K. Thakur et al., *Emerging ICT Technologies and Cybersecurity*
https://doi.org/10.1007/978-3-031-27765-8_6

6. Internet of Things (IoT)

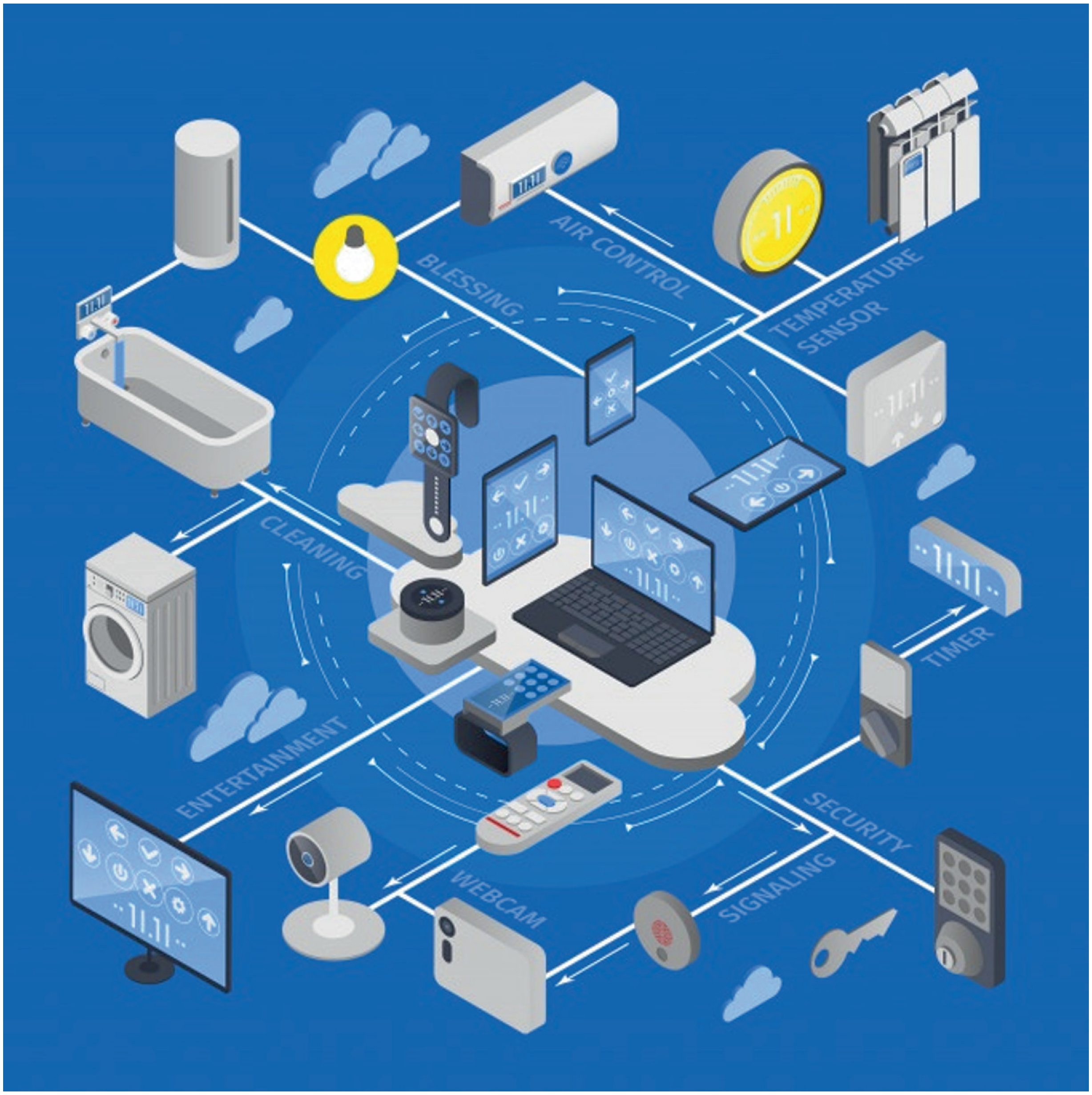
Kutub Thakur[1] ✉, Al-Sakib Khan Pathan[2] ✉ and Sadia Ismat[3] ✉

(1) Department of Professional Security Studies, New Jersey City University, Jersey City, NJ, USA
(2) Department of Computer Science and Engineering, United International University, Dhaka, Bangladesh
(3) Department of Professional Security Studies, New Jersey City University, Jersey City, NJ, USA

✉ **Kutub Thakur (Corresponding author)**
Email: kthakur@njcu.edu

✉ **Al-Sakib Khan Pathan**
Email: sakib.pathan@gmail.com

✉ **Sadia Ismat**
Email: sismat@njcu.edu



Introduction to Internet of Things (IoT)

Internet of Things, precisely referred to as the IoT, is a relatively new concept of the connected physical devices or appliances through the Internet. In other words, the network of connected devices such as home appliances, office equipment, industrial machines, motor vehicles, and many such types of things that can be controlled through built-in embedded software applications through the intercommunication with mobile applications or other centralized platforms. The connected physical devices have in-built sensors to sense different types of signals such as light, blow, touch, temperature, moisture, and many other things and convert them into digital signals through embedded software applications and get automated instructions to act according to the preconfigured conditions. The Internet of Things (IoT) has expanded exponentially in the recent years. It is expected to cross 22 billion devices by 2025 [181]. The schematic diagram of IoT network is shown in Fig. 6.1.

Fig. 6.1 Pictorial concept of Internet of Things. (***flickr***)

Importance of IoT

The concept of IoT is so important because it sits at the core of numerous automation schemes such as home automation, office automation, industrial automation, and many other automated processes in all domains of businesses. When all machines and devices can communicate and take action and instructions, the whole world will become very much connected and efficient. The main benefits of IoT include:

- Work efficiency and process productivity

- Effective use of modern technologies for betterment of lives
- Substantial energy and cost saving on different home, office, and business processes
- Reduced footprints of greenhouse gases.

Main Features of Internet of Things

Internet of Things (IoT) is a world of interconnected devices with power to interact and communicate through different sensors and communication protocols. The main features of IoT are mentioned below [182]:

- Effective endpoints management
- High level of scalability, analytic capability, and system integration
- Robust automation and security of the physical assets
- Increased device efficiency and energy saving
- Efficient connectivity among the devices and controlling persons
- Deployment of greater sensing capabilities
- Highly active engagement between the modern technologies and daily-life devices
- Incorporation of cutting-edge technologies like artificial intelligence and machine learning.

History of Internet of Things

The predecessor of the concept of automation through Internet of Things can be traced back in 1950 when the supervisory control and data acquisition (SCADA) system was introduced for the automation of industrial processes based on complex sensing and transmitting systems. The modern concept of automation based on IoT can be marked in 1980, when a code dispenser was modified through computer code by the programmers at Carnegie Melon University, to check the temperature, availability, and waiting queue of coke bottles in the dispenser [183, 184].

- **1999—**The term “ *Internet of Things*” was coined by Kevin Ashton and Radio Frequency Identification (RFID) technology was introduced.

- **2000**—The first smart refrigerator was introduced by LG Corporation.
- **2008**—The number of connected devices crossed the number of people on the Earth.
- **2009**—Google Inc started testing the driverless cars.
- **2011**—Google's Nest smart thermostat was introduced in the market.
- **Present**—The IoT world has already expanded tremendously and is expected to make significant impact on all walks of life very soon with the adaptation of 5G technology.

What Is Ambient Intelligence in IoT?

The concept of ambient intelligence, precisely referred to as AmI, is the development of such devices or elements that use pervasive computing, sensing power, adaptivity, and intelligence by collected data from the environment and processing through computing power. The concept of ambient intelligence was coined by Eli Zelkha and colleagues in 1990 [185].

The main examples of ambient intelligence that have used the high-level of sensing devices and artificial intelligence in their invention include Neura app, Otter.ai, ElliQ and others. These services helped a range of categories of people to make their lives so easy.

Autonomous Control in IoT

Autonomous control is a new concept of Internet of Things in which the devices use knowledge-enhanced electronic logic, precisely referred to as KEEL, to make decisions in the connected environment of IoT. As we know, IoT gets the instructions based on a logic when certain conditions are met, but the autonomous control devices use the sensors and artificial intelligence to make decisions for the human being. This concept is known as Internet of autonomous things, precisely known as IoAT. The actuators used in the autonomous things collect and process the information from multiple surrounding sources in the environment and make decisions like the human do [186].

Range of Enabling Technologies Behind Internet of Things

Internet of Things has evolved through numerous concepts that use a range of modern technologies, especially information technology, electromechanical technologies, sensing device electronics, and others. The most common technologies that enabled the concept of IoT to grow exponentially include the following [187]:

- Low Power Sensors
- Cloud Computing
- Artificial Intelligence
- Machine Learning
- Data Analytics
- Big Data
- Enhanced Connectivity
- Internet Protocol V6.

Low Power Sensors

The low-power sensors make the IoT devices more useful and efficient for home automation, building automation, and many other automation environments. The notable examples of low-power sensors for IoT include low-power Bluetooth devices, ambient light sensors, smart hubs, digital geomagnetic sensors, digital microphones, programmable push buttons, integrated environment sensors, smart heat sensors, and so on.

Cloud Computing

Cloud computing has revolutionized almost all types of business solutions based on information technology. It offers highly efficient, low-cost, fully-connected, and managed system for building centralized control systems for the IoT systems.

Artificial Intelligence (AI)

Artificial intelligence enables the IoT environments to be dynamic, robust, and interactive in certain given conditions due to the power of software application that incorporates the artificial intelligence such as similar patterns, figure prints, facial recognition, and many others.

Machine Learning

The capability of machines to learn from the experience or training through data input to consume for understanding the surroundings is another very important technology that enables the Internet of Things, especially in the field of driverless vehicles and aviation domains.

Data Analytics

As the sizes of the interconnected devices increase, the data generated by the devices and systems expand exponentially. To handle that big volume of data, we would need high level of data analysis power. The modern technologies powered by big data and artificial intelligence can handle and process huge piles of data in a very short time period.

Big Data

Big data solutions are very helpful for the IoT environments and solutions because handling of enormously huge data generated by the IoT devices is an uphill task. Big data technologies are assisting IoT systems tremendously to handle the huge volume of data created by those connected devices.

Short Range Wireless Technologies

The short-range wireless technologies are proving to be the backbone of IoT in office, home, building, community, healthcare, and other automation systems. The most important short-range wireless technologies that are highly supportive in IoT environments are [188]:

- ZigBee wireless technology
- Near-Field Communication (NFC)
- Bluetooth and BLE technology
- Radio Frequency Identification (RFID)
- Low-Power WAN (LPWAN)
- Z-Wave Technology
- Wi-Fi Technology.

Medium and Long-Range Wireless Technologies

The medium and long-range wireless technologies that play a pivotal role in the connecting and building centralized control systems in clouds include those technologies that are available in wireless cellular environments. They are used as the backhaul technologies in IoT environments. In both the technical and commercial definitions, the term '*backhaul*' generally refers to the side of the network that communicates with the global Internet. A few examples of medium and long-range wireless technologies include:

- 2G/3G/4G technologies
- LTE, LTE-A, LTE-A Pro
- Wi-Max, GSM, CDMA
- Fifth-Generation Wireless.

Effective Communication Protocols

The most important protocols that play very vital roles for the enhancement of IoT solutions and environments are those that operate behind the short, medium, and long-range wireless technologies, sensing communication, control communication and others.

Internet Protocol V6

The number of connected devices has crossed many times the count of the people on the earth. This number will continue to expand exponentially in the future. The IPV4 will not be able to cater to such a huge number of elements in an IoT network. IPV6 is the best option that can help and cater to this huge demand for IP addresses for the connected devices across the globe.

Architecture of Internet of Things Ecosystem

As far as the architecture of the IoT ecosystem is concerned, there is no comprehensive agreement among the researchers on the layers of the architecture of IoT environments. There are different concepts for the architecture of IoT in the marketplace. A few very important architectures are mentioned below [189]:

Three Layer Architecture

Three-layer architecture of IoT consists of three layers that are commonly adopted in the deployment and operations of the IoT networks. They include:

- **Perception layer**—This layer deals with the physical devices, sensors, actuators, and other elements that collect data from the surrounding.
- **Network layer**—The network layer consists of the connectivity of the devices used in the perception layer with the upper layers such as routers, hubs, servers, cloud, and other domains. The processing and transmission of the data is done in this layer.
- **Application layer**—The processing of the sensor related data is done in network layer but in the application layer, the processing of sensor data (for creating an application-specific command and control) is done in the application.

Four Layer Architecture

Another very common architecture of Internet of Things environment is referred to as four-layer architecture as mentioned below:

- **Application layer**—This layer deals with the entire communication or application service between end-device and software application to control and monitor the entire IoT environment.
- **Data processing layer**—This layer handles the sensor data processing and sends it to the application in such a way that it is obtained from reliable/authorized source and is secure or protected from any kinds of threats for the network environment.
- **Network layer**—It is also known as transmission layer. The main responsibility of this layer is to connect the network elements, i.e., sensors, servers, routers, and other intermediatory devices and transmitting data between those devices and application layer.
- **Perception layer**—This is like a physical layer that consists of different elements or end-devices in an IoT environment. It is also known as sensor layer, which generates data based on the environmental conditions and processes that to digital information and sends to the network layer.

Five Layer Architecture

The five-layer architecture of IoT environment is more comprehensive with many functionalities and processes. The five layers of this architecture are:

- **Perception layer—**This like a physical layer and deals with the sensors, actuators, sensor embedded devices physically. This layer is similar to that of the three-layer model.
- **Transport Layer—**The transport layer deals with the communication to and from perception layer to the processing layer of this model. It deals with the interconnectivity of end-devices and the network elements such as routers, hubs, servers, and others.
- **Processing layer—**This layer deals with the data storing, processing, and analyzing of huge piles of data created through end-devices. The results are transported to the transport layer for further communication. It is also known as middleware layer of IoT architecture.
- **Business layer—**This layer deals with different business models used in the IoT business environment. The cloud-based different models are deployed under this layer of IoT ecosystem.
- **Application layer—**This is the upper layer of this model, which deals with the application services to provide the application-specific information to the end users of the IoT environment. The interface between the end-user and IoT system is established through this layer for monitoring and operational purposes.

What Is Decentralized Internet of Things Concept?

Decentralized IoT is a modern concept motivated by the prospects of highly cutting-edge technologies such as distributed ledger blockchain technology, multi-access edge computing (MEC), artificial intelligence (AI), and machine learning (ML). These technologies implemented into the IoT ecosystem provide highly effective, cost-efficient, reliable, secure, and robust solutions to the businesses. The deployment of MEC and blockchain technology into IoT is known as smart IoT or decentralized IoT. MEC improves scalability, efficiency, performance, and software defined resources to the nearest point in the cloud and blockchain develops high level of trust, security and reliability to the systems [190].

What Is Industrial Internet of Things?

Industrial Internet of Things, precisely referred to as IIoT, is also known as Industry 4.0 in the modern world. The IIoT is the concept of interconnection of a wide range of industrial sensors, actuators, machines, processes, and human beings simultaneously to enhance the level of automation in the industrial processes. This revolutionizes the industrial automation due to adaptation of power of artificial intelligence, machine leaning, big data analytics, cloud computing, edge computing, and many other modern technologies. The use of robotics with the control applications and other actors of different industrial processes are governed by numerous enabling technologies to take industrial automation to a new height.

Industrial Internet of Things Standard Bodies

All international and regional standard bodies that define different types of standards for different technologies and platforms are relevant to IIoT. In addition to those standards bodies, a few more domain-specific bodies that play very vital role in the enhancement of Industrial Internet of Things include the following:

- **Industrial Internet of Things Consortium (IIC)**—This is an object management body to provide standards useful for enhancing transformative business value in the industries. It was established in 2014 and provides the fundamental support on enhancing transformation of digital processes in a range of industries.
- **IoT Acceleration Consortium**—The main objective of this standard body is to combine different players such as academia, governments, industries, and research organizations to build a structure for developing, deploying, and operating the best technologies for industrial automation to enhance revolution 4.0 in the industries.

- **Alliance for Internet of Things Innovation (AIOTI)**—This is a very strong alliance of European academia, industries, IoT players, SMEs (Small and Medium-sized Enterprises), and others with a focus on the enhancement of creating dynamic European IoT ecosystem. This alliance was established in 2016.
- **Open Platforms Communication Foundation (OPC)**—The main objective of this platform is to build standards for the software developers, end-users, application platforms, industries, and other players for the smooth operations with strong interoperability of the devices, applications, interfaces, and operations and maintenance.

As mentioned earlier, IoT standards and regulations are under development and many of them have not yet matured, especially in the field of security, privacy, network connectivity policies and many other operations related matters. The above-mentioned bodies along with numerous other traditional international standard bodies are continuously working to streamline the development, deployment, operations, security, and privacy policies of this fast-growing domain of information technology.

Important Industrial Internet of Things IIoT Platforms

Industrial automation has become an integral part of almost every industry, especially mining, IT, oil and gas, aviation, automobiles, manufacturing, processing, operations and maintenance, community management, smart cities, civic utilities, etc. According to the Valuates Research information, the global market size of IIoT platforms is expected to cross USD $102.4 billion by 2028 from USD $71.16 billion in 2021 with a graceful growth rate of over 5.3% CAGR over the forecast period between 2022 and 2028 [192]. There are numerous major players with a sizeable share in the global IIoT platform market. A few of them are listed below:

- Azure IoT
- Oracle IoT Cloud
- IBM Watson IoT
- AWS IoT

- Siemens Mind Sphere
- Flutura Cerebra
- Thing Worx
- GE Predix.

Let us have a look into them individually with their respective features, capabilities, characteristics, and applications in certain industries.

Azure IoT

Azure IoT platform is a professional-grade IIoT application that supports numerous features such as SDK (Software Development Kit) for development, cloud computing, faster deployment, effective contracting and evaluation, and best support services. This platform is offered by Microsoft Corporation, which is an American technology giant.

Oracle IoT Cloud

Oracle IoT platform is a cloud-based efficient application for managing a wide range of devices under a unified monitoring and maintenance. It supports range of capabilities, especially big data management, data analytics, KPI (Key Performance Indicator) settings, performance monitoring automated functions to take action against any kinds of operational anomaly or security threats.

IBM Watson IoT

IBM's Watson is a highly powerful IoT system that uses high level of cognitive intelligence in its functionalities. It can support automation environment powered by machine learning, artificial intelligence and data analytics. It can support capabilities of large-scale device integration, operations and maintenance, data analysis, data virtualization, etc.

AWS IoT

Amazon Web Services (AWS) is the largest player in the cloud computing solutions. It offers professional platform for managing industrial devices in IoT environment. It is a very comprehensive platform that supports a wide range of operations and management environment that are based on high-grade automated solutions.

Siemens Mind Sphere

Siemens is one of the leading manufacturing companies based in Germany. The Siemens PLC automated systems for manufacturing industries are very well known worldwide. The MindSphere is the latest industrial automation platform from Siemens for effective O&M (Operations and Maintenance), integration, and security solutions in a range of manufacturing processes.

Flutura Cerebra

Cerebra IIoT platform is offered by Flutura. This is one of the pioneers in the IIoT software management and automation. It supports numerous modules and IoT networks for unified automation solutions in the industries. It is easy to add, configure, deploy, and manage a range of modules in IIoT ecosystem.

Thing Worx

Thing Worx is a comprehensive and end-to-end industrial automation platform that can integrate a variety of devices in IIoT ecosystem and collaborate through secure and reliable communication systems in such a way that an industrial-grade automation system is achieved for the operations and maintenance of a range of industrial processes.

GE Predix

General Electric Inc (GE) offers a cloud-based digital application for IIoT automation ecosystems. It is highly flexible, secure, scalable, and reliable platform that offers edge-to-cloud automation services in the IoT environment. It is a modular system that can support a range of modules such as HMI (Human Machine Interface), SCADA (Supervisory Control and Data Acquisition), ERP (Enterprise Resource Planning), Controller, Sensor, and others.

IIoT Use Cases in Different Industries

Industrial Internet of Things (IIoT) can be used in numerous applications across the industries. Many new concepts have been created due to the emergence of modern IIoT in different industries. The connected world of devices based on IIoT is used in many domains as example use cases. A few of them are listed below:

- Smart Cities
- Smart Home
- Manufacturing
- Process Automation
- Energy Management
- Supply Chain
- Healthcare
- Agriculture
- Military
- Transportation.

Let us know more about the use cases of Industrial Internet of Things in different domains of industries and walks of modern community management systems.

Smart Cities

The use of industrial IoT in smart cities is taking the center stage in the management of traffic, water supply, electricity, drainage systems, and many other civic services by using IIoT connectivity. Smart cities use numerous types of light sensors, water sensors, imaging sensors and other devices for collecting data from numerous systems in the modern cities and devise a comprehensive solution for managing the systems effectively and efficiently.

Smart Home

Smart home is another use case of IoT. A smart home is that one in which the lights, heaters, air-conditioning equipment, physical security, access control, cooking, and other processes are automated through integrated ecosystem based on IIoT platforms. The sensors send data to the controlling unit for processing and taking the suitable automated decisions based on pre-defined criteria of operations.

Manufacturing

Manufacturing has been using automated systems based on PLC (Programmable Logic Controller) for many years now. To clarify, a PLC is an industrial computer control system that continuously monitors the state of input devices and makes decisions based on a custom program to control the state of output devices. With the advent of modern IIoT platforms, the automation in manufacturing based on IoT platforms has taken a central position instead. A network sensor could be deployed to collect manufacturing process data. Again, it can be used to assess the efficiency and performance of the processes in manufacturing. The customized manufacturing, robotics, and safety mechanism are a few processes to name for this.

Process Automation

The automation of numerous processes that involve data from different elements to process and respond accordingly has been done through the usage of IIoT. Many operations and maintenance processes, data analysis processes, reporting and others are extensively automated through modern IIoT platforms.

Energy Management

The analysis of energy usage and its patterns in different conditions and circumstances are analyzed and proper plan are devised on the basis of that useful insight of the energy consumption in any industrial or commercial activities. This is known as energy management through automated system of connected devices. An IIoT-based solution for energy management can integrate multiple sources of energy and manage the most efficient use of the energy in your businesses.

Supply Chain

Supply chain has become highly automated in recent years as compared to the traditional models of supply chain management. Supply chain management is using numerous processes from quality control through delivery of the products to the client that are controlled by the automated processes managed by the IoT and associated software platforms. With the passage of time, the supply chain management will become fully automated and mechanized under the control of IIoT models.

Healthcare

Many automatic health monitoring tools have been introduced in the market place that can be governed and controlled through IIoT platform under the centralized control systems. The tracking of patient health, medical records, and doctor advises are possible to be monitored through IIOT platforms. The automated management of healthcare processes for elderlies are also extensively monitored through IoT network effectively.

Agriculture

Automation of irrigation systems based on the field monitoring and analysis results is known as automated agriculture. Modern IoT-based field monitoring and analysis systems have been developed to track different parameters such as crop density, moisture, temperature, humidity, crop health and other factors. Based on those results, an automated solution is devised to provide the required support to the crop in the form of watering, soil manuring, pesticide spraying, and other processes.

Military

An integrated and comprehensive ecosystem based on IoT is being used by almost all militaries in the world to track the positions of their own resources and spy on the resources and movements of the adversaries. A unified network of automation of the information collected from a range of sensors and radars can help the militaries extensively.

Transportation

Transportation is using integrated network of different elements of transportation networks such as tolls, roads, vehicles, speeds, traffic, and associated components. The major applications of IoT in transportation industry include, automated traffic management and signaling systems, toll collection, vehicle tracking, vehicle tax collection and monitoring, public transportation management, route management and other activities.

Challenges Posed by Internet of Things

The field of IoT is expanding unprecedentedly with millions of new devices getting added in just the matter of days and weeks. In such huge growth and unavailability of comprehensive regulation and control protocols, IoT poses numerous challenges for all concerned people in this field. Those challenges can be classified into many categories. A few of those main challenges associated with IoT are listed below:

- Cybersecurity
- Privacy
- Complex Operations and Management
- Environment Impact
- Bulky Data.

Let us have a closer look at those challenges to understand the reasons behind them.

Cybersecurity

Cybersecurity is one of the most important challenges posed by the ever-expanding environment of IoT worldwide due to numerous reasons and conditions. This topic will be dealt separately in the closing section of this chapter.

Privacy

When every device, equipment, appliance, or item that people use is exposed to the public through different ways such as monitoring and tracking systems, through less secure network, and multiple points of intrusion, the privacy of the users will be on stake for sure. The main reasons and causes of the violation of privacy of a person are directly associated with the security of the networks, which will further be discussed in the closing part of this chapter.

Complex Operations and Management

The operations and management devices are manufactured by a huge number of different manufacturers who use proprietary platforms and operating systems to run their products. This creates a great complexity to integrate all those types of devices, equipment, and items into an automated monitoring system that can support a range of operating systems, device features, specifications, and capabilities. Thus, the configuration, monitoring, and maintenance of the operations of the diverse set of equipment is a big challenge in the IoT environments. In fact, the absence of end-to-end compatible protocols, regulations, and agreement on procedures, makes the challenge even more difficult to cope with.

Environment Impact

Continuously increasing demand for the power and batteries used in the equipment will impact critically on the environment one way or the other. For instance, additional batteries for the equipment, routers, control systems, local equipment will require additional landfills/dumping yards and the impact on the environment will also be somewhat adverse.

Bulky Data

The IoT-based networks expand the volume of data rapidly. This data created by such gigantic networks will become so bulky that it will pose a big challenge to deal with or to deduce any valuable information from that data. The concept of big data basically deals with this and researchers are trying to come up with effective solutions as the data would be produced in terabytes. According to an estimated projection (at the time of writing this book), about 463 exabytes (1 exabyte = one billion gigabytes) of data will be created on a daily basis in 2025 [193]. Managing such a huge pile of data will become a big challenge for the concerned industry experts and technologists.

Impact of IoT on Cybersecurity

The impact of IoT environment on cybersecurity is huge due to many reasons. To understand those main causes associated with the IoT ecosystems that impact the cybersecurity can easily be understood when the main features of IoT are figured out (i.e., features that are directly related to cybersecurity). Let us figure out the key features of IoT ecosystem that would directly impact the cybersecurity [194].

- IoT is expanding exponentially without any strict rules and regulations
- IoT ecosystem is not mature yet and it will take time to get real maturity
- Number of devices is enormous
- All devices are not so powerful to support security measures and ensuring that is quite difficult
- Professional management of such a large network of devices is not possible always
- Compatibility and interoperability are other major issues
- Low power devices sometimes cannot connect with other devices continuously
- Diverse and easy to access locations for hackers is a big challenge for security
- Large volumes of data are stored in the cloud from where the data can be stolen
- Regular monitoring and upgrading of the devices are some big challenges
- Password management is very difficult in a large number of devices
- Lack of trained personnel and users with awareness about cybersecurity is a major challenge
- Lack of proper legislation and regulatory laws (which would work anywhere as it demands)
- Unavailability of in-built security features and capabilities in all types of devices used in IoT networks.

All above-mentioned characteristics of IoT networks or ecosystems pose serious threats to cybersecurity. The hackers can get physical access to devices connected to the IoT network. The number of devices increases the chance of hackers to intrude into the system. The less in-built security and devices with low computing power provide an easy way to intrude into the systems, especially into the cloud to compromise the valuable data. Managing and updating all software and firmware programs is not possible for such a huge number of devices because there is not enough sufficiently skilled manpower to carry out such a huge activity on a regular basis. This problem may not ever be solved! In such circumstances, the challenge to the cybersecurity is huge in the IoT ecosystems.