Internet of Things

Ajay Prasad
Thipendra P. Singh
Samidha Dwivedi Sharma *Editors*

Communication Technologies and Security Challenges in IoT

Present and Future

Springer

Internet of Things

Technology, Communications and Computing

The series Internet of Things - Technologies, Communications and Computing publishes new developments and advances in the various areas of the different facets of the Internet of Things. The intent is to cover technology (smart devices, wireless sensors, systems), communications (networks and protocols) and computing (theory, middleware and applications) of the Internet of Things, as embedded in the fields of engineering, computer science, life sciences, as well as the methodologies behind them. The series contains monographs, lecture notes and edited volumes in the Internet of Things research and development area, spanning the areas of wireless sensor networks, autonomic networking, network protocol, agent-based computing, artificial intelligence, self organizing systems, multi-sensor data fusion, smart objects, and hybrid intelligent systems.

Indexing: *Internet of Things* is covered by Scopus and Ei-Compendex **

Ajay Prasad · Thipendra P. Singh ·
Samidha Dwivedi Sharma
Editors

Communication Technologies and Security Challenges in IoT

Present and Future

Springer

Editors
Ajay Prasad
School of Computer Science
University of Petroleum and Energy Studies
Dehradun, India

Samidha Dwivedi Sharma
Department of Information Technology
Saudi Electronic University
Abha, Saudi Arabia

Thipendra P. Singh
School of Computer Science Engineering and Technology
Bennett University
Greater Noida, Uttar Pradesh, India

ISSN 2199-1073 ISSN 2199-1081 (electronic)
Internet of Things
ISBN 978-981-97-0051-6 ISBN 978-981-97-0052-3 (eBook)
https://doi.org/10.1007/978-981-97-0052-3

Preface

IoT is becoming part of our day-to-day activities. There are lots of areas where IoT has made its mark. There are many areas where IoT solutions are being or will be explored. The IoT is being adopted, incorporated, and envisioned in multiple areas of human life. It is also an area that is fast evolving. Also, many new communication technologies [8] are taking shape specifically suited for IoT in terms of problem solutions or domains. Major application domains include health care, industrial IoT, smart vehicles, agriculture, homes [6], cities, sustainability, etc. Different application domains will have a different set of challenges [1] in terms of implementation, mass expectations, mass acceptance, change management, privacy, security, etc. Challenges in terms of implementation will involve technology-related challenges. The available technology around IoT solutions has constraints and needs careful study before incorporation. The domains of IoT solutions as discussed in [5] desire high scalability, reliability, and availability. Above all, since the IoT adds to the comfort zones of people and organizations it is always going to be vulnerable to various attacks. There are challenges about sensor technologies, communication systems, communication protocols, edge computing [4], fog computing [2], etc. Both the technology and application areas in IoT involve several challenges that need to be pointed out. The book will present a collection of various challenges corresponding to both IoT application domains and IoT technology domains. The book will also present best practices that need to be followed while carrying out designing and developing IoT solutions. Every aspect of applications and corresponding technology will be covered through a set of case studies from several sources and industrial inputs. The book will be useful for IoT solution designers and developers to get initialization guidance and will help them channelize their approaches. Communication technologies play a vital role in IoT, and hence must be fast to adapt to the evolving security threats. It is obvious that apart from ensuring basic requirements of IoT solutions, security challenges of IoT and communication technologies and protocols are vital aspects of which a developer must be aware. The book is also designed to present the overall communication technologies and protocols used in IoT like focusing on the architecture and threat perseverance of each. The book also presents the new/future technological additions and changes coming up in communication

systems like blockchain in IoT [3] and its possible security aspects. The book will also cover security aspects in communication mechanisms in domain-specific IoT solutions about healthcare, smart cities, smart homes, smart vehicles, etc. The overall objective of the book is to assist IoT developers to have a good insight into available and upcoming communication technologies so that they can employ the best possible practices while designing and developing IoT solutions.

Organization of the Book

The book is organized in a fashion where the Communication methodologies and their security challenges are discussed in the first ten chapters. The range of discussion starts from various communication modes and models towards the quantum era. The later nine chapters focus on a few application areas of IoT ranging from smart logistics, Smart Homes to healthcare. Here the case studies and architectures are presented with suggestive approaches addressing several security issues. The last six chapters present the advancements in IoT communication each with a different view and related security aspects. The book is organized into twenty-six chapters. A brief description of each of the chapters follows:

Chapter "Communication Technologies and Security Challenges in IoT: An Introduction" sets the preamble of entire topic and gives a comprehensive outlook on the topic.

Chapter "IoT Communication Models and Modes of Connectivity" presents various standard ways in which sensor data can be communicated which are hereby referred to as "communications models" and various means that are used to establish connections between different entities of IoT which are hereby referred to as "modes of communication". The technologies pertaining to these are also presented.

Chapter "Challenges and Key Issues in IoT Privacy and Security" addresses the challenges of IoT security and suggests methods to improve its security so that more benefits can be realized by the growing number of connected devices and services.

Chapter "Security Challenges in IOT" presents another way of looking into IoT Security Challenges. It discusses various IoT security challenges, IoT security architectures, IoT security solution trust zones and boundaries, potential risks of IoT devices, notable cases of IoT security breaches, solutions to IoT security breaches, strategies for securing IoT data, and best IoT security practices.

Yet another way to look into IoT Challenges is to perceive the fact that IoT platforms are rapidly changing. Chapter "Survey of IoT Security: Application Areas, Threats and Solutions" presents different technologies currently in use and those still in the development stage. The enhancement of IoT security is the focus of current research into four distinct technologies: edge computing, fog computing, blockchain, and machine learning.

People can use SaaS, PaaS, IaaS, and other benefits of cloud computing even though many cloud computing providers, like Google, Microsoft, IBM, and Amazon, are moving toward adopting cloud technology, which is causing a noticeable increase

in the utilization of various cloud services. There are still numerous difficulties that users must overcome. Chapter "Security and Privacy Issues in Cloud and IoT Technology and Their Countermeasures" brings the Cloud into picture and relates the security challenges thus.

Chapter "Security Threats in IOT and Their Prevention" looks at IoT as layered architecture and discusses various security issues deeply in layer-wise fashion. It describes different kinds of security issues pertaining to each layer as a reference point for the beginners in IoT and discusses the means and methods to deal with these security threats.

In the context of IoT, Chapter "IPV6: Strengths and Limitations" focuses on the strengths and weaknesses of IPV6. It does give a good background of IPv6 and its transitioning intricacies.

Chapter "A Survey: Internet of Things (IoTs) Technologies, Embedded Systems and Sensors" brings in an elaborate study of various embedded systems such as Raspberry Pi, ZYNQ, Jetson, Altera Cyclone II, Beagle Bone, Odroid, STM32, and PSoC, were investigated, along with IoT communication protocols including IPv6, 6LowPAN, ZigBee, Bluetooth, Wi-Fi, LoRaWAN, Z-Wave, NFC, and Sigfox. Furthermore, a comparative analysis of the sensors utilized in these systems and their respective application areas has been provided.

Though the IP-based communications are more prevalent since the internet, the non-IP communications are taking charge in largely low-powered IoT setups. Chapter "Non-IP Based Communication in IoT: Handling Security Challenges" discusses IoT non-IP communication security issues. It outlines threats and attacks that can compromise the integrity and confidentiality of non-IP-based communication technologies and their inherent risks and vulnerabilities. Real-world case studies demonstrate non-IP-based IoT communication and analyze the security concerns and solutions in each scenario.

Bringing in the inevitable. Chapter "Security Challenges to IOT and Cloud-Based Systems in the Era of Quantum Attacks" discusses the threats to internetworked devices and their mitigation in the era of quantum computers.

Chapter "Overview of Internet of Things-Based Smart Logistics Systems" outlines essential technologies and effects of IoT-based smart logistics research and implementations, as well as their industry and regional distributions, are shown through a bibliometric analysis of articles published between 2008 and 2019.

Chapter "Fault Sensor Detection and Authentication Mechanism for Improving Quality of Services in Smart Homes" presents a fault sensor detection and authentication mechanism for improving the quality of services in smart homes. This chapter presents a fault identification mechanism of various sensors that help to resolve the fault and get the proper and enough information for various services. Further, the chapter validates the data source which helps to improve the data integrity.

Chapter "Security in IOT-Enabled Smart Agriculture Systems" discusses criteria for security based on a proposed architecture for smart agriculture that is irrespective of any core technologies that could be deployed. The authors confer the technology of IoT-based smart ecosystem for agriculture by estimating their framework, and

their claim. In addition, it also presents opportunities and trends of IoT claims for precise agriculture and specifies the open challenges and issues of IoT in agriculture.

Chapter "Comprehensive Study of Intelligent Transference System in a Contemporary IoT Commuting Environment" discusses resourceful message communication amid the automobiles and RSUs in IoT setup for the Intelligent Transference System.

Chapter "Redefining Urban Development: Technology and Automation in India" explores the significance of technology and automation in transforming urban development in India. It highlights the key areas where technology and automation can revolutionize urban planning, infrastructure, governance, and sustainability. Additionally, the challenges and opportunities associated with implementing technology-driven solutions are discussed, along with examples of successful initiatives in Indian cities.

Chapter "Trust-Free Homes: The Zero-Trust Paradigm in a Smart Home Setting" is aimed to serve as a guide to implementing a Zero-Trust network model in Smart Home systems.

Chapter "Security Challenges of IoT-Enabled Vehicular Communications and Their Countermeasures" provides a comprehensive overview of the state of the art in this area and identifies challenges and solutions for securing current and future IoT-enabled vehicular communications.

Chapter "Industrial IoT Security Infrastructures and Threats" discusses essential ways to mitigate cyber-attacks on Industrial IoT systems and is presented with a comprehensive review and security strategy that includes risk assessment, threat modeling, and vulnerability testing as well as the proposed countermeasure models keeping IoT infrastructure in context.

Chapter "Industrial IOT: Security Threats and Counter Measures" comprehensively examines the security threats faced by industrial IoT systems and presents effective countermeasures to mitigate these risks. By exploring the unique characteristics of IIoT environments, such as interconnectedness, heterogeneity, and resource constraints, this study identifies potential vulnerabilities that can be exploited by adversaries.

Chapter "Internet-of-Things Enabled Smart Health Monitoring System Using AutoAI: A Graphical Tool of IBM Watson Studio" presents the use of internet-of-things (IoT) enabled smart health monitoring systems to improve healthcare service quality using a method including IBM Watson studio and AUTO AI services to produce a real-time warning and precise predictions of patient health.

Chapter "Phase Noise Performance of MIMO—GFDM Systems for Millimeter Wave 5G Technology" provides an understanding of phase noise effects and their implications for MIMO-GFDM systems, thus enhancing the development of efficient communication systems for millimeter wave 5G networks.

Chapter "Credit Card Fraud Detection Using Deep Learning for Internet-of-Things Enabled Smart Digital Financial System" discusses cases of a few machine learning-based and deep learning-based methods for Internet-of-Things-enabled smart digital financial systems and the associated difficulties.

Chapter "Development of a Secure and Transparent Blockchain for Electricity Bill Management in Smart Cities Using Enhanced Proof of Energy Consumption"

presents a case of a blockchain-based model for electricity use in smart cities to address the issues of maintaining transparency and protecting consumers' privacy.

Chapter "A Comparative Study of Threat Detection for IoT Devices Using Machine Learning Techniques" brings forth a study of threat Detection for IoT Devices Using Machine Learning Techniques and examines how machine learning is applied to the IoT defense.

Chapter "Exhaustive Theoretical Study of Practical Free Space Optical Cooperative Relaying Technology: New Trends in IoT Communication" discusses a new trend of communication in IoT, i.e., "Optical Cooperative Relaying Technology". It brings insights into the key components of Optical Wireless transmission and to highlight various factors that need to be included in mixed radio/ Optical Wireless relaying systems to quantify the impact of its practical problems.

Dehradun, India — Ajay Prasad
Greater Noida, India — Thipendra P. Singh
Abha, Saudi Arabia — Samidha Dwivedi Sharma

References

1. Abiodun, O.I., Abiodun, E.O., Alawida, M. et al. A Review on the Security of the Internet of Things: Challenges and Solutions. Wireless Pers Commun 119, 2603–2637 (2021). https://doi.org/10.1007/s11277-021-08348-9
2. Adel, A. Utilizing technologies of fog computing in educational IoT systems: privacy, security, and agility perspective. J Big Data 7, 99 (2020). https://doi.org/10.1186/s40537-020-00372-z
3. Alfa, A.A., Alhassan, J.K., Olaniyi, O.M. et al. Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions. J Reliable Intell Environ 7, 115–143 (2021). https://doi.org/10.1007/s40860-020-00116-z
4. Jazaeri, S.S., Jabbehdari, S., Asghari, P. et al. Edge computing in SDN-IoT networks: a systematic review of issues, challenges and solutions. Cluster Comput 24, 3187–3228 (2021). https://doi.org/10.1007/s10586-021-03311-6
5. Kaur, J., Jaskaran, Sindhwani, N., Anand, R., Pandey, D. (2023). Implementation of IoT in Various Domains. In: Sindhwani, N., Anand, R., Niranjanamurthy, M., Chander Verma, D., Valentina, E.B. (eds) IoT Based Smart Applications. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-031-04524-0_10
6. Touqeer, H., Zaman, S., Amin, R. et al. Smart home security: challenges, issues and solutions at different IoT layers. J Supercomput 77, 14053–14089 (2021). https://doi.org/10.1007/s11227-021-03825-1
7. Waverley Team and Iryna Hladun, TOP 12 TECHNOLOGY TRENDS IN IOT TO WATCH FOR IN 2023, June 21, 2023, https://waverleysoftware.com/blog/top-iot-tech-trends/

Acknowledgements

Editing a book is harder than we thought. None of this would have been possible without so many persons behind us. And this is next to impossible to enlist them here. The editors want to thank all those who were directly or indirectly involved in the project.

The editors want to thank their families, colleagues, and all well-wishers who helped them in achieving this milestone. We also want to put on record our appreciation for our respective Organizations **University of Petroleum and Energy Studies, Bennett University**, and **Saudi Electronic University** and their respective management to provide such a wonderful opportunity to let us grow academically.

Although the entire period of editing the book was filled with many ups and downs, our time with colleagues at office was worth of priceless. Many a time we felt low but people around us kept going. Our heartfelt thanks to you all.

Above and over, we feel thankful to the almighty to shower all His blessings upon us to complete this project.

Dr. Ajay Prasad
Dr. Thipendra P. Singh
Dr. Samidha Dwivedi Sharma

Contents

Communication Technologies and Security Challenges in IoT: An Introduction

Ambrish Kumar, Ajay Prasad, and Thipendra P. Singh

Abstract The Internet of Things (IoT) has become integral to our daily lives. IoT is tightly governed by the principles of communication and the technologies around it. Thus an in-depth discussion on Communication Technologies and Security Challenges in IoT is required for a professional to design and develop IoT applications. The core aspects that need elaborate discussion are being brought forward in this chapter. It is identified here that three major aspects of IoT Security are vital and require extensive discussion. They are, Communication methodologies and their security challenges, Application areas and approaches addressing several security issues, and the advancements/New trends in IoT communication and related security aspects.

Introduction

Kevin Ashton first used the term "Internet of Things" (IoT) in 1999, and the International Telecommunication Union (ITU) formally adopted it in 2005. The interconnectivity of IoT devices is also referred to as a "Network of Things" (NoT) [1]. Every NoT has a distinct function and goal, and together they make up the overall Internet of Things [2]. A global network of interconnected physical and virtual objects that are embedded with sensors, software, and network connectivity that allows these objects to gather and exchange data is what the ITU defines as the Internet of Things. These gadgets can be anything from basic household items to highly advanced industrial tools. Establishing independent connections between actual objects and applications

A. Kumar · T. P. Singh
School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India
e-mail: ambrish.kumar@bennett.edu.in

T. P. Singh
e-mail: thipendra@gmail.com

A. Prasad (✉)
School of Computer Science UPES, Dehradun, India
e-mail: aprasad@ddn.upes.ac.in

A. Prasad et al. (eds.), *Communication Technologies and Security Challenges in IoT*, Internet of Things, https://doi.org/10.1007/978-981-97-0052-3_1

to facilitate information transfer and intelligent decision-making is the core concept of the Internet of Things. IoT makes it possible to link real-world activities to digital ones, which spurs the creation of a wide range of services and applications that are advantageous to professionals, enterprises, and individuals alike. The Internet of Things (IoT) is growing quickly; projections indicate that there will be more than 75 billion connected devices globally by 2025. Technological developments, falling costs, and the growing need for connected devices and services are the main drivers of this growth.

IoT System Model

The IoT is having a transformative impact on various industries, including healthcare, manufacturing, logistics, and smart cities. It enables new levels of automation, efficiency, and personalization. A generic IoT system model can be represented by three key layers [3]. Perception Layer, Transportation Layer, and Application Layer. Each of these layers summarized in Fig. 1 has its technologies that bring issues and some possible security weaknesses.

- **Perception Layer (PL)**: The Perception layer is responsible for collecting the data from the physical objects using sensors, actuators, and other embedded devices.
- **Transportation Layer (TL)**: The transportation layer is mainly responsible for transmitting the data between the perception layer(PL) and the application layer (AL). The data is typically transmitted over wireless networks, for example, Wi-Fi, Bluetooth, and cellular networks.
- **Application Layer (AL)**: In addition to offering services to consumers, the application layer is in charge of handling and assessing the data it receives from the

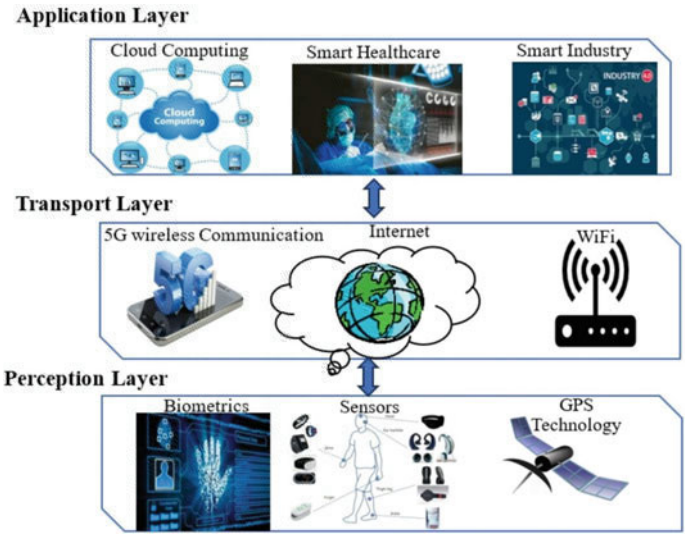

Fig. 1 IoT system model

layer of perception. This layer typically consists of software applications that can control the overall IoT system.

IoT Communication Models and Technology Requirements

The best communication technology for a particular IoT application will depend on several factors, including the range required, and the power consumption. The most commonly used communication technologies in IoT are as under:

- **IoT (Internet of Things) Sensors and Models of Communication Systems** [4]: Wireless sensor networks (WSNs) are used to connect and manage large numbers of low-power devices. These networks typically use short-range communication protocols such as ZigBee, Thread, and Bluetooth Low Energy (BLE). The networks are often used in industrial and environmental monitoring applications such as monitoring the temperature, humidity, and vibration of equipment in a factory or the air quality in a city.
- **Low-Power Communication Systems** [5]: Low-power communications are used to connect devices over long distances with low power consumption. Networks typically use protocols such as LoRaWAN, NB-IoT, and Sigfox. These networks are often used in smart cities and smart agriculture applications, for example, to monitor the level of water in a reservoir or the temperature of crops in a field.
- **Long-Range Communication Systems** [6]: Cellular networks are used to provide high-speed, reliable connectivity for long-range communication to IoT devices. Cellular networks typically use protocols such as LTE-M and LTE Cat-1. These networks are often used in connected car and wearable device applications, for example, to track the location of a vehicle or to monitor the health of a person wearing a fitness tracker.
- **Non-Internet Protocol (NON-IP) based Communication Systems** [7]: Cellphones and additional gadgets are frequently connected to Internet of Things (IoT) devices via Bluetooth connectivity, a short-range communication technology. IoT devices are frequently connected to smartphones and other devices via Bluetooth. It can be used to connect a smartwatch to a smartphone or a smart thermostat to a smartphone app.
- **Wireless Fidelity (*Wi-Fi)***: IoT devices are frequently connected to home networks and other Wi-Fi networks via Wi-Fi, a medium-range communication protocol. IoT devices are frequently connected to home networks and other Wi-Fi networks via Wi-Fi. Additionally, it can be used to link a smart doorbell to a Wi-Fi-enabled doorbell chime or a smart speaker to a home network.
- **Ethernet**: IoT devices are frequently connected to wired networks via Ethernet, a high-speed communication protocol. IoT device connections to wired networks are frequently made using it. Additionally, it can be used to link a smart TV or security camera to a wired network.

IoT Sensors and Models of Communication

Sensors are key components of the IoT system for gathering information or data from physical objects and converting the data into digital signals for processing and analysis. These sensors can be extremely important in Internet of Things applications since they allow for automation, data-driven decision making, and continuous surveillance. Communication models in IoT systems define the way data is exchanged between devices, networks, and applications. These models play a significant role in ensuring efficient and reliable data transmission, especially in large-scale IoT deployments.

IoT Sensors: According to the Measurement Capabilities, IoT Sensors can be Defined as Follows

- **Environment Sensors**: These sensors measure environmental parameters such as temperature, humidity, pressure, light, and air quality. They are widely used in weather monitoring, smart homes, and industrial control systems.
- **Motion Sensors**: These sensors detect motion, including acceleration, tilt, and rotation. They are used in security systems, wearables, and robotics.
- **Proximity Sensors**: These sensors detect the presence of nearby objects. They are used in collision avoidance systems, proximity sensing for user interaction, and gesture recognition.
- **Chemical Sensors**: These sensors detect the presence and concentration of specific chemicals. They are used in environmental monitoring, industrial process control, and healthcare applications.
- **Biological Sensors**: These sensors detect biological phenomena such as heart rate, blood pressure, and blood glucose levels. They are used in wearable health monitoring devices and medical diagnostics.

Communication Models

Common Communication Models for IoT Applications Are as Follows [8].

- **Client–Server Model**: In this model, IoT devices act as clients, requesting data or services from servers. The server responds to client requests and provides the requested information or services. This model is widely used in web-based IoT applications.
- **Publish-Subscribe Model**: In this model, devices publish data to a central broker or messaging system. Subscribers interested in the data can subscribe to the topic and receive updates whenever new data is published. This model is well-suited for real-time data dissemination and event-driven applications.
- **Peer-to-Peer Model**: In this model, devices communicate directly with each other without the need for a central server or broker. This model is often used in mesh networks and applications that require decentralized control and data sharing.
- **Hybrid Models**: Combinations of the above models can be used to create more complex and flexible communication architectures for specific IoT applications (Fig. 3).

Communication Methodologies and Their Security Challenges

Many IoT devices are vulnerable to attack due to weak or default passwords, inadequate authorization mechanisms, insecure communication protocols, lack of regular software updates and security patches, limited resources, and the heterogeneous nature of the IoT landscape. An overview of security challenges in IoT systems that needs to be tackled is presented in Fig. 2. IoT device growth presents a number of security problems that should be carefully considered. Vulnerabilities in IoT devices due to their limited computing capacity can make them susceptible to viruses and hacking attempts, exacerbated by the absence of regular security updates. Privacy and data integrity are paramount, particularly in sensitive domains like healthcare and smart cities, where securing the confidentiality and integrity of data is imperative. Additionally, the scalability of IoT ecosystems, often comprising millions of devices, poses significant challenges to conventional centralized security methods. Ensuring that only authorised users can interact with IoT devices requires robust access control and authentication procedures. This is because poor or nonexistent authentication can result in unauthorised access and data breaches. This study examines the various security issues that arise in the Internet of Things environment and addresses appropriate risk mitigation techniques. Therefore, security is a critical concern for IoT systems, as they collect and transmit a vast amount of sensitive data. By understanding the security challenges at each layer of the IoT system, organizations can take steps to mitigate these risks and protect their data and systems. The security challenges at different layers of the IoT system are described in Table 1.

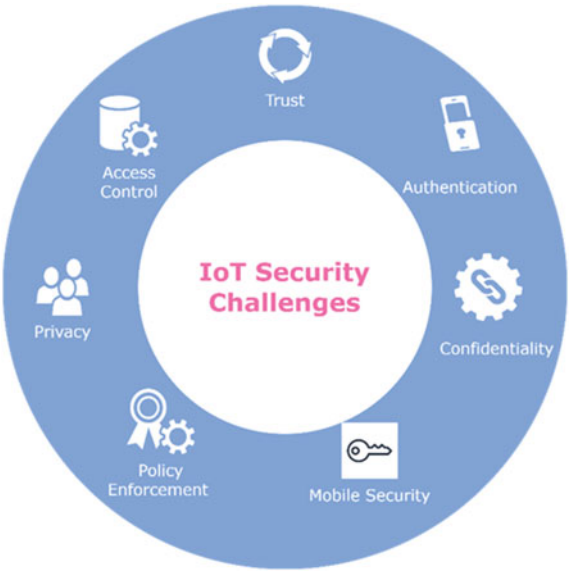

Fig. 2 An overview of security challenges in IoT systems

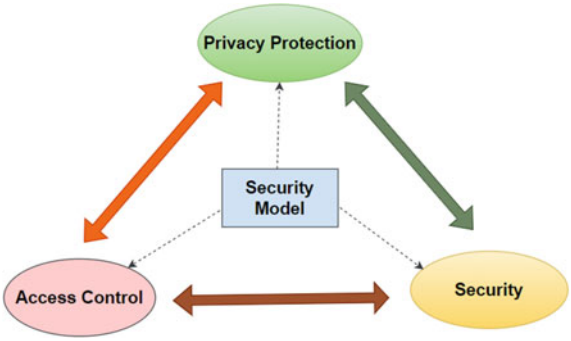

Fig. 3 Security model of the IoT system

Table 1 Threats in IoT system model

Layer	Main threats
Prediction layer	Data leakage
	DoS attacks
	Malicious code injection
Transportation layer	Routing attacks
	DoS attacks
	Data transmit attacks
Application layer	Physical attacks
	Impersonation
	DoS attacks
	Routing attacks (e.g. in WSN, RSN)
	Data transmit attacks (e.g. in WSN, RSN)

Challenges at the Perception Layer

- **Data Tampering at Physical Object**: An Internet of Things system's data obtained through a sensor node may contain inaccurate or deceptive information. Furthermore, a physical injection of malicious malware could grant an attacker access to the IoT system.
- **Impersonation**: During the authentication process, an attacker may use a fictitious identity to launch harmful attacks against an IoT system.
- **Denial of Service (DoS)**: An attacker uses the legitimate node's limited processing power to prevent it from accepting new requests for service.
- **Routing attacks**: The routing pathway of the network is changed by a malicious intermediary node during the data collection and forwarding operation.
- **Data transit attacks**: These happen when an attacker compromises the integrity and confidentiality of information being transported throughout the data processing process..

Security Challenges at the Transportation Layer

- **Interception**: Internet of Things (IoT) gadgets may be employed to track adherence to medications, keep an eye on the vitals of patients, and offer distant treatment.
- **Manufacturing**: IoT devices can be used to optimize production processes, monitor equipment health, and track inventory levels.
- **Logistics**: IoT devices can be used to track shipments in real-time, optimize delivery routes, and reduce costs.
- **Smart Cities**: IoT devices can be used to monitor traffic congestion, optimize energy consumption, and improve city services.

Security Challenges at the Application Layer

- **Unauthorized Access**: A malicious actor can access the application server or cloud infrastructure that can steal or modify the system configurations in order to disturb the IoT system.
- **Vulnerabilities in Application Software**: An adversarial node may utilise the application software to obtain private information or take over the Internet of Things.
- **Data Breaches**: A malicious node can expose the sensitive information about the users of the IoT system itself.

Communication Protocols in IoT Systems

The Internet of Things (IoT) depends on protocols for communication to facilitate data flow and device engagement [8]. By defining the guidelines and formats for data transfer, these protocols guarantee interoperability and compatibility across various internet of things networks and devices.

- **Internet Protocol Version 6 (IPv6) protocols**

  IPv6 is the successor to IPv4, the current protocol that underpins the Internet. IPv6 has been in development since the early 1990s and was officially standardized in 1998. However, it has only recently begun to be widely adopted. Some key IPv6 protocols can be described as follows.
- **Control Message Protocol version 6 (CMPv6)**: CMPv6 is responsible for sending control messages between IPv6 devices, such as error reports and diagnostic information.
- **Neighbor Discovery Protocol (NDP)**: NDP protocol is used to discover and maintain neighbor relationships between IPv6 devices on a local network.
- **Stateless Address Autoconfiguration (SLAAC) Protocol**: SLAAC allows IPv6 devices to automatically configure their own IP addresses without requiring manual configuration or DHCP servers.
- **Dynamic Host Configuration Protocol version 6 (DHCPv6)**: It is an additional sophisticated method for configuring IPv6 devices with an IP address alongside additional network-related settings.
- **Path MTU Discovery (PMTUD) Protocol**: In order to prevent message fragmentation and increase transmitting effectiveness, the PMTUD protocol is used to calculate the maximal transmitting unit (MTU) size over a network path.

- **Multicast Listener Discovery (MLD) Protocol**: In order to control multicast group membership and guarantee that multicast packets are only sent to interested devices, the MLD standard is utilised.
- **Secure Neighbor Discovery (SND) Protocol**: This protocol provides cryptographic authentication for neighbor discovery messages to prevent attackers from impersonating other devices and disrupting network communications.
- **Authentication Header (AH) Protocol**: The AH protocol provides optional authentication and integrity protection for IPv6 packets.
- **Encapsulating Security Payload (ESP) Protocol**: It can provide optional encryption and authentication for IPv6 packets.

Internet Protocol (IP)-Based Protocols

Internet protocol (IP)-based is the fundamental aspect of the IoT system. It is an underlying protocol suite that enables devices to exchange data between objects over the internet [9]. In IoT, IP-based communication is very important as it can manage and connect a vast network of devices by enabling them to share information. IP-based communication is a cornerstone of the IoT, providing a standardized, scalable, and secure framework for connecting and managing a vast network of devices. Its integration with existing infrastructure, support for diverse network technologies, and ability to accommodate future protocols make it an essential enabler for the continued growth and development of the IoT. The key IP-based communication protocols given in Table 2 can be described as follows.

- **Transmission Control Protocol (TCP)**: The connection-oriented protocol TCP offers dependable and systematic transfer of information across apps. In order to ensure the confidentiality of information and avoid loss or fraud, it connects both ends, divides the data into segments, then reconstructs these at the point of reception.

Table 2 Communication protocols in IoT systems

IPv6 protocol	IP based protocol	Non-IP based protocol	RFID protocols	NFC protocols
CMPv6	TCP	LoRaWAN	EPC Class 1 Generation 2 (ISO 18000–3)	TNEP
NDP	UDP	Sigfox	Mifare (ISO 14443)	DOP
SLAAC	IP	Zigbee	EPCglobal Gen 2	BCP
DHCPv6	ICMP	BLE	UHF RFID	LAC
PMTUD	ARP	6LoWPAN	HF RFID	SNEP
MLD	DHCP		LF RFID	SNEP +
SND				
AH				
ESP				

- **User Datagram Protocol (UDP)**: UDP is a connectionless protocol that provides best-effort data delivery between applications. It sends data packets without establishing a prior connection, making it faster and less overhead-intensive than TCP. UDP is suitable for applications where data delivery is less critical, such as streaming audio or video.
- **Internet Protocol (IP)**: The network layer protocol known as IP is responsible for addressing and directing information packets over the Internet. It gives devices and networks distinct IP addresses, allowing routing algorithms to choose the most efficient route for information packets to take in order to get to their intended location.
- **Internet Control Message Protocol (ICMP)**: ICMP is a network layer protocol used for sending control messages between devices. It provides error reporting, diagnostic information, and network management capabilities, enabling troubleshooting and monitoring of network connectivity and performance.
- **Address Resolution Protocol (ARP)**: ARP is a protocol at the network layer that maps IP addresses to MAC addresses. By doing so, devices on the same local network are able to communicate directly with one another by learning the physical MAC address of a device linked to an IP address that is particular.
- **Dynamic Host Configuration Protocol (DHCP)**: A protocol at the network layer called DHCP is used to give IP addresses and other network configuration parameters to connected devices dynamically. It lowers administrative cost and streamlines network administration, especially in large networks with changing configurations of devices.

Protocols not Based on IP

The IoT applications can benefit greatly from non-IP-based connectivity [7]. These protocols are appropriate for limited IoT contexts due to their low power consumption, low latency, and immunity to interference, in contrast to IP-based communications. The following is a description of the non-IP-based protocols listed in Table 2.

- **Wide Area Network for Long Range (LoRaWAN)**: Using chirp spread spectrum technology, LoRaWAN is a low-power wide-area network (LPWAN) protocol that enables low-power, long-range communication. It works especially well with Internet of Things devices that need to transmit data only sometimes, like asset tracking devices and sensors for environmental monitoring.
- **Sigfox**: This other LPWAN protocol makes use of ultra-narrowband technology to provide low-power, long-range communication. While operating at a higher frequency than LoRaWAN, it is comparable and allows for quicker data throughput. IoT devices like smart parking systems and smart metres that need to transmit data sometimes are a good fit for Sigfox.
- **Zigbee**: Zigbee is a low-power wireless personal area network (WPAN) protocol that uses the unlicensed 2.4 GHz frequency. It is frequently utilised in enclosed spaces, such smart homes and buildings, for short-range communication between

IoT devices. Mesh networking is made possible via Zigbee, which allows devices to relay data for greater coverage.

- **Bluetooth Low Energy (BLE)**: BLE is a low-power Bluetooth wireless protocol variation created especially for short-range, low-power communication. In order to facilitate data sharing and configuration, it is frequently used to couple Internet of Things devices with smartphones or tablets. Beacon technology, which enables proximity-based location tracking applications, is another application that uses BLE.
- IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): Zigbee and 802.15.4 are examples of low-power wireless networks that can support IPv6 communication thanks to the 6LoWPAN protocol. It changes IPv6 packets into more manageable, smaller datagrams that can be sent over these low-power networks. IoT devices can join bigger IoT ecosystems and connect to the Internet thanks to 6LoWPAN.

Protocols for radio frequency identification (RFID)

RFID [10, 11] technology can wirelessly identify and monitor objects, it has become a critical enabler for the Internet of Things. RFID readers enable real-time tracking and monitoring of a variety of assets by the attachment of RFID tags, which are embedded with unique IDs. These guidelines consist of.

The most popular RFID protocol is EPC Class 1 Generation 2 (ISO 18000–3), which is especially useful for supply chain management and asset monitoring applications. It can read at a distance and operates in the ultra-high frequency (UHF) band.

- Mifare (ISO 14443): Applications for contactless payments and proximity cards frequently employ this protocol. It provides a good mix of performance and range while operating in the high frequency (HF) band.

Another well-liked protocol for contactless and proximity card applications is iCOde (ISO 15693). It provides a performance and security combination while operating in the HF band.

- EPCglobal Gen 2: Developed by EPCglobal to improve interoperability and compatibility among RFID systems, this is a standardised version of ISO 18000–3. It specifies extra requirements for reader communication, tag identification, and data encoding.
- RFID systems that operate in the UHF band, usually at frequencies between 860 and 960 MHz, are referred to as Ultra High Frequency (UHF) systems. Because UHF RFID tags can read over a long distance, they are useful for inventory management and asset tracking applications.
- High Frequency (HF) RFID: This describes RFID systems that use frequencies in the HF band, usually 3.56 MHz to 13.56 MHz. Due to its ability to balance performance and range, HF RFID tags are a good fit for contactless payment applications, access control systems, and proximity cards.

- RFID systems that operate in the LF region, usually at frequencies between 30 and 500 kHz, are referred to as low-frequency (LF) systems. Although LF RFID tags have a limited reading range, they are less prone to interference and can pass through metal and water.

Protocols for Near Field Communication (NFC)

NFC [12] is a 13.56 MHz short-range wireless communication technology which enables data sharing between two devices when they are near together, usually less than 10 cm. NFC is commonly utilised in mobile phones, contactless payment cards, and other devices for peer-to-peer data transfer, access control, and secure transactions. Numerous NFC protocols are optimised for Internet of Things applications, providing improved functionality and features catered to the particular requirements of IoT networks and devices. These guidelines consist of.

- Tag NDEF Exchange Protocol (TNEP): NFC-enabled devices can communicate with one other by exchanging NDEF (Near Field Communication Data Exchange Format) messages thanks to this lightweight protocol. NDEF messages are appropriate for a variety of Internet of Things applications since they can contain multiple data kinds, including text, URLs, and contacts.
- Device Orientation Protocol (DOP): NFC devices can detect their relative positions and orientations by exchanging orientation information using the standardised method provided by DOP. Applications like augmented reality and indoor navigation that depend on exact placement need this information.
- Battery Check Protocol (BCP): BCP enables power management and guarantees that devices have enough power for communication by enabling NFC devices to inquire about the battery level of other NFC devices.
- Logical Access Control (LAC) Protocol: NFC devices can transmit sensitive data, including encryption keys and authentication credentials, via a secure channel with LAC. Applications that need higher security, such financial transactions and access control systems, depend on this protocol.
- Simple NDEF Exchange Protocol (SNEP) Protocol: This protocol is designed to make it easier for NFC devices to exchange NDEF messages with one another. It is especially helpful for low-power Internet of Things sensors and tags, as well as other devices with constrained memory or processing capabilities.
- Secure NDEF Exchange Protocol (SNEP+): SNEP+ uses Secure Sockets Layer (SSL) encryption to improve the security of NDEF message exchange. Applications requiring the highest level of security, like sensitive data sharing and financial transactions, are advised to use this protocol.

Securing IoT Applications

The network of physically connected objects that communicate and share data with one another over the Internet is known as the Internet of Things (IoT). IoT applications offer creative answers to a variety of problems across a broad range of sectors and use cases. Figure 4 displays a few typical IoT applications from various industries.

The domains listed in Fig. 4 are just a few examples, and the applications of IoT continue to expand as technology advances. The potential of gadgets together and exchange data in real time opens up numerous possibilities for improving efficiency, reducing costs, and creating new services across various industries.

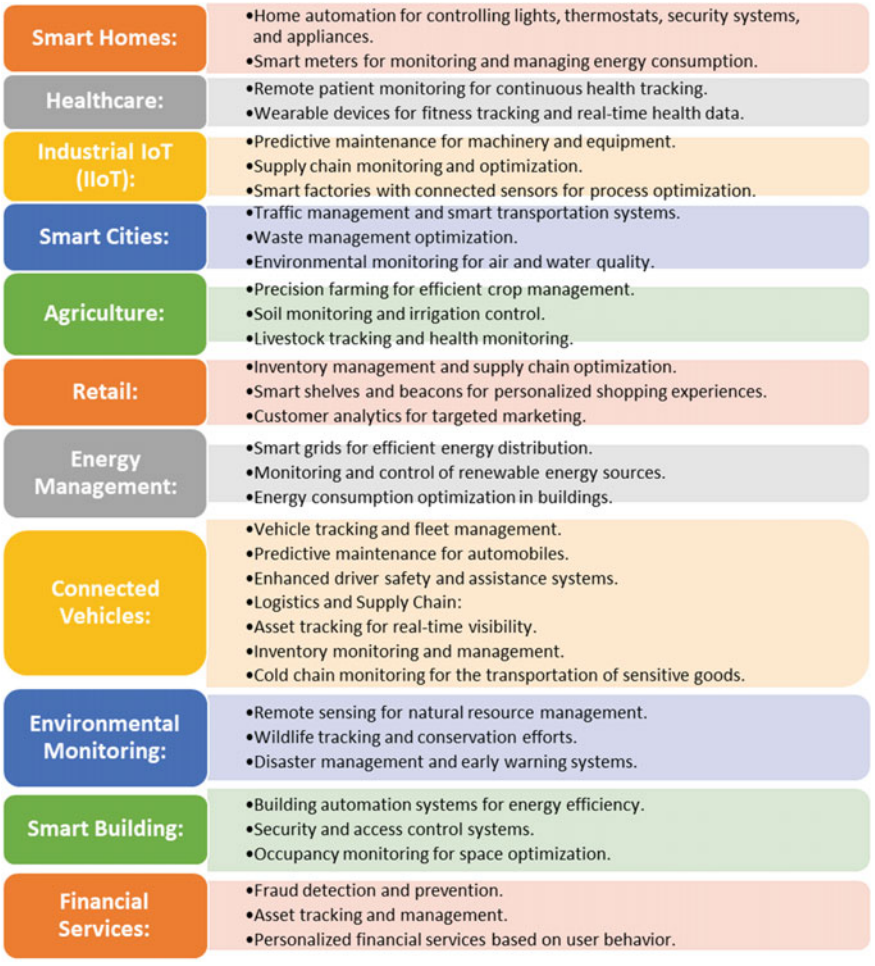

Fig. 4 IoT application domains

Ensuring the security of IoT applications is paramount in safeguarding the interconnected network of devices that form the Internet of Things (IoT) [13]. With the proliferation of connected gadgets across various industries, the complexity of securing these applications has grown exponentially. Robust security measures begin with strong device authentication, utilizing unique identifiers and secure key management protocols. Secure communication channels, employing encryption methods such as TLS or DTLS, are important to safegaurd data in transit. Regular firmware updates and patch management are critical for addressing vulnerabilities and maintaining the resilience of IoT devices. Network security, both through segmentation and the deployment of firewalls and intrusion detection systems, helps mitigate the impact of potential breaches. Physical security measures, including tamper-evident packaging and access controls, add a layer of protection. Privacy considerations, user education, and compliance with regulatory standards contribute to a holistic approach to IoT application security. Ongoing security testing, incident response planning, and vendor security assessments are integral components of a comprehensive strategy to identify and address potential threats in this dynamic and evolving landscape.

When studying IoT (Internet of Things) application security, there are several factors that need to be considered. Here are some key areas to focus on:

Device Security

Put robust permission and authentication processes in place to manage who has access to IoT networks and devices. To limit access to authorised users exclusively, utilise restricted access lists, encryption, and distinctive passwords. There are a number of factors to consider when thinking about IoT device safety [14]. Following are a few important things to think about:

- Secure Hardware Design: Ensuring that the hardware components of IoT devices are designed with security in mind. This includes using secure elements for storing cryptographic keys, implementing tamper-resistant hardware, and protecting against physical attacks.
- Secure Software Development: Following secure coding practices during the software development process for IoT devices. This includes minimizing vulnerabilities such as buffer overflows, input validation issues, and insecure configurations. Secure coding practices should also address authentication, encryption, and access control mechanisms.
- Authentication and Authorization: Implementing best authentication mechanisms to verify the identity of IoT devices and users accessing the devices. This may involve using unique device credentials, digital certificates, or secure tokens. Additionally, implementing proper authorization mechanisms to control device access and permissions is crucial.
- Encryption and Data Protection: Encrypting sensitive data both at rest and in transmission. This includes using strong encryption algorithms to safegaurd information from unauthorized access or tampering. Encryption should cover communication between devices, as well as data stored on the device and transmitted to the cloud or other systems.

- Over-the-Air (OTA) Updates: Implementing a safe and robust mechanism for delivering OTA updates to IoT devices. This includes verifying the authenticity and integrity of updates, ensuring secure communication channels for delivering updates, and providing rollback mechanisms in case of failed updates.
- Physical Security Measures: Protecting the physical integrity of IoT devices to prevent unauthorized access, tampering, or theft. This may involve using tamper-evident seals, secure enclosures, and physical access controls.
- Secure Communication Protocols: Using secure communication protocols, such as HTTPS, MQTT with TLS, or CoAP with DTLS, to establish encrypted and authenticated communication between devices and other components in the IoT ecosystem. This helps protect data privacy and integrity.
- Device Management and Monitoring: Implementing robust device management and monitoring capabilities to detect and respond to security events. This includes monitoring device behavior, detecting anomalies, and implementing mechanisms for remote device management, such as revoking device access or disabling compromised devices.
- Privacy Considerations: Considering privacy implications when designing IoT devices. Minimizing the collection and use of personal data, implementing privacy-by-design principles, and complying with relevant privacy regulations are important aspects of IoT device security.
- Security Testing and Vulnerability Management: Conduct regular security testing, including penetration testing and vulnerability assessments, to identify and remediate security vulnerabilities in IoT devices. Establishing a process for managing and patching vulnerabilities is crucial to maintaining the security of IoT devices over their lifecycle.

It's important to note that IoT device security requires a holistic approach, considering both hardware and software components, as well as the broader ecosystem in which the devices operate.

Data Security

Encrypt data at rest and in transit to protect it from unauthorized interception or tampering. Use secure protocols like HTTPS, TLS/SSL, and IPSec for data transmission. Implement data encryption algorithms like AES, RSA, or ECC to safeguard sensitive data. Data security in IoT (Internet of Things) applications is a critical aspect that involves protecting the confidentiality, integrity, and availability of data generated and exchanged by connected devices. Several key considerations contribute to robust data security in IoT applications [15]:

- Encryption: Utilize strong encryption algorithms to protect data both in transit and at rest. This prevents unauthorized access to sensitive information as it travels between devices and the cloud.
- Authentication and Authorization: Implement secure authentication mechanisms to ensure that only authorized devices and users can access IoT data. Proper authorization controls define what actions and data each device or user can access.

- Secure APIs: Use secure Application Programming Interfaces (APIs) for communication between devices and backend systems. API security involves employing authentication tokens, encrypted connections, and proper access controls.
- Data Integrity: Implement mechanisms to ensure the integrity of IoT data. This involves verifying that data has not been tampered with during transmission or storage, ensuring its accuracy and reliability.
- Role-Based Access Control (RBAC): Enforce role-based access controls to limit access to sensitive data based on the roles and responsibilities of users and devices. This helps prevent unauthorized users from gaining access to critical information.
- Secure Device Onboarding and Lifecycle Management: Securely onboard devices to the IoT network by using secure provisioning methods. Implement proper lifecycle management to handle device activation, deactivation, and updates securely.
- Data Minimization: Adopt a principle of data minimization, where only the necessary data is collected and stored. This reduces the potential impact in case of a security breach.
- Secure Cloud Services: If data is stored in the cloud, ensure that cloud services are secured with strong authentication, access controls, and encryption. Regularly monitor and audit cloud infrastructure for security vulnerabilities.
- IoT Gateway Security: Secure IoT gateways that mediate communication between devices and the cloud. Apply security measures such as firewalls, intrusion detection systems, and regular security updates.
- Privacy by Design: Integrate privacy considerations into the design and development of IoT applications. This involves minimizing the collection of personally identifiable information (PII) and ensuring that privacy controls are implemented.
- Security Analytics and Monitoring: Implement security analytics and monitoring tools to detect unusual patterns or anomalies in data traffic. Prompt identification of security incidents allows for swift response and mitigation.
- Regulatory Compliance: Adhere to relevant data protection and privacy regulations. Understand the legal requirements for handling IoT data and ensure compliance with standards such as GDPR, HIPAA, or industry-specific regulations.

A comprehensive approach to data security in IoT applications involves a combination of technological measures, secure development practices, and ongoing monitoring and adaptation to emerging threats. As the IoT landscape continues to evolve, maintaining a proactive stance on data security is essential to building and maintaining trust in connected systems.

Other application security measures

- User Awareness and Training: Educate users about IoT security risks and best practices. Train users on strong password management, phishing awareness, and secure device handling procedures.
- Vulnerability Management: Regularly scan IoT devices and networks for vulnerabilities and misconfigurations. Use vulnerability scanning tools and penetration testing to identify and remediate security weaknesses.

- Incident Response: Establish an incident response plan to effectively handle security incidents. Define clear roles, responsibilities, and communication protocols for incident response.
- Compliance: Adhere to relevant industry regulations and data privacy laws. Implement data governance practices to ensure compliance with data protection requirements.
- Continuous Improvement: Continuously review and update IoT security practices to adapt to evolving threats and technologies. Stay informed about emerging security trends and vulnerabilities, and implement appropriate countermeasures.

New Trends in IoT Communication and Related Security Aspects

IoT security and communication technologies have a bright future ahead of them, with a number of exciting new innovations planned. The creation of new, more secure communication protocols is one important trend. One new area of study is post-quantum cryptography, which is creating new cryptographic algorithms that are immune to assault by quantum computers. In the future, these algorithms might be applied to secure Internet of Things communication protocols. The creation of fresh security solutions created especially for the Internet of Things is another important trend. Moreover, new intrusion detection and prevention systems that are more adept at recognising and obstructing malicious traffic can be created using artificial intelligence (AI) and machine learning (ML) technology. The Internet of Things is being more and more linked with other technologies, such edge computing and 5G, which opens up new possibilities for processing data and facilitating safe communication. Furthermore, Edge computing can handle data from Internet of Things devices closer to the point of collection, which can lower latency and boost security. Future IoT communication technologies may be secured by promising new technologies like homomorphic encryption, zero-trust security, and post-quantum cryptography. New security solutions that are being developed expressly for the Internet of Things include safe device management solutions, blockchain-based security solutions, and AI and ML-based intrusion detection and prevention systems. In the Internet of Things, edge computing, 5G, and other cutting-edge technologies are opening up new possibilities for data processing and secure communication. IoT security and connectivity technologies have a bright future ahead of them. An increasingly dependable and safe Internet of Things is being created via the creation of new integrated technologies, security solutions, and communication protocols.

Because it allows businesses and organisations to make well-informed decisions based on data acquired from IoT sensors, forecasting is a crucial component of the Internet of Things. IoT forecasting can offer useful insights into future behaviour by evaluating past data and seeing patterns and trends. This allows for proactive planning and resource allocation. Furthermore, protecting linked devices, networks, and the data they produce requires addressing risks associated with the Internet of Things.