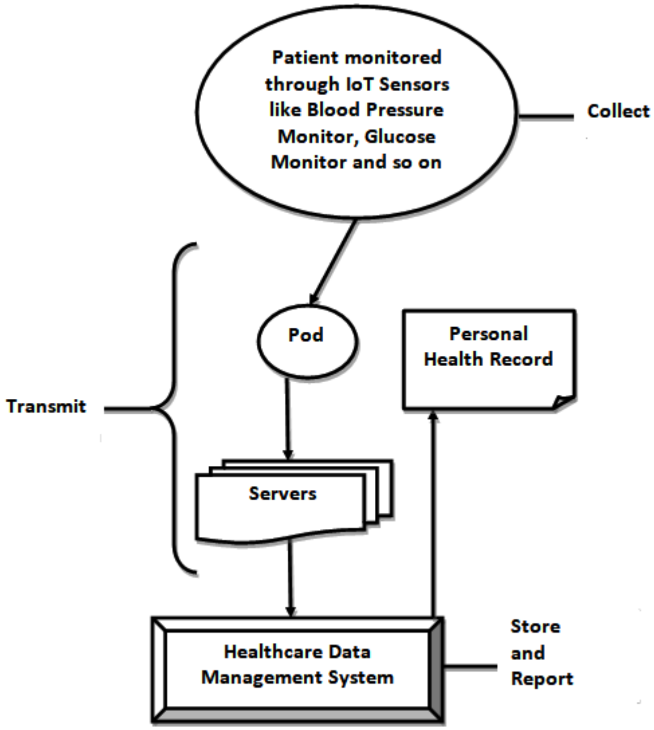

Patient monitored through IoT Sensors like Blood Pressure Monitor, Glucose Monitor and so on
Collect
Pod
Personal Health Record
Transmit
Servers
Healthcare Data Management System
Store and Report

***Figure 6.3**: Health care remote monitoring*

Telehealth applications where a doctor treats a patient via video conferencing will grow in leaps and bounds. IoT devices and their advancements will make Telehealth and digital diagnostics more accurate.

Another trend that is likely to become popular in the future is smart pills. Smart pills are equipped with ingestible monitors that send signals to sensor patches worn on a patient's body. These sensors then keep track of the patient's vital signs and relay them to a doctor or medical professional.

Recent developments in this field show that there will be a continuous surge in the popularity of robotic surgery. Industry research reveals that by 2024, the market for surgical robots will exceed more than 98 billion US dollars. MarketsandMarkets (it offers market research reports and custom research services on 30,000 high growth opportunities.) conducted a study on the expected growth of IoT and various other technologies in the health care sector, projecting a 30.7% annual growth rate between 2017 and 2025.

- **Augmented analytics**: As per industry experts, 74% of businesses worldwide intend to invest in new technologies, especially BI tools such as augmented analytics, to enhance their operational productivity and efficiency.

  Traditional analysis is slowly and steadily fading away, and there is a consistent growing focus on using more machine learning dynamics; and in the near future, organizations will focus more on analytics-driven by advanced artificial intelligence dynamics.

  Moreover, organizations will begin to focus heavily on managing metadata about their products and services through specialized data management in the near future to enhance their augmented analytics solutions.

- **Industrial IoT**: The current prime focus will shift to Industrial IoT from merely on consumer IoT. As per industry experts, IoT is set to create a 200 billion US dollar market for hardware manufacturers within the next five years as the need for more versatile devices increases.

  Beacons for better work management in industrial IoT settings will become the norm for monitoring employees and scheduling tasks in the near future. Computer vision for visual inspection will gain more popularity as it provides a plethora of benefits such as improving efficiency and quality control.

  Several key mergers in this domain have occurred in the recent past. For example, in 2021, Cisco partnered with Newark to offer industrial IoT network solutions for harsh and non-carpeted setups to customers across North America, and Plataine partnered with SAP to integrate IIoT and AI-based software for digital manufacturing as a part of its business offering. Such mergers are bound to happen in the future too.

- **Architectural groundwork, interoperability, and platforms**: This will lead to the creation of novel use cases. Though new architectural groundwork is being laid, and new protocols and platforms are being introduced to work with cutting-edge IoT systems, several organizations will always have some legacy systems that use different standards, protocols, and platforms. In the future, such organizations are more likely to develop some sort of intermediary such as platform-independent IoT gateways. Organizations will need to connect existing legacy devices and assets and implement new architectures and platforms for bringing about optimization and interoperability.

This trend will be hastened by customers as customers will not buy devices and solutions that do not speak a common language or are not able to interoperate in a seamless manner. The explosion of data combined with the need for more analytics will accelerate the demand for and creation of specialized IoT platforms.

As organizations will continue to face interoperability issues, there will be an emergence of new use cases to deal with this. We will see major stakeholders coming together to develop standardization of protocols and frameworks in regards to inter-communication, data acquisitions, protocol translation, and so on for organizations, vendors, and manufacturers for minimizing the interoperability issues.

The next phase of interoperability is about cutting through the stack of various vertical silos and getting them to work together in a seamless manner. The future trend in this segment is about moving away from vertical silos toward a horizontal way of doing things, and this is where the interoperability standards will come into play.

Unified, standardized integration and interoperability protocols and frameworks will gain more attention and momentum in the upcoming years, thereby allowing organizations to handle incredibly complex systems.

- **Edge**: As more and more IoT devices get to process increasing volumes of data, there is a need for decentralization. And this need will lead to organizations focusing on developing local edge computing devices located close to the data sources. With more and more companies adopting the remote work dynamic, edge computing will become a significant trend in the coming period.

- **Connectivity**: Although Bluetooth, WiFi, and many more are the de facto standard for IoT wireless protocols, LiFi, WiFi6, network virtualization, and so on are relatively new wireless protocols, and they will be incorporated more and more in the upcoming years.

  WiFi6, also known as 802.11ax, is the next generation of WiFi. With WiFi6, organizations are able to support new systems on their existing wireless local area network infrastructure while running older systems. It brings about a wider spectrum, higher bandwidth, and more simultaneous data streams. Network virtualization allows the creation of virtual networks and network functions without being tied to physical infrastructure. It helps to overcome geographical limitations and reduces equipment costs.

- **Security**: Be it 2021 or 2022 or even beyond, organizations will put more impetus on securing their internal networks and beyond. With more than half of organizations falling prey to cyber risks and attacks, the need for more effective threat remediation measures will be developed. They will work with more segmentation strategies. By segmenting or isolating devices, organizations will be less vulnerable to cyber-attacks. According to experts, through 2023, organizations that do so will experience 25% fewer successful cyber-attacks.

- **Green deals**: IoT will play a major role in the design, implementation, and monitoring of green deals, sustainability programs, and so on. This trend will become more popular with government-level projects and programs.

- **Cellular IoT**: The number of cellular IoT connections is expected to reach 3.5 billion in 2023. And this trend will be fueled by a combination of IoT and Digital 2.0 technologies.

- **Work-from-home solutions**: These will become more popular so as to be able to tackle current as well as future disruptions. IoT devices will play a major role in these dynamics, right from video conferencing to automated scheduling. Moreover, whenever physical activity needs to happen, especially in industrial IoT in terms of machines, assets, and equipment, advanced IoT solutions can help to coordinate between on-premise and off-premise elements of work. IoT can help maintenance engineers and workers to effectively monitor these machines, assets, and equipment remotely. This is one popular scenario, and it is already being implemented and will be applied across domains and their sub-domains in the next decade or so.

- **Blockchain**: IoT devices are already using Blockchain to organize, store and share streams of data in a reliable manner, and this trend will only get stronger in the next few years. Blockchain cryptographic algorithms are one of the most robust encryption standards currently available, and more work will be done on them in the near future.
- **Digital twins**: This technology creates a virtual asset that corresponds directly with a physical object (*figure 6.4*). This allows for the physical object to be thoroughly tested digitally before it is implemented in the real world.

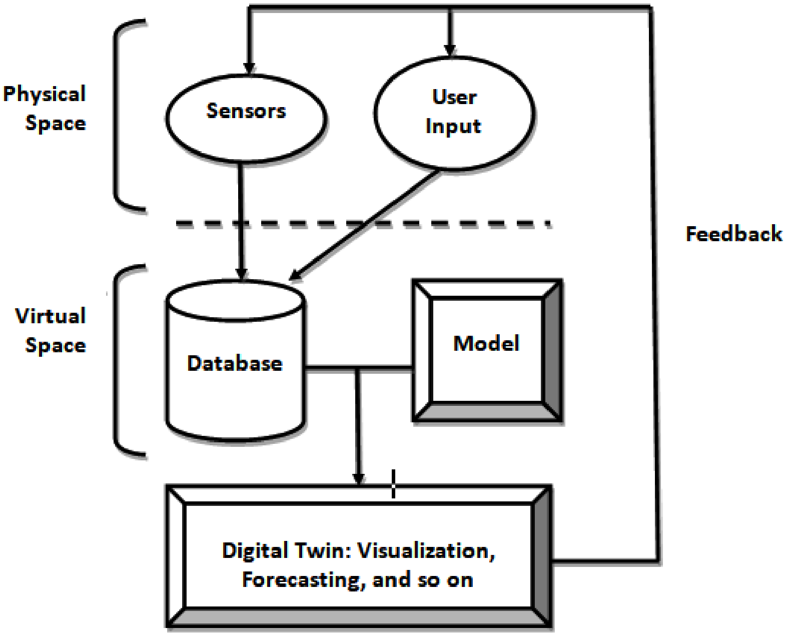


***Figure 6.4**: Digital twin*

This technology allows organizations to perform *"what if"* simulations. These simulations can be used to identify and prevent problems proactively, reduce downtime, and speed up the development of new products.

- **Voice-controlled devices, voice biometry**: Recent global crisis has triggered the development of this field, and it will grow at a high pace in the near future. Going touchless is becoming the new norm, and it has led to the emergence of new fields such as voice control panels, no-touch ATMs, and so on (refer to *figure 6.5*). In the coming period, smart systems can be operated by giving commands, changing settings, and receiving results anywhere, anytime.

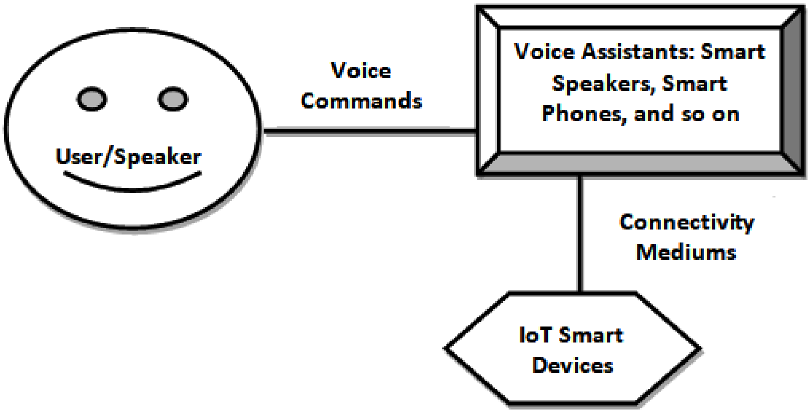


***Figure 6.5**: Voice-controlled devices*

Voice biometry is another trend to watch out for. This technology lets organizations build a digital profile of someone's voice based on various parameters such as tone, pitch, and so on. Organizations will be using this technology more and more in the near future for security and recognition purposes.

Table 6.3 presents the emerging IoT trends and their range and mass level in terms of growth and adoption.

Trend	Range	Mass
Advanced computer vision	Within a year	High
Edge AI	Within a year	Very high
Natural language processing	Within a year	High

Cyber security	1 to 3 years	High
Augmented analytics	1 to 3 years	High
Edge	1 to 3 years	High
Platforms	3 to 6 years	Very high
Digital twins	3 to 6 years	High
Blockchain	6 to 8 years	Medium
Smart spaces	6 to 8 years	High

Table 6.3*: Emerging IoT trends and their range and mass level in terms of growth and adoption*

Spotlight

This is certainly not a full list of current and future trends shaping the current and future landscape of the IoT world, but it certainly gives a complete picture of what to expect in the coming years.

6.3 Final words

The future of IoT looks pretty bright and promising. Research shows that 66% of US cities are investing in smart city technologies, and nearly half of the ongoing smart cities projects are developed in Europe. It is predicted that within the next five years, our homes will be slowly filling up with more and more IoT devices.

According to Cisco's Connected Vehicles division research, driverless cars could eliminate up to 85% of head-on collisions. According to the findings by *iotsworldcongress.com* (it is the global meeting place for business and tech executives looking to leverage technology to achieve innovative, disruptive, and game-changing outcomes), the global smart agriculture market size is expected to triple by 2025, reaching 15.3 billion US dollars mark.

Spotlight

Although IoT is still in the development phase, one thing is for sure–it is here to stay. IoT is revolutionizing most domains today and the future is bound to hold many exciting and endless possibilities.

In order to successfully match businesses and their efforts with the new IoT capabilities, it is essential for all stakeholders to get an in-depth understanding of the IoT's current and future trends.

6.4 Conclusion

In this final chapter of this my book, right from edge computing to smart home devices and much more has been tackled. With the latest technologies moving to their next stage of advancement, IoT devices and systems will become more intuitive and convenient to use. All these dynamics have been covered along with their research findings and statistics.

6.5 Questions for reflection

1. Are the current protocols and frameworks of IoT good enough to tackle future trends?
2. Why has IoT gained so much buzz in recent years?
3. How can we prepare for the advancements in IoT technologies?
4. How is the competitive landscape in the global healthcare market?
5. What is the scale of use of IoT devices in contemporary times?
6. Which technologies will make IoT a game-changer in the future?
7. How big is the future of the overall IoT market?

Index