

## Chapter 1

# Introduction to IoT

Tajkia Nuri Ananna <sup>1</sup>, Munshi Saifuzzaman <sup>2</sup>

<sup>1</sup> Department of CSE, Metropolitan University, Sylhet 3104, Bangladesh

<sup>2</sup> Dynamic Solution innovators, Dhaka 1206, Bangladesh

Email Address of the Corresponding Author: munshisaifuzzaman@gmail.com

### Abstract

The Internet of Things has rapidly transformed the 21<sup>st</sup> century, enhancing decision-making processes and introducing innovative consumer services such as pay-as-you-use models. The integration of smart devices and automation technologies has revolutionized every aspect of our lives, from health services to the manufacturing industry, and from the agriculture sector to mining. Alongside the positive aspects, it is also essential to recognize the significant safety, security, and trust concerns in this technological landscape. This chapter serves as a comprehensive guide for newcomers interested in the IoT domain, providing a foundation for making future contributions. Specifically, it discusses the overview, historical evolution, key characteristics, advantages, architectures, taxonomy of technologies, and existing applications in major IoT domains. In addressing prevalent issues and challenges in designing and deploying IoT applications, the chapter examines security threats across architectural layers, ethical considerations, user privacy concerns, and trust-related issues. This discussion equips researchers with a solid understanding of diverse IoT aspects, providing a comprehensive understanding of IoT technology along with insights into the extensive potential and impact of this transformative field.

**Keywords:** Architectural Layers, Ethical Considerations, Security Threats, Hardware Platforms, Trust-related Issues, Taxonomy of technologies.

### 1.1 Introduction

In today's ubiquitous digital landscape, the Internet has profoundly impacted global existence, marking an ongoing journey towards even more pervasive connectivity—ushering in the era of the Internet of Things (IoT). A groundbreaking invention in recent decades, IoT revolutionizes the interaction between the physical and digital realms, as defined by Verme-san et al. [1]. In this interconnected landscape, the digital world engages with the physical

world through an array of sensors and actuators. Pena-López et al. [2] offer an expansive interpretation, characterizing IoT as a paradigm where computing and networking seamlessly integrate into virtually any object, empowering remote querying and modification. Broadly, the term "Internet of Things" describes a transformative realm where nearly every daily device is intricately linked to a network, enabling collaborative utilization for intelligent and automated tasks. The concept of IoT was first introduced by Peter T. Lewis in 1985, defining it as the fusion of individuals, processes, and technology with interconnected devices and sensors. This facilitates remote monitoring, status assessment, manipulation, and trend analysis of these devices [3]. The IoT journey, far from its conclusion, promises a future where diverse devices seamlessly connect to the web, reshaping human existence in unprecedented ways.

The IoT is a network of interconnected devices with sensors, actuators, processors, and various communication technologies. Sensors collect real-time data from both internal states and external surroundings, ranging from mobile phones to microwave ovens. Actuators, in turn, respond to data or commands, enabling automation and remote control of physical devices. Data collected by sensors undergoes processing either at the network edge or on central servers, with some preprocessing occurring directly in the sensors or end devices. Processed data is then transmitted to remote servers for further analysis, storage, and processing. These data form the basis for analysis, decision-making, and subsequent actions, which can be physical (e.g., adjusting a smart thermostat) or virtual (e.g., sending notifications) [4]. The applications of IoT are extensive and diverse, impacting various aspects of our lives. From personal convenience in smart homes to healthcare and fitness innovations, IoT has the potential to influence personal, financial, physical, educational, professional, and mental aspects of individuals. In smart homes, IoT enables remote control of electrical appliances, lighting, coffee brewing, thermostat adjustments, and even hands-free operations through voice commands [5]. In healthcare, wearable IoT devices offer remote monitoring, allowing caregivers and healthcare professionals to provide timely assistance in emergencies. Additionally, individuals can use wearable devices to track sleep patterns, physical activity, and overall fitness [6]. These examples only scratch the surface of IoT's broad application landscape, indicating the exciting possibilities and challenges that researchers are exploring for the future.

The IoT has the potential to transform how people interact with technology, providing greater convenience, efficiency, and personalization in daily life. Despite its transformative impact, IoT faces challenges. The sheer number of devices and the substantial data generated pose significant challenges, with a projected 41.6 billion IoT devices producing 79.4 zettabytes of data by 2025 [7]. Addressing this requires scalable architectures and enhanced processing capabilities. Moreover, IoT heavily relies on wireless communication, leading to challenges such as distortion and unreliability in geographically dispersed locations. Ensuring dependable data transmission becomes a pivotal challenge, emphasizing the critical role of communication technologies in the IoT landscape. Beyond technical hurdles, various general and domain-specific challenges are crucial for the success of IoT. Identifying and addressing these multifaceted challenges collectively is essential to unlocking the full potential of IoT and overcoming obstacles for broader adoption and integration into our lives.

**Motivation of this chapter:** IoT is not a novel concept; researchers have been exploring this field for decades. Consequently, the question arises: what sets this chapter apart

from others, and why should readers invest their time in exploring the basics presented here? While there are several book chapters introducing IoT, many share outdated concepts, lacking the latest insights from the ongoing exploration of this dynamic field. For instance, in [8], only IoT applications are discussed, and in [9], authors overlook major domains, including IoT applications, advantages, challenges, and technologies. Notably, Nagaraj et al. [10] present a well-structured discussion covering technologies, architectures, applications, and challenges. However, their discussion is limited to these aspects, with a less extensive exploration of the application section. Therefore, the need arises for a comprehensive chapter that covers all aspects and incorporates recent additions in the IoT field. This chapter goes beyond the basics, encompassing fundamental components, characteristics, and advantages. It delves into architectures, provides a taxonomy of technologies used in IoT, explores a significant number of applications across diverse domains, and addresses ethical considerations as well as legal and regulatory issues. In essence, our chapter serves as a holistic guide, covering the most significant facets of IoT, from foundational principles to emerging research challenges and future directions. Readers are encouraged to explore this chapter for a thorough and up-to-date understanding of the evolving landscape of IoT.

**Contributions:** The contributions of this chapter can be summarized as follows:

1. This chapter provides an introductory overview of the IoT with the aim of assisting future contributors. It assesses the benefits, generic architecture, key technologies underpinning IoT, and its diverse applications across various domains.
2. Recent studies have been examined to facilitate this assessment. Additionally, this chapter encompasses a taxonomy of IoT technologies, including extensive coverage of field communication.
3. In conclusion, this chapter offers a comprehensive discussion of the open research challenges, ethical considerations, as well as the legal and regulatory aspects of IoT.

**Chapter organization:** It begins with an exploration of the fundamentals in Section 1.2, covering the history 1.2.1, components 1.2.2, and characteristics 1.2.3. In Section 1.3, the advantages of IoT are examined. By introducing a generic architecture in Section 1.4, the taxonomy of technologies that underpin IoT operations are discussed in detail in Section

Table 1.1: List of abbreviations

Name	Abbreviation	Name	Abbreviation	Name	Abbreviation
FDMA	Frequency Division Multiple Access	LBT	Listen Before Talk	CDMA	Code Division Multiple Access
FHSS	Frequency Hopping Spread Spectrum	CSS	Chirp Spread Spectrum	OOK	On-Off Keying
TDMA	Time Division Multiple Access	GSM	Global System for Mobile Communications	PPM	Pulse Position Modulation
GFSK	Gaussian Frequency Shift Keying	UMTS	Universal Mobile Telecommunications System	OFDM	Orthogonal Frequency Division Multiplexing
DWPSK	Differential Quadrature Phase Shift Keying	GMSK	Gaussian Minimum Shift Keying	TDD	Time Division Duplex
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance	LTE-A	Long-Term Evolution Advanced	FDD	Frequency Division Duplex
BPSK	Binary Phase Shift Keying	3GPP	3rd Generation Partnership Project	ALHOA	Adaptive Link Hopping On Air
CSMA/CD	Carrier Sense Multiple Access with Collision Detection	WCDMA	Wideband Code Division Multiple Access	DBPSK	Differential Binary Phase Shift Keying
O-QPSK	Offset Quadrature Phase Shift Keying	OFDMA	Orthogonal Frequency Division Multiple Access	QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying	SC-FDMA	Single Carrier Frequency Division Multiple Access	CP-OFDM	Cyclic Prefix Orthogonal Frequency Division Multiplexing

1.5. Furthermore, Section 1.6 explores the extensive array of application domains of IoT, with a focus on multiple promising research works within each domain, aiming to provide a comprehensive understanding of its real-world applications. It concludes in Section 1.7 by addressing the key challenges that IoT faces today, considering insights from the reviewed literature, and sheds light on potential future scopes and developments in the ever-evolving realm of IoT technology. Table 1.1 represents some abbreviations mentioned in this chapter.

## 1.2 Fundamentals of IoT

At its core, the IoT revolves around the concept of connecting everyday objects and devices to the internet, enabling them to communicate, collect data, and perform actions autonomously or in response to commands. This basic concept involves three key elements: sensors and actuators that gather and interact with data, a network infrastructure for data transmission, and cloud-based platforms for data storage, processing, and analysis. By interconnecting these elements, IoT empowers us to enhance efficiency, gain real-time insights, and create smart, responsive systems that impact various aspects of our lives, from smart homes and cities to industries and healthcare. The evolution of IoT, which has unfolded over several decades, began with the concept of smart objects. Since then, IoT has undergone numerous groundbreaking transformations that have left the world astounded, thanks to its unique and convenient characteristics. The advantages brought by this technology are unquantifiable, as it touches nearly every aspect of people’s lives, simplifying and improving them. This section comprehensively discusses these fundamental IoT concepts, covering the following topics: *history, components, characteristics*.

### 1.2.1 Historical Development

Since the invention of the first landline, the telegraph, in the 1830s and 1840s, machines have been instrumental in facilitating direct communication. A significant step towards the IoT occurred on June 3, 1900, with the first radio voice transmission, often referred to as “wireless telegraphy”. This paved the way for IoT. The development of computers, which began in the 1950s, is another crucial aspect of IoT.

In 1962, the Internet, a fundamental component of IoT, started as a DARPA<sup>1</sup> project. A group of renowned researchers initiated efforts to connect computers and systems. By 1969, DARPA had evolved into ARPANET<sup>2</sup>, a precursor to today’s Internet [11].

While the term “Internet of Things” is relatively new, the concept of integrating computers and networks to monitor and manage devices has a rich history spanning decades. In the late 1970s, various stakeholders, including businesses, governments, and consumers, began exploring ways to connect personal computers (PCs) and other machinery. This led

---

<sup>1</sup>The Defense Advanced Research Projects Agency is a research and development agency of the United States Department of Defense responsible for the development of emerging technologies for use by the military.

<sup>2</sup>The Advanced Research Projects Agency Network (ARPANET) was the first wide-area packet-switched network with distributed control and one of the first computer networks to implement the TCP/IP protocol suite. Both technologies became the technical foundation of the Internet.

to the practical use of systems for remotely monitoring electrical grid meters via telephone lines during that era [12].

In the 1980s, there was a growing interest in enhancing physical objects with sensors and intelligence. Commercial service providers began supporting public access to ARPANET, an early precursor to the modern Internet, during this time. Satellites and landlines played pivotal roles in establishing the foundational communication infrastructure for the emerging IoT. The concept of a network of smart devices was initially explored as early as 1982 when a Coca-Cola vending machine<sup>3</sup> at Carnegie Mellon University was modified to connect to ARPANET. This allowed local programmers to remotely monitor the vending machine’s contents, ensuring drinks were available and cold before making a purchase. However, the technology was challenging to manage, and progress in this field was limited during that period [13]. In parallel, during the 1980s, local area networks (LANs) gained popularity and proved effective for real-time communication and document sharing among groups of PCs.

In the 1990s, advancements in wireless technology set the stage for the widespread adoption of “machine-to-machine” (M2M) solutions in enterprise and industrial contexts, particularly for equipment monitoring and operation. However, many of these early M2M solutions relied on closed, purpose-built networks and proprietary or industry-specific standards rather than utilizing Internet Protocol (IP)-based networks and Internet standards [14]. By the mid-1990s, the Internet had expanded its global reach, offering new possibilities for researchers and technologists to explore ways to enhance connections between humans and machines. A significant milestone in this journey was the creation of the first Internet-connected ‘device’ by John Romkey—an IP-enabled toaster that could be controlled over the Internet. This innovative toaster was showcased at an Internet conference in 1990, marking an early example of the IoT in action [15].

In 1991, Mark Weiser’s paper “The Computer of the 21st Century” [16] and academic events like UbiComp and PerCom shaped the contemporary IoT vision [14]. Global Positioning System (GPS) became a reality in early 1993 with the Department of Defense establishing a stable system of 24 satellites. Privately owned commercial satellites soon followed, enhancing IIoT functionality [3]. In early 1994, Reza Raji introduced the IoT concept in IEEE Spectrum, describing it as “moving small data packets to integrate and automate from home appliances to entire factories” [17]. Later that year, Steve Mann invented the near-real-time WearCam, powered by a 64-processor setup. Between 1993 and 1997, companies proposed IoT solutions, including Microsoft’s “at Work” and Novell’s NEST. Momentum grew as Bill Joy introduced device-to-device communication in his “Six Web” framework at the 1999 World Economic Forum [3].

The term “Internet of Things” was coined by Peter T. Lewis in a 1985 speech during the Congressional Black Caucus Foundation’s 15th Annual Legislative Weekend in Washington, D.C. Lewis defined IoT as the integration of people, processes, and technology with connectable devices and sensors for remote monitoring, status assessment, manipulation, and trend evaluation related to these devices [3]. In 1997, Paul Saffo described sensors and their future roles. British technologist Kevin Ashton, while serving as the executive director of the Auto-ID Center at MIT, independently coined the term “Internet of Things”. During his time at Procter and Gamble, he explored radio-frequency identification (RFID), a tech-

---

<sup>3</sup>The “Only” Coke Machine on the Internet. Available at: [Carnegie Mellon University](#)

nology framework enabling physical devices to connect via microchips and wireless signals. In the same year, they developed a global RFID-based item identification system [14].

In 1999, Kevin Ashton was the first to describe the IoT and proposed the name “Internet of Things” during a presentation for Procter and Gamble. He believed RFID technology, primarily designed for inventory tracking, was a significant prerequisite for the IoT, allowing computers to efficiently manage and monitor individual objects. The concept of tagging objects has been realized through technologies like digital watermarking, barcodes, and QR codes, used for identification and tracking purposes [18]. Subsequent technological advancements, including the proliferation of smartphones, cloud computing, improved processing power, and enhanced software algorithms, along with the availability of sophisticated sensors capable of measuring various parameters, laid the foundation for robust data collection, storage, and processing for the IoT’s growth.

As a significant step forward in commercializing IoT, LG announced plans to launch a smart refrigerator capable of autonomously managing its contents in 2000. Walmart and the US Department of Defense pioneered inventory tracking using RFID and the IoT in 2002–2003. RFID gained prominence in the US Army’s Savi program in 2003, and Walmart expanded its RFID usage worldwide that same year. In 2004, Cornelius “Pete” Peterson, CEO of NetSilicon, predicted that IoT devices would dominate the next era of information technology, particularly in fields like medical devices and industrial controls [3]. In 2005, numerous articles in mainstream newspapers such as The Guardian, Scientific American, and The Boston Globe discussed IoT’s future direction.

The IPSO Alliance was founded in 2008 to promote the use of IP in networks of “smart objects”, while the FCC allowed the use of the “white” label in 2008. Google initiated the development of autonomous cars in 2009, and in 2011, Google’s Nest smart thermostat entered the market, enabling remote heating management. In June 2012, major Internet service providers and web-based companies agreed to expand the global Internet’s address space by enabling IPv6 for their services and products, a significant step towards a viable IoT. This led to substantial growth and interest in the field. IT giants like Cisco, IBM, and Ericsson later took numerous educational and commercial initiatives related to IoT. Cisco Systems estimated that the IoT was “born” between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84 in 2010 [18].

## 1.2.2 Components

The IoT consists of several key components that serve as the essential building blocks for constructing an IoT system. This section provides an in-depth exploration of the principal components of the IoT. IoT comprises three main components: (1) sensors/devices, and actuators; (2) storage and data analytics; and (3) interpretation and visualization tools. Each of these is further categorized into various subcomponents.

### *Sensors/Devices and Actuators*

1. Sensors/Devices: Sensors play a crucial and essential role within an IoT system. Given that IoT operates by gathering data from the surrounding environment, it is necessary



for all IoT applications to incorporate one or more sensors to meet this need. A defining characteristic of IoT devices is their context awareness, which is made possible through the utilization of sensor technology. Sensors are not only compact and cost-effective but also energy-efficient. However, they are subject to limitations such as battery capacity and ease of deployment. [4]. An overview of various types of sensors has been provided below.

(a) Mobile-based Sensors

Smartphones, which are widespread and commonly used, are equipped with various sensors. Given their extensive usage, researchers are exploring the potential of using smartphones as integral components in building smart IoT solutions. These applications can harness sensor data from smartphones to generate valuable insights and outcomes. Some of the general sensors found in smartphones include an accelerometer, gyroscope, GPS, magnetometer, light sensor, and proximity sensor [19]. Certain smartphones, like the Samsung Galaxy S4, come equipped with extra sensors, including a thermometer, barometer, and humidity sensor [4].

(b) Medical Sensors

The healthcare industry is one of the most influential fields where innovation and IoT have paved the way. Wearable devices and sensors have facilitated remote monitoring for physicians and enabled researchers to collect data continuously and in real-time. These devices come in different forms, such as wristbands, smartwatches, and monitoring patches. Smartwatches and fitness trackers, known for their versatility, have gained popularity among consumers. Likewise, monitoring patches have emerged as a valuable asset to the healthcare sector by enabling remote treatment for patients.

(c) Neural Sensors

Neural sensors play a crucial role in comprehending the workings of human neurons by enabling us to decode brain signals, assess the brain's current state, and, when necessary, optimize it for improved focus and attention. This practice is commonly referred to as *Neurofeedback* [22].

(d) Environmental and Chemical Sensors

While conventional tools manage parameters such as temperature and pressure, specialized environmental sensors play a crucial role in evaluating air quality. These sensors detect gases and particulate matter [23], while also measuring factors like temperature, humidity, pressure, and pollution. Besides, chemical sensors play a crucial role in detecting both chemical and biochemical substances. Among the innovative technologies available are the electronic nose (e-nose) and electronic tongue (e-tongue), which rely on pattern recognition to sense chemicals based on odor and taste. These sensors find valuable applications in smart cities for monitoring pollution levels [24].

(e) Radio-Frequency Identification (RFID)

RFID technology, which serves as sensors, finds widespread use in various IoT applications. For instance, it is employed for tracking products within extensive inventories or monitoring items within large retail stores.

2. **Actuators:** Actuators hold a crucial role and operate in direct contrast to sensors. They transform energy into physical motion and are typically positioned on the outer periphery of a system. Take, for instance, a scenario involving a smart home system that incorporates numerous sensors and actuators. In this setup, the actuators receive signals from the sensors and, depending on the context, carry out actions such as locking or unlocking doors, toggling lights or electrical devices on or off, regulating the house's temperature, or setting alarms for emergencies. Essentially, actuators respond to and execute commands based on the signals they receive from sensors or other devices.

### *Storage and Data Analytics*

Another crucial aspect of IoT is the management of the substantial volume of data generated and exchanged by IoT devices continuously. Storing this data presents a significant challenge within IoT networks. Furthermore, the data collected from these devices must undergo filtering, processing, and analysis to enable the effective functioning of the IoT system. In this process, gateways, cloud services, and analytics collaborate to handle data storage and processing tasks.

1. **Gateway:** Gateways, designed to simplify the IoT system, function as the intermediate medium of communication between the devices and the central cloud system. The major functionalities of IoT gateways are listed below:
  - (a) *Data Preprocessing*

The IoT gateway serves as an intermediary between sensor devices and the central cloud, conducting basic data analytics before forwarding information directly to the cloud. This layer performs the tasks of local data filtering, cleaning, preprocessing, and protocol translation. During this process, it may also aggregate, remove duplicates, or summarize the data to enhance response times and lower transmission costs [25].
  - (b) *Data Acquisition*

In this layer, data is collected from multiple sources, converted into the desired format, and then transferred to the processing layers. The role of the gateway in this stage is to provide secure connectivity between IoT devices and processing structures [26].
  - (c) *Data forwarding and Temporary Storage*

The primary role of the gateway is to ensure secure data transfer between the sensor layer and the central cloud [27]. Additionally, this layer serves as the temporary storage repository for the collected data.
  - (d) *Device Management*

This layer facilitates real-time device configuration, allowing adjustments to device statuses, operational modes, error acknowledgments, and more [27].
  - (e) *Diagnostics*

The IoT gateway identifies errors and faults within the entire technology layer, including self-diagnostics for the IoT gateway itself [27].



2. Cloud: The cloud serves as the central hub of an IoT network, taking on pivotal roles in data processing, storage, and management. The key characteristics of the cloud include the ability to store and process extensive data generated by devices, scalability to effortlessly handle thousands of devices, flexibility by allowing devices to be added or removed as needed without requiring a complete system reconfiguration, supervision and management by the cloud service provider, and cost-effectiveness.

While cloud services are not mandatory for IoT, the recent shift toward edge and fog computing empowers local data processing. Nevertheless, the cloud is incorporated into the system for its scalability, storage and cost-effective service provision [28]. Furthermore, cloud-based services offer security functionalities such as encryption and authentication while enabling remote access and control of IoT devices.

3. Analytics: This represents one of the most intricate and vital layers within IoT. It involves the analysis of data, generating valuable insights through the application of diverse machine learning (ML) algorithms and statistical analysis techniques. Numerous applications of analytics in IoT encompass anomaly detection, environmental monitoring, energy management, smart cities, and agriculture [29].

#### *Interpretation and Visualization Tools*

This segment essentially serves as the user interface (UI). The UI offers a platform for users to interact directly with the application or system, facilitating communication. A user interface is not always reliant on a screen. For instance, a TV remote utilizes a user interface comprising multiple buttons, while devices like the Amazon Echo respond to voice commands for control. *Receiving Automatic Notification, Monitoring Information Proactively, and Controlling the System Remotely* are some common examples for user interfaces in IoT systems [30].

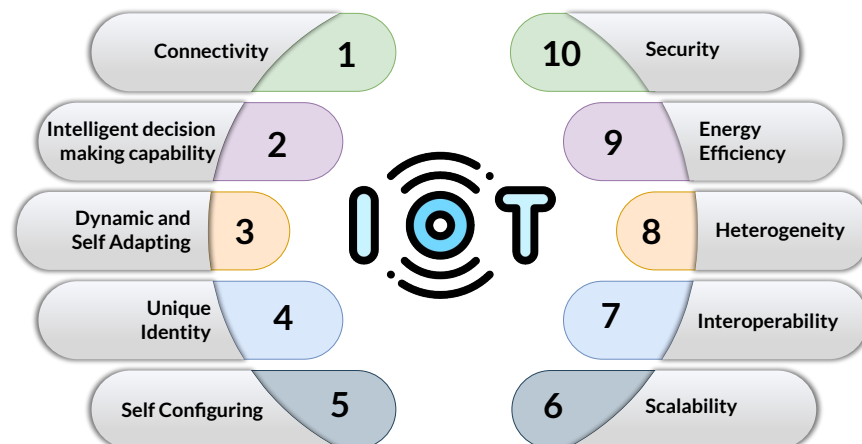


Figure 1.1: IoT characteristics

### 1.2.3 Characteristics

This segment essentially serves as the user interface (UI). The UI offers a platform for users to interact directly with the application or system, facilitating communication. A user interface is not always reliant on a screen. For instance, a TV remote utilizes a user interface comprising multiple buttons, while devices like the Amazon Echo respond to voice commands for control. Receiving automatic notifications, monitoring information proactively, and controlling the system remotely are some common examples of user interfaces in IoT systems [30]. The IoT characteristics discussed in this chapter are illustrated in Figure 1.1.

1. *Connectivity*: Connectivity is the most vital requirement of IoT. The main aspect of IoT is a network with millions of devices connected to each other. The connectivity remains constant, allowing anyone from anywhere to connect to the IoT network at any given moment.
2. *Intelligent decision making capability*: The extraction of knowledge from the data generated is highly significant. Consider a sensor that produces data; however, the true value of that data lies in its proper interpretation. This represents a crucial aspect of IoT, wherein IoT devices possess the capability to transform raw data collected by sensors into meaningful information and make decisions based on it.
3. *Dynamic and Self Adapting*: IoT devices should have the ability to adapt to changes in context, their surrounding environment, and the existing situation. For instance, within a surveillance system, cameras are capable of switching between day and night modes or adjusting their resolution in response to motion detection, demonstrating their adaptability.
4. *Unique Identity*: Every IoT device should have a unique identity and unique identifier. IoT device interfaces enable users to inquire about device information, monitor their status, and remotely manage them. Having a distinct identity is essential to empower users to safeguard their devices, whether through password protection or alternative security measures [33].
5. *Self Configuring*: IoT devices possess the capability to autonomously update their systems in response to the situation, eliminating the need for user intervention. Moreover, they exhibit flexibility in network management, allowing new devices to seamlessly join the network and permitting any device to depart from the network at any time.
6. *Scalability*: The IoT network is experiencing a continual growth in the number of connected devices, resulting in a substantial and continuous generation of data. Consequently, scalability emerges as the foremost feature of any IoT system.
7. *Interoperability*: IoT devices rely on standardized protocols and technologies to guarantee seamless communication among themselves and with other systems. Interoperability represents a fundamental block of the IoT, signifying the capacity for various IoT devices and systems to interact and share data, irrespective of the underlying technology or the manufacturer. Hence, IoT devices employ standardized protocols, data formats, and technologies to uphold interoperability.

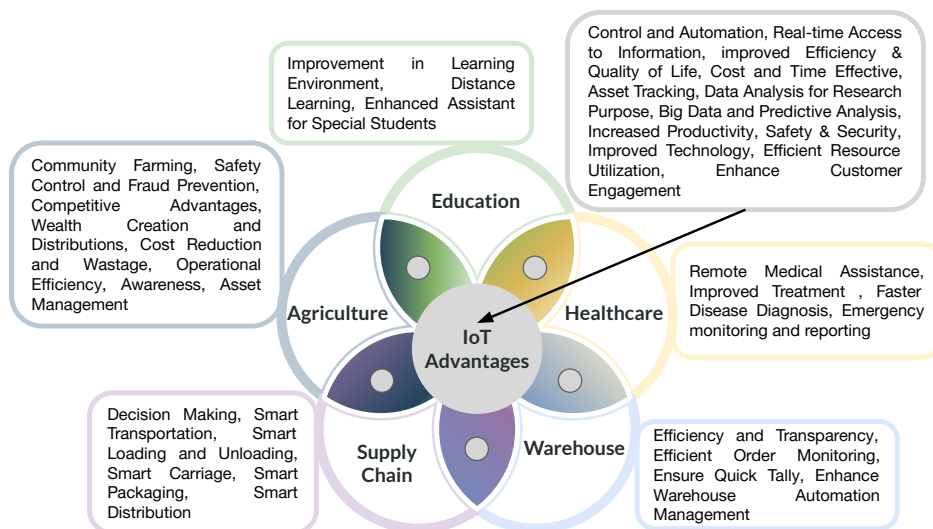


Figure 1.2: Advantages of IoT

8. *Heterogeneity*: The devices within an IoT network exhibit heterogeneity, showcasing the network's capability to accommodate diverse elements.
9. *Energy Efficiency*: Energy efficiency stands out as a significant characteristic of IoT. Numerous IoT devices are purposefully crafted to minimize energy consumption and create low-power devices. Furthermore, various IoT approaches are tailored to optimize power usage, such as opting for fog/edge computing over cloud computing to decrease bandwidth requirements and reduce power consumption when constructing an IoT system [34].
10. *Security*: The presence of millions of internet-connected devices and the vast amount of data generated underscore the vulnerability of the IoT network to security threats. Hence, safety and security emerge as pivotal characteristics of the IoT. Ensuring safety is of paramount importance to preserve the effectiveness of IoT's advantages, including efficiency and novel experiences.

### 1.3 Advantages of IoT

The amount of benefits IoT offers to people's lives is the main reason IoT is becoming more popular by the day. IoT solutions are developed and invented to make people's lives easier and more convenient. IoT technology affects almost every field, including healthcare, education, and business. This section elaborates on the most visible benefits of IoT in people's daily lives [35, 36], and Fig. 1.2 provides a visual overview.

1. *Efficient Data Collection*: IoT-based data collection has been particularly beneficial in sectors such as healthcare and finance [37]. A straightforward illustration of efficient data collection is the integration of IoT in the retail sector. Internet-connected tags can provide data on purchase decisions and sales trends, whether weekly or monthly.

This enhanced data gathering can improve inventory management and reveal valuable insights into customer behavior, ultimately contributing to the prosperity of the business.

2. *Control and Automation*: IoT has provided its customers with a more convenient lifestyle and allows them to control their daily activities with the touch of a button. One simple yet remarkable example is the smart bulb, which can be controlled without even touching the switches; the user can simply turn off or on the light remotely. Not only can the light bulb, coffee maker, or any other electrical device in the home be controlled with the tip of the device, but they can also be controlled using a voice command when they are linked to Google's or Amazon's voice assistants.
3. *Real-time Access to Information*: IoT devices offer immediate access to information, proving invaluable across healthcare, business, and everyday applications. A prime illustration of the advantages of real-time data access is within the healthcare sector. Physicians can access patient data in real-time, enabling continuous health monitoring. This capability becomes particularly crucial in delivering emergency medical assistance swiftly when unexpected health issues arise.
4. *Improved Efficiency*: IoT systems operate autonomously, which is a valuable asset in various domains. Reduced human intervention leads to increased efficiency and decreased labor reliance. For instance, a company with a fleet of delivery vehicles can effortlessly track their real-time locations, eliminating the need for manual employee involvement in this task.
5. *Improved Quality of Life*: The advent of IoT has significantly improved the lives of its users in numerous ways. Real-time health monitoring, including devices like blood pressure monitors and fitness trackers, empowers users to maintain their well-being effectively. Smart homes offer a stress-free and effortless lifestyle. These advantages extend beyond individuals and can benefit entire industries or communities. Smart devices, linked not only to intelligent traffic lights but also to road safety monitors and toll gates, can provide drivers with real-time information about road conditions on their route.
6. *Cost and Time Effective*: IoT minimizes human effort and relies heavily on real-time data transmission, leading to time savings. For example, real-time patient monitoring benefits both patients and doctors by eliminating the need for physical meetings, thus saving time for both parties. IoT aids businesses in streamlining their workflows by offering valuable insights and real-time information, resulting in cost reductions. In addition to businesses, individuals can reduce their everyday expenses through the use of IoT.
7. *Asset Tracking*: This process involves tracking products within a business or logistics management system. Manual asset tracking is labor-intensive and time-consuming, but it can be streamlined through the application of IoT technologies like barcodes and RFID tags. These technologies allow for remote monitoring of goods and provide stakeholders with information about any faults or problems in real time [38].

8. *Data Analysis for Research Purpose*: The enormous amount of data collected from IoT devices has become a blessing for researchers in various fields like healthcare, education, business, etc. The healthcare researchers can use the data collected via biosensors to invent cures and vaccines for disease; the finance industry can use the data to understand trends and improve customer experience; the super shops can analyze customer behavior and improve their businesses; and so on.
9. *Big Data and Predictive Analysis*: “Big data” has been a widely recognized term in the world long before the emergence of IoT. It involves the collection and analysis of massive volumes of data. One of the primary objectives of IoT is to amass data from diverse sources, sending this information back to systems for analysis. Effective analysis of big data can yield valuable insights, spanning from stock market predictions to understanding customer behavior, thereby enhancing the business landscape.
10. *Increased Productivity*: IoT utilization in both industry and homes has the potential to boost productivity significantly. For instance, in a smart home, users can streamline various household tasks using voice commands, enabling efficient multitasking. Similarly, in a business setting, analyzing customer behavior can enhance customer satisfaction, ultimately contributing to the prosperity of the enterprise. As an example, 46% of businesses that embraced IoT strategies saw improvements in efficiency, even though only 29% initially anticipated such improvements [39]. In the healthcare sector, doctors can offer more extensive services to their patients if they do not need to make physical visits to each patient individually.
11. *Safety and Security*: The incorporation of IoT offers users a means of security not only in their homes but also in their businesses, schools, offices, and virtually anywhere. Individuals can remotely monitor their valuable assets, such as vehicles and other important items. Parents can even keep track of their children’s whereabouts from their workplaces, providing peace of mind. IoT allows for vehicle tracking and the setup of alert systems in case of unusual incidents. Financial companies and banks can enhance the security of their confidential rooms or vehicles by utilizing IoT [34].
12. *Enhance Customer Engagement*: The IoT offers several avenues for enhancing customer engagement. It achieves this by leveraging valuable customer data, personalizing experiences, improving convenience, and enabling real-time interactions.
13. *Efficient Resource Utilization*: IoT facilitates efficient resource utilization through various mechanisms and capabilities. Its ability to collect and monitor real-time information allows organizations to track the status of their resources, such as equipment and machinery, enabling the identification of inefficiencies. Predictive maintenance powered by IoT in the industrial sector can anticipate machinery failures, reducing downtime and optimizing resource allocation for maintenance.
14. *Improved Technology*: The innovation brought about by IoT leads to the creation of newer and more advanced technologies on the market. For instance, consider the scenario of an air conditioner that was initially controlled manually with a remote. With the advent of IoT, users can now operate it using voice commands or control it

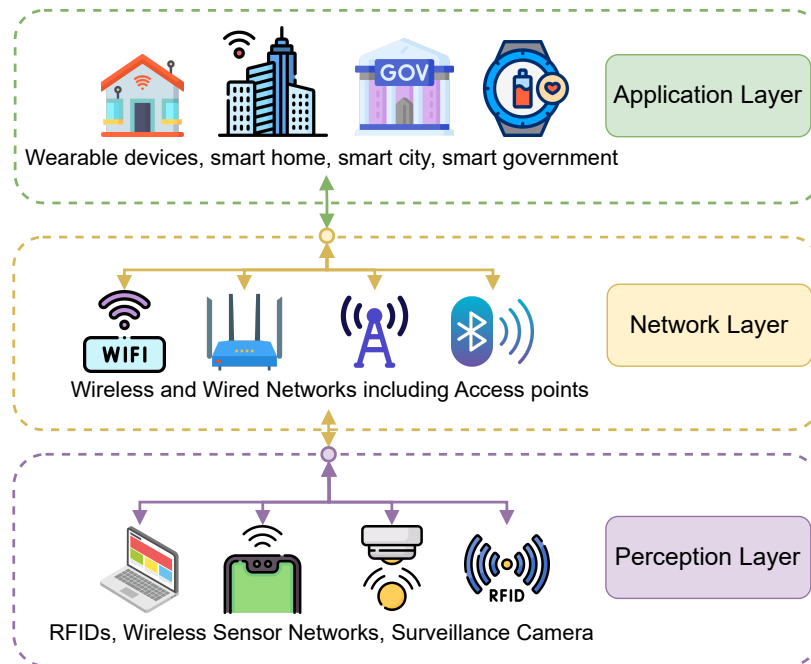


Figure 1.3: Generic architecture of IoT

remotely. When such innovations hit the market, they spark competition, driving the development of improved solutions based on user feedback. This cycle of innovation in response to IoT advancements contributes to the continuous progression of technology [37].

## 1.4 IoT Architecture

Architecture refers to a structured framework depicting the tangible components of a network, their operational arrangement and setup, underlying principles and structures, as well as the manner in which data is organized and utilized within its functioning. IoT architecture comprises a collection of devices, sensors, actuators, end users, cloud services, and most importantly, various communication layers and IoT protocols. All IoT systems inherently follow the generic three-layer architecture. However, based on necessities or specific application requirements, the generic model can be modified by adding extra layers, thus forming four- or five-layer architectures [4].

The IoT architecture can be divided in two ways: (1) layered architecture and (2) domain-specific architecture. In this section, we have presented a generic architecture of IoT. IoT follows a layered architecture, which refers to the structured framework used to design and organize the various components and functions of an IoT system. This architecture is composed of multiple layers, each with its own specific role and responsibilities, allowing for efficient communication, data processing, and management within the IoT ecosystem. The typical layers in the IoT architecture include the perception layer, network layer, and application layer. These layers collaborate to ensure the smooth operation of IoT devices, data transmission, and the provision of IoT services to end users.



According to this generalized architecture, also known as the three-layer architecture, the IoT system is divided into three layers [61], namely (i) the application layer, (ii) the network layer, and (iii) the perception layer. Every one of these layers possesses inherent security challenges [62]. A visual representation of the generic three-layer architecture is featured in Fig. 1.3. The details are described below.

1. *Perception Layer*: The perception layer, also known as the sensor layer, is the foundational layer of IoT architecture [61]. This layer engages with smart devices, including but not limited to smartwatches and smart rings, employing an array of sensors and actuators. The principal objective of this layer pertains to the collection of data from these intelligent devices via sensors, subsequently transmitting the acquired data to the upper layer known as the network layer.
2. *Network Layer*: The network layer, also known as the transmission layer, is the middle layer of the IoT architecture [63]. This layer is responsible for receiving the information passed from the perception layer and determining the routes to transmit the processed data to various connected IoT devices and applications using integrated networks such as wired or wireless secure connections. The network layer is the core layer of the IoT three-layer architecture, as it uses various devices such as routing devices, gateways, switches, and hubs and operates them by using various communication technologies such as WiFi, Bluetooth, 3G, LTE, Zigbee, etc. In summary, the network layer is responsible for transmitting data to and from several applications through interfaces and gateways using multiple communication technologies and protocols.
3. *Application Layer*: Serving as the uppermost tier within the IoT architecture, denoted as the application layer or business layer, as referenced in [58], this layer is tasked with the aggregation of data from the network layer, thereby striving to attain the objective of establishing a smart environment, the ultimate aim of the IoT paradigm. This layer accommodates a diverse array of applications, each characterized by their own requirements. Examples of such applications are smart grids, smart cities, and smart transportation, as elaborated in [62]. Moreover, this layer assumes the responsibility of upholding the data's authenticity, integrity, and confidentiality, as elaborated in [64].

The three-layer architecture is the generalized and most common architecture, and several systems have integrated this architecture [64]. Although this multi-layer architecture seems simple at first glance, the functionalities of the network and application layers might get complex at times. For example, the network layer is not only responsible for data transmission but also provides data services such as data aggregation and processing, etc. On the other hand, the application layer is not solely responsible for providing service to customers and users but also provides data analysis, conducts data mining, etc. Therefore, in response to specific requirements, additional layers have been incorporated, building upon the fundamental layers. For instance, the four-layered or five-layered architectures enhance the system's flexibility. Nonetheless, the three-layer architecture serves as the foundation for all these variations. Furthermore, new-generation applications require shorter response times and low energy consumption as IoT devices have limited capacity [65, 66]. Therefore, researchers have utilized fog and cloud layers, which are visualized in Fig. 1.4.

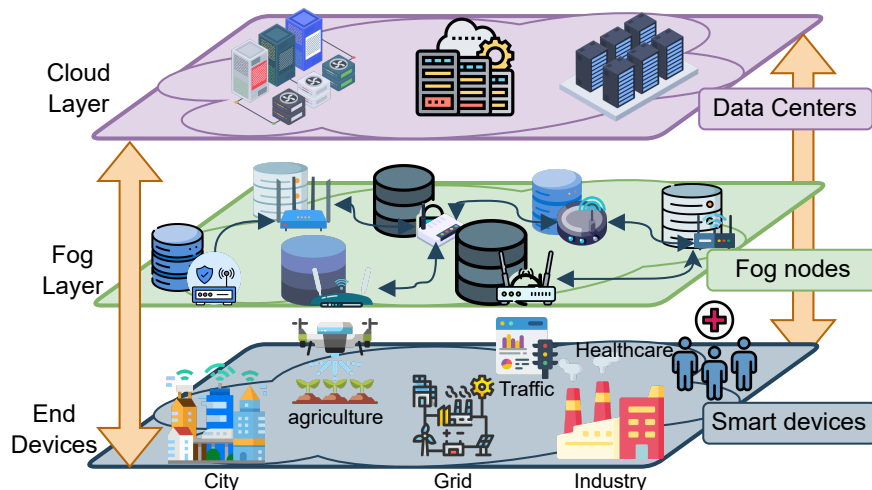


Figure 1.4: Visual representation of Fog vs Cloud

## 1.5 Key Technologies of IoT

IoT requires a variety of technologies to operate, which are deployed in various layers of an IoT architecture, and there are many different sorts of technologies, including hardware technology, software technology, and, most crucially, communication technology. This section discusses crucial IoT technologies that are used to ensure the successful operation of an IoT system. Fig. 1.5 depicts the taxonomy of IoT technologies.

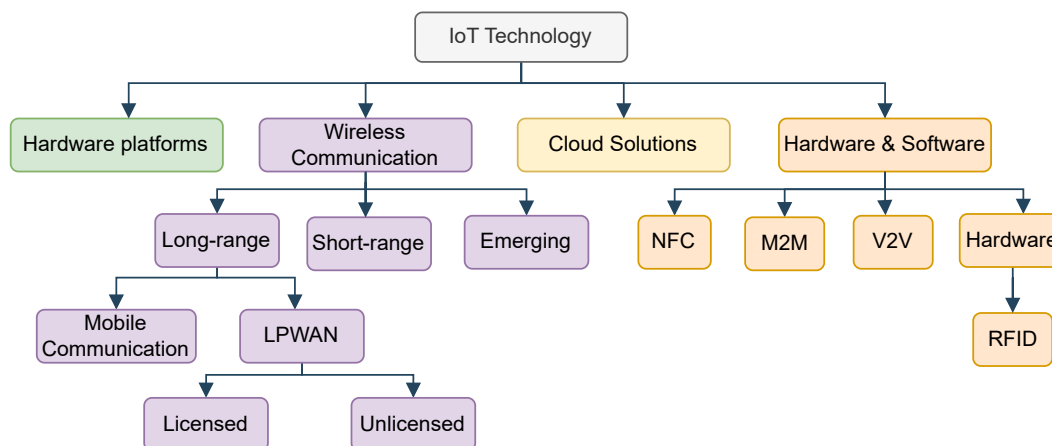


Figure 1.5: Technology Taxonomy of IoT

### 1.5.1 Hardware Platforms

The major components of an IoT system are devices attached to sensors or wearable devices that are used for data collection. Therefore, various types of hardware platforms are used in order to build these sensor devices. Several key points need to be considered before selecting

Table 1.2: Comparison between popular short-range technologies based on various parameters.

Parameters	Bluetooth	ZigBee	LR-WPAN	Wi-Fi	OWC	
					VLC	BS-ILC
Standard	IEEE 802.15.1	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.11a/b/c/d/g/n/ac/ah	IEEE 802.15.7m IEEE 802.15.13	LoRaWAN
Frequency Band	1MHz - 2.48GHz	Mainly at 2.4 GHz Optionally 868MHz or 915MHz	868/915 MHz, 2.4 GHz	a: 5GHz, b: 2.4GHz, g: 2.4GHz, n: 2.4GHz 802.11ah: 1/2/16MHz	400-800 THz	Varies by region, Europe: 868 MHz USA: 915 MHz
Data Rate	1Mbps - 3 Mbps	20kbps to 250kbps	40-250 kbps	a: 54Mbps, b: 11Mbps, g: 54Mbps, ah: 300Mbps n: 600Mbps, ac: 7Gbps	15.13: multi gigabit Recent: 100 Gbps	100Gbps
Transmission range	Classic: 100m BLE: 240m	10-100 meters	10-100 meters	100m to 1km	Typically, within a room 7m: 200 meters 15.13: Several meters	200 meters
Energy consumption	Classic: High BLE: Low	Low	Low	Moderate to high	Transmitters: Moderate Receivers: Minimal	Very low
Cost	Cost-effective	cost-effective	Cost-effective	moderate to high	moderate to high	Cost-effective
RA protocol	FHSS, FDMA TDMA based polling	CSMA/CA	CSMA/CA	CSMA/CD, CSMA/CA	CSMA/CA, TDMA/CDMA	LBT
Modulation type	GFSK, DQPSK, $\pi/4$ -DQPSK	BPSK/O-QPSK	BPSK/O-QPSK	BPSK/QPSK/QAM	OOK/PPM/OFDM	CSS

the hardware platforms, such as the purpose of the IoT device or the type of connectivity it requires.

The two most accessible and popular hardware platforms are the Raspberry Pi and Arduino. Both of them have strong data acquisition, processing, and storage capabilities and provide both wireless and wired connectivity. However, in terms of power management, Arduino is superior to Raspberry Pi because Raspberry Pi does not contain sleep or suspend modes for power utilization, while Arduino does [67]. Intel Galileo Gen and Intel Edison are examples of using an Arduino IDE.

## 1.5.2 Wireless Communication Technology

Given the vast number of devices in the current IoT network and the expectation of diverse connected devices in future IoT applications, there's an urge to develop various technologies to facilitate their connectivity. This subsection explores the existing wireless technologies designed for IoT connectivity and categorizes them into three groups.

### *Short-Range Technologies*

Short-range technologies are commonly used in IoT applications to enable communication between devices within a limited proximity. These technologies are well-suited for scenarios where devices need to exchange data within a small coverage area, typically spanning from a few meters to a few kilometers. There are several short-range technologies, each with unique characteristics and advantages suited for specific purposes. Table 1.2 provides a comprehensive overview of various short-range technologies used in the IoT environment, categorized based on various parameters such as frequency band, data rate, transmission range, and more. The table summarizes the technical specifications of Bluetooth, ZigBee, Wi-Fi, LR-WPAN, VLC, and BS-ILC [68, 32].

Table 1.3: Comparison between popular long-range technologies based on various parameters.

Technologies Parameters	Mobile Communication Technology					LPWAN TECHNOLOGIES			
	2G	3G	4G	5G	WiMax	UNLICENSED LPWAN LoRa	LPWAN Sigfox	LICENSED LPWAN LTE-M	LPWAN NB-IoT
Standard	GSM, CDMA	UMTS, CDMA2000	LTE, LTE-A, IEEE 802.16	5G NR, Wi-Fi 6 (802.11ax)	IEEE 802.16	LoRaWAN R1.0	Proprietary technology	3GPP LTE	3GPP LTE
Frequency band	850MHz, 900MHz, 1800MHz, 1900MHz	850MHz, 1900MHz, 2100MHz	700MHz, 1700/2100MHz, 2500MHz	60MHz - 80GHz	2.3GHz, 2.5GHz, 3.5GHz	Unlicensed ISM bands, 125kHz, 250kHz	Unlicensed ISM bands, 100Hz	Licensed LTE bands, 1.4MHz	Licensed LTE bands, 200kHz
Data rate	9Kbps - 384Kbps	384Kbps - several Mbps	100Mbps - 1Gbps	1Gbps - 20Gbps or higher	16d: 75Mbps 16e: 1Gbps	0.3Kbps - 50Kbps	100bps - 600bps	300bps - 1Mbps	200bps - 250kbps
Transmission range	several kilometers	several kilometers	several kilometers	several kilometers	several kilometers	Urban: 5km Rural: 20km	Urban: 10km Rural: 50km	Urban: 1km Rural: 10km	several kilometers
Energy consumption	low	Moderate	Moderate to high	Low (Energy-efficient)	high	Extremely low	Low	Moderate	Low
RA protocol	TDMA/CDMA/FDMA	CDMA/WCDMA	OFDMA/SC-FDMA	Massive MIMO/beamforming/CP-OFDM	OFDMA/TDD/FDD	ALOHA/Slotted-ALOHA	ALOHA	Slotted-ALOHA	Slotted-ALOHA
Modulation type	GMSK/QPSK	QPSK/16-QAM	OFDM/QPSK/16-QAM/64-QAM/256-QAM	256-QAM	OFDM, QPSK, 16-QAM, 64-QAM	CSS	GFSK/DBPSK	QPSK/QAM/BPSK	QPSK/BPSK
Cost	Cost-effective	Moderate	high	high	high	Cost-effective	Depends on subscription model	Moderate to high	Moderate to high

Bluetooth, ZigBee, LR-WPAN, and BS-ILC offer cost-effective communication solutions, whereas the overall cost of Wi-Fi and VLC may vary depending on usage. In terms of frequency bands, most technologies operate around 2.4 GHz, except for VLC, which utilizes a much larger frequency band. The frequency of BS-ILC varies by region. VLC and BS-ILC prioritize achieving high transmission rates of approximately 100 Gbps, while Wi-Fi transmission rates can vary across different standards. Notably, VLC and BS-ILC exhibit very low energy consumption, as indicated in the table.

### *Long Range Technologies*

Long-range technologies are designed to transmit data or signals over considerable distances, typically much farther than short-range technologies like Bluetooth or Wi-Fi. Long-range technologies are commonly used in various applications, such as long-distance wireless communication, remote monitoring, tracking, and more, and are essential for scenarios where data needs to be transmitted reliably over extensive geographical areas. These technologies can be classified into two main categories: mobile communication technology and LPWAN technologies. Table 1.3 presents a detailed overview of various long-range technologies utilized in the IoT environment. It provides a summary of the technical specifications for various versions of mobile communication technologies as well as different versions of LPWAN technologies.

It is evident from the table that when it comes to mobile communication technologies, 2G, 3G, and 4G operate within a frequency band ranging from approximately 850MHz to 2100MHz, while 5G utilizes a much broader frequency band of up to 80GHz. Additionally, of all five technological variations, 5G offers the highest data rate, exceeding 20Gbps. In terms of energy efficiency, both 2G and 5G have low consumption rates, whereas WiMax exhibits high energy consumption. However, it is worth noting that 3G, 4G, and 5G all come with higher implementation costs. In the UNLICENSED LPWAN category, the top contenders are LoRa and Sigfox, while the most promising options in the LICENSED LPWAN technology are LTE-M (Long-Term Evolution for Machines) and NB-IoT (Narrowband IoT). The key distinction highlighted in the table is that UNLICENSED LPWAN technology operates within unlicensed spectrum resources, leading to lower deployment costs, whereas LICENSED LPWAN technology relies on licensed spectrum resources, resulting in relatively higher expenses for both devices and deployment [68].

### *Emerging For Massive Connectivity*

While current wireless IoT technologies have achieved some success in supporting various IoT applications, they still face challenges in meeting the future demands of IoT. For example, handling the connectivity among a vast number of IoT devices with a limited transmission payload and several random access protocols used by existing technologies often results in significant problems such as frequent access collisions, increased delays, and a high amount of signaling overhead for IoT devices. Furthermore, the constrained availability of wireless resources for connecting IoT devices creates shortages and inefficient utilization of these resources. Hence, there have been numerous ongoing initiatives to tackle the limitations of current technologies. Among these, the solutions CS, NOMA, mMIMO, and ML stand out as the most promising [68].

These emerging technologies offer the capability not only to support massive connectivity

but also to deliver high reliability and low-latency transmissions. However, it is essential to acknowledge that there are existing issues and constraints that must be resolved for their effective implementation. It is anticipated that the development of even more advanced technologies will address critical IoT challenges. Simultaneously, efforts should focus on intelligently integrating existing and emerging technologies to unlock their full potential and optimize system performance [68].

### 1.5.3 Cloud Solutions

IoT cloud solutions offer various services like real-time data collection, data transmission, monitoring, data analytics, improved decision-making, and device management. These services are available on a pay-as-you-use basis, allowing users to pay only for the services they actually use. Cloud platforms can be integrated into numerous domains, including health-care, smart cities, agriculture, education, and supply chain management. For simplicity, Table 1.4 presents several popular platforms in the agriculture domain [32].

Table 1.4: Popular IoT cloud solutions in agriculture domain

IoT Cloud platform	Provider	Real-time Data Capture	Data Visualization	Cloud Service Type	Data Analytics	Developer Cost
ThingSpeak	MathWorks	Yes	Yes (Matlab)	Public	Yes	Free
Plotly	Plotly Technologies Inc.	Yes	Yes	Public	Yes	Free
Carriots	Altair	Yes	Yes	Private	No	Limited up to: 10 devices
Exosite	Exosite	Yes	Yes	IoTSaaS	Yes	2 devices
GroveStreams	GroveStreams LLC	Yes	Yes	Private	Yes	Limited up to: 20 stream, 10K transaction, 5 SMS, 500 Email
ThingWorx	PTC	Yes	Yes	Private	Yes	Pay per use
Nimbits	Open-source	Yes	Yes	Hybrid	No	Free

### 1.5.4 Hardware and Software Technology

This category encompasses a range of hardware and software technologies responsible for different aspects of IoT communication channels. Several technologies, such as NFC and M2M, are considered both hardware and software technologies, whereas RFID is classified as a hardware-only technology. The subsequent sections will provide brief insights into these technologies.

#### *RFID*

RFID is a technology that consists of one or more readers and several RFID tags. These tags are small microchips, have unique codes, and can be on items like products in a store or even access cards. When an RFID reader device sends out electromagnetic radio waves, the tags respond with their unique Electronic Product Codes (EPCs) [69]. The reader captures these codes and sends them to a computer, which can then figure out what the tags belong



to. This technology is used in various ways, like keeping track of inventory in stores, allowing access to secure areas, or monitoring packages as they move through the delivery process.

#### *Near Field Communication (NFC)*

NFC, an extension of RFID technology, is a short-range wireless connectivity technology that uses magnetic field induction to establish communication between devices when they are brought within close proximity of each other without the need for prior connection establishment. NFC chips are equipped in most modern phones, supporting applications like Apple Pay and Google Pay. NFC operates in the unlicensed radio frequency band at 13.56MHz. Its typical range is about 20 meters, with the actual distance often determined by the size of the antenna in the device. It is expected that NFC technology will play a vital role in the future of IoT by providing a wireless connection tool to link with other smart objects. For instance, using NFC on a mobile device, a user can transform their phone into various objects, such as using it as a credit card for transactions [69].

#### *M2M*

M2M communication is gaining popularity and involves direct communication between computers, embedded processors, smart sensors, actuators, and mobile devices. It comprises four main components: *sensing, heterogeneous access, information processing, and applications and processing*. In practical terms, M2M functions within a five-part framework: a device for responding to requests, gateways to interact and connect, an area network for providing connectivity between devices and gateways, applications serving as middleware, and a communication network to facilitate communication between gateways and applications. M2M technology is applied across various sectors, including healthcare, smart robotics, cyber transportation systems (CTS), manufacturing systems, smart home technologies, and smart grids [69].

#### *Vehicle-to-Vehicle Communications (V2V)*

V2V Communications treats each vehicle as a node and enables wireless data exchange (omnidirectional) between vehicles regarding their speed, location, and more. Vehicles equipped with appropriate software, often referred to as safety applications, can use messages from nearby vehicles to detect potential collision risks in real-time. There are two types of communication within this network: one is between vehicles, and the other involves road infrastructure. However, the structure or arrangement of this communication is flexible as vehicles move from one location to another. This network can be divided into four main categories: *safety and collision avoidance, traffic infrastructure management, vehicle telematics, and entertainment services with Internet connectivity* [69].

## 1.6 Applications of IoT

IoT has been effectively integrated into various domains, leading to the development of intelligent applications. While some of these applications are already available, others are still in the research phase. Nevertheless, the essence of these applications indicates that IoT is set to enhance people's lives by providing convenience and flexibility. The following section

has categorized and provided brief descriptions of the areas where IoT integration has been implemented or proposed.

### 1.6.1 Smart Cities

The concept of smart cities can be seen as a complex IoT paradigm where the management of public affairs incorporates the introduction of information and communication technology (ICT) solutions [70]. A smart city utilizes public resources to digitize the city and enhance the quality of life. A real-world example of a smart city implementation is “Padova Smart City”, which has been put into practice in the city of Padova, Italy [71]. Barcelona and Stockholm are two noteworthy examples of smart cities. Barcelona has embarked on the CityOS project, with the primary goal of creating a centralized operating system to manage all the smart devices and services available within the city. Their focus has predominantly been on enhancing smart transportation and water systems. Similarly, Stockholm has also placed significant emphasis on these two domains and holds the distinction of being one of the pioneering cities to implement the concept of congestion charges, wherein users are imposed fees for entering congested areas [4]. In addition, Table 1.5 summarizes related research works in this domain.

Table 1.5: Relevant applications in different Smart Cities domain

Applications	Related Works	Applications	Related Works
Structural health of buildings	[72, 70]	Waste management	[70]
Air quality and noise monitoring	[73, 74]	Smart Transport and Traffic congestion	[4, 75, 76, 77, 78]
Smart grid	[79, 80]	Smart water systems	[81, 4]

#### *Structural Health of Buildings*

This service involves continuous monitoring of areas prone to various external factors and measuring the health of any building. IoT sensors connected to the buildings can store information about the building’s strength, which will help analyze how sturdy the building is or if it requires any refinement [72]. Depending on the usage, one can employ various kinds of sensors, including those for tracking vibrations to measure the stress on the building, temperature and humidity sensors, or other types of atmospheric sensors to assess the level of pollution in an area [70]. Employing IoT in this area can reduce manual labor, where humans have to manually assess the building’s health and environmental conditions, and it can also reduce the overall cost to a great extent.

#### *Waste Management*

Waste management is a crucial operation in any city, whether it is considered a smart city or not, as it directly impacts the livability of the area. Thus, an efficient waste management system is essential for any society. Integrating the IoT into waste management offers multiple benefits. It enables the detection of waste levels and real-time tracking of garbage truck routes, leading to more efficient route planning. Moreover, it can streamline the manual labor involved in waste separation and monitor the disposal process. Sensors on garbage vehicles

connected to a central software system achieve these tasks by analyzing and controlling the system based on the data collected [70]. This approach reduces the cost of manual processes and enhances recycling management.

#### *Air Quality and Noise Monitoring*

Creating a healthy and safe environment for all living beings is crucial, and monitoring air quality and noise levels in any area is a key part of achieving this goal. Various environmental sensors, including soil sensors, temperature and humidity sensors, and gas sensors, can detect the presence of toxic and pollutant substances in the air and assess pollution levels. This information enables local authorities to control pollution, implement effective measures to reduce pollutant levels, identify highly polluted or toxic areas, and designate suitable locations for outdoor activities with good air quality [73, 74]. Likewise, it is essential to maintain a balanced noise level for all living beings in society, including humans and animals. Using noise sensors to measure decibel levels, the central authority can collect data to identify noisy areas and regulate noise levels to keep them within acceptable limits.

#### *Smart Transport and Traffic Congestion*

In today's world, traffic congestion is a widespread issue affecting nearly every country and city, particularly as more than half of the world's population now resides in urban areas [4]. To tackle this issue, many cities have adopted IoT solutions to establish smart transportation systems aimed at managing traffic congestion. These initiatives include *smart traffic lights* [4] and *smart parking system* [77, 78], which collectively enhance transportation capacity and improve safety and speed for travelers. The primary advantages of smart transportation systems are reducing traffic congestion, ensuring hassle-free travel, and facilitating easy parking. Moreover, these systems enable quicker responses in case of accidents and contribute to accident reduction by effectively managing traffic flow [4]. These objectives are achieved through the use of a variety of sensor technologies, including accelerometers for measuring speed, RFIDs for vehicle identification, GPS sensors for location tracking, gyroscopes for direction detection, and cameras for recording traffic patterns and vehicle movements. Some real-world uses of these sensors can be seen in *applications for managing and monitoring traffic* [4, 75], *applications to ensure safety* [76], and *application for detecting accidents*.

#### *Smart grid*

A traditional grid system is an electrical grid that includes transmission lines, transformers, and various communication utilities responsible for delivering electricity from power plants to homes or businesses. One significant limitation of the traditional grid is its one-way communication, which prevents power plants from efficiently responding to increasing power demands from consumers. To address this challenge, the smart grid establishes a two-way communication system between utilities and consumers, which enables more effective management of economic, sustainable, and secure power resources [79]. Integrating IoT into grid systems enables equipping houses and businesses with smart meters that monitor energy generation, storage, and consumption, and transmit this data to the smart grid.

#### *Smart Water Systems*

Water is one of the most critical natural resources, and its scarcity is a prevalent issue in

many parts of the world. Therefore, implementing smart water systems is not a luxury but a necessity. The primary role of smart water systems is to monitor, measure, and efficiently distribute water usage. Hauber-Davidson and Idris have designed a notable model in this field, the smart water metre [81]. These metres can detect water inflow and outflow and identify any potential leaks. Additionally, smart water metres can utilize data from smart river sensors and weather information to assist in flood prediction [4].

## 1.6.2 Medical and Healthcare

The healthcare sector has experienced remarkable advancements through the integration of IoT, offering solutions to real-life healthcare challenges and enhancing people’s lifestyles. Researchers have proposed various applications in healthcare that utilize wearable sensor devices to monitor patients’ health, diagnose diseases, issue emergency alerts, and notify users when necessary. Remote monitoring saves time for both patients and doctors while reducing overall healthcare costs. Furthermore, sharing data collected from these wearable devices with healthcare researchers contributes to the development of safer and more timely healthcare solutions and aids in the discovery of cures and vaccines for emerging diseases. This section explores several IoT applications in healthcare, and a summary of the associated research papers is presented in Table 1.6.

### *Electrocardiogram (ECG) Monitoring*

An ECG measures the heart’s electrical signals and serves as an indicator of heart health, aiding in the detection of conditions like arrhythmia, prolonged QT interval, and myocardial ischemia. An interesting example would be Wu et al.’s ECG data monitoring system [82], where a bipotential chip is utilized by attaching to the user’s t-shirt and transmitting data to a smartphone via Bluetooth. Combining IoT systems with big data analytics enables real-time ECG data monitoring.

### *Glucose Level Monitoring*

Diabetes is a medical condition characterized by higher blood glucose levels than those found in individuals without diabetes. Among various approaches to identifying diabetes, the fingerstick method, involving a small pinprick to the fingertip followed by blood glucose level measurement, remains the most commonly used diagnostic approach. The advent of IoT technology has brought about improvements in this process, making it quicker and more

Table 1.6: Relevant works in medical and healthcare applications

Applications	Related Works	Applications	Related Works
ECG Monitoring	[82, 83]	Glucose level monitoring	[84, 85]
Temperature monitoring	[86, 87]	Blood pressure monitoring	[88, 89]
Oxygen saturation monitoring	[90, 91]	Mood monitoring	[92, 93]
Medication management	[94, 95]	Wheelchair management	[96, 97]
Rehabilitation	[98, 99]	Fitness	[100, 101]
Other notable application	[102, 103, 104, 105], [106, 107, 108, 109]		

convenient for patients. Istepanian et al. [84] have introduced an IoT-integrated noninvasive blood glucose monitoring device to continuously monitor glucose levels, eliminating the need for fingerstick testing. It is worth noting that optical sensors, such as infrared LED and near-infrared photodiode setups, have also been used for glucose level measurements.

#### *Temperature Monitoring*

Traditionally, temperature measurement methods involve using thermometers placed in the mouth, ear, or rectum, but these methods often cause discomfort for the patient and pose an elevated risk of infection. However, recent advancements in IoT-based temperature monitoring applications have effectively addressed these issues. For instance, authors in [86] have introduced a 3D-printed wearable device designed to be inserted into the ear. This device utilizes an infrared sensor to measure temperature from the tympanic membrane, ensuring accuracy while remaining environment-independent.

#### *Blood Pressure Monitoring*

In many diagnostic processes, measuring blood pressure is a compulsory step. However, the major issue with the traditional method is that it requires one person to record the blood pressure. Therefore, the integration of IoT into blood pressure monitoring has been a blessing for both doctors and patients. A wearable cuffless gadget [88], for example, is capable of measuring both systolic and diastolic pressure, with the results stored in the cloud.

#### *Oxygen Saturation Monitoring*

Pulse oximetry, a highly beneficial noninvasive device for measuring oxygen saturation, addresses the limitations of traditional methods and allows for real-time monitoring. The integration of IoT-based technology has led to significant advancements in pulse oximetry, particularly in the healthcare industry. In a study [90], an advanced noninvasive pulse oximetry system has been proposed, capable of measuring oxygen levels, heart rate, and pulse parameters while transmitting this data to a central server.

#### *Mood Monitoring*

The integration of IoT into the mood monitoring domain offers numerous advantages. IoT can detect a person's mental state by analyzing heartbeats through wearable devices. Kaur et al. [92] have proposed a wearable device capable of tracking a driver's emotions, including anger, stress, terror, and sadness. The intelligent system, by analyzing emotion variations, determines whether the driver has entered a subconscious state and stops the vehicle's DC motor accordingly.

#### *Medication Management*

Adherence to medication schedules is vital but challenging for elderly individuals with memory issues. Fortunately, the integration of IoT offers a solution to this problem, and numerous research efforts have explored using IoT to track patients' medication compliance. In [94], a medical box was created to remind individuals to take medications, featuring three trays for different times of the day. The system also measures vital health parameters (i.e., blood pressure, temperature, blood oxygen levels, etc.) and facilitates two-way communication between patients and doctors through a mobile application.

### *Wheelchair Management*

Wheelchairs are vital tools in the lives of individuals who are physically unable to move independently, providing both physiological assistance and psychological support. However, for individuals with brain damage who lack the capability to operate a wheelchair, researchers have been exploring the addition of navigation and tracking systems, with IoT playing a crucial role in these wheelchair advancements. An advanced and automated smart wheelchair was reported in a study [97], which not only monitors movement but also offers features such as an umbrella, foot mat, head mat, and obstacle detection. These innovations have significantly improved interaction with the living environment and enhanced the user's overall experience.

### *Rehabilitation System*

The application of IoT in this field is versatile and has proven effective in various areas, including cancer treatment, sports injury recovery, stroke rehabilitation, and addressing physical disabilities. For instance, an innovative smart walker was introduced in a particular study [98]. Doctors and caregivers can access the collected data through a mobile application, facilitating better monitoring and support, as this walker utilizes a multi-modal sensor to monitor the patient's walking pattern.

### *Fitness*

Regular physical activity and maintaining a high level of fitness significantly influence the quality of an individual's life. Developers have created various applications leveraging the IoT to facilitate fitness monitoring and promote healthier lifestyles. These approaches include assessing users' activity levels and revealing metrics, including the duration of physical activity and periods of inactivity, by utilizing smartphone accelerometer data. Nowadays, wearable fitness trackers are readily available in the market and have gained popularity as convenient devices for monitoring fitness levels, for instance, smart mats to provide insights into users' workout routines [100] and fitness assessment and training load monitoring to optimize athletes' hydration strategies [101].

### *Other Notable Applications*

The application of IoT in the healthcare industry is incredibly diverse, extending far beyond the previously mentioned areas. There are numerous domains where IoT has already been implemented and where its potential benefits are being realized, leading to a significant increase in the adoption of healthcare IoT (HIoT) technology. For cancer treatment, IoT-based methods, for example, have emerged as powerful tools. An innovative IoT-based cancer treatment approach is introduced in a recent study that encompasses various stages, including chemotherapy and radiotherapy [102]. Additionally, this system securely stores lab test results on a cloud server, allowing physicians to monitor medication dosages and enabling remote consultations through a dedicated mobile application. Furthermore, HIoT has found applications in detecting skin lesions [103], with notable advancements in lung cancer detection through state-of-the-art ML algorithms and IoT-based systems [104, 105, 106].

IoT has revolutionized the realm of surgical training and medical procedures by creating next-generation solutions. One such development involves a surgical training framework that



employs virtual reality to simulate realistic training environments. This framework also enables interaction with surgeons from around the world, fostering collaborative learning and expertise sharing [107]. Monitoring haemoglobin levels in the blood has become more accessible through portable devices equipped with photoplethysmography sensors, light-emitting diodes (LEDs), and photodiodes. These devices enable the non-invasive measurement of haemoglobin levels, enhancing healthcare monitoring and diagnosis [109].

Numerous other HIoT applications are currently in use or under research, underscoring the ongoing revolutionary impact of IoT in the field of healthcare. It is expected that the IoT will continue to drive advancements and improvements in healthcare delivery and patient outcomes.

### 1.6.3 Smart Agriculture and Environment

Agriculture holds a crucial position in a country’s economic progress. Various factors, including soil moisture and environmental variables like carbon dioxide levels, temperature, and humidity, can significantly impact crop yields. To enhance agricultural outcomes, it becomes essential to implement robust surveillance systems in the fields. The integration of the IoT enables efficient achievement of this goal. The following section has explored several applications in this smart agricultural domain as well as a summary of the related research work in Table 1.7.

Table 1.7: Relevant studies in smart agriculture and environment domain

Applications	Related Works	Applications	Related Works
Water-saving irrigation	[111, 112]	Diseases Monitoring	[113, 114]
Animal and plant life information monitoring	[115, 116]	Intelligent agricultural machinery	[117, 118]
Agricultural product quality safety and traceability	[119, 120]	Crop growth environment monitoring	[121, 122]

#### *Water Saving Irrigation*

Water scarcity in agriculture is a growing concern, necessitating a dynamic irrigation approach due to varying crop water requirements. IoT integration revolutionizes traditional flood irrigation, offering a solution to water shortage problems in crop growth. Yang et al. [111] have proposed an wireless sensor network based system leveraging neural networks for water-efficient irrigation. This method enhances irrigation efficiency by minimizing human intervention and reducing wastage due to excessive drainage.

#### *Crop Growth Environment Monitoring*

Various environmental factors, including temperature, humidity, air pressure, carbon dioxide levels, soil temperature, and soil pH, play a crucial role in crop growth. IoT devices integrated into agricultural systems can sense and analyze these environmental factors, enabling remote field monitoring and the creation of an optimal farming environment tailored to these variables. Lin et al. [114] have designed a wireless environmental monitoring system that harnesses soil energy to enable cost-effective remote monitoring of farmland environments.

### *Animal and Plant Life Information Monitoring*

Effective agricultural production requires comprehensive monitoring of both plant and animal information, which is crucial for enhancing production, increasing profitability, and ensuring high-quality product development.

1. **Animal Life Information Monitoring:** Monitoring diverse aspects of animal behavior, including their food consumption, body temperature, activity levels, and health status, enables the tracking of their physiological and nutritional well-being, ensuring their healthy development. In [115], the authors have proposed an infrared-based body temperature measurement system for pigs, allowing the early detection of diseases.
2. **Plant Life Information Monitoring:** Wireless sensor devices, when connected to plants, enable remote and continuous monitoring of both external factors (such as diseases, pests, and leaf color) and internal factors (including chlorophyll content and photosynthetic rate). This technology allows for early disease detection and promotes overall healthy plant growth. Porto et al. [116] have introduced a citrus traceability system that assesses environmental conditions for optimal growth, identifying and preventing plant diseases to ensure robust citrus crop health.

### *Intelligent Agricultural Machinery*

Intelligent machinery autonomously manages a wide range of agricultural operations, such as cultivation, sowing, transplanting, fertilization, pesticide application, feeding, irrigation, picking, and harvesting, all executed with precision and efficiency. Moreover, it has the capability to gather a variety of data about the farm, including soil moisture and water quality, as well as ambient information like temperature and humidity, which can be effectively harnessed to implement precision agriculture and enhance breeding practices [123]. IoT technology plays a key role in minimizing manual labor in agriculture by enabling remote monitoring and standardizing machinery functions through sensors and wireless communication [123]. Sowjanya et al. have introduced a versatile autonomous robot vehicle in [117] where the vehicle is equipped with Bluetooth technology for remote control and is capable of independently executing a range of tasks including farming, seeding, and irrigation.

### *Agricultural Product Quality Safety and Traceability*

IoT significantly improves agricultural product quality, safety, and traceability, particularly in warehousing, logistics, and distribution, by enabling automatic identification, tracking, and accurate tallying of products. Various countries have implemented real-time traceability systems, such as the American, European, Swedish, Japanese, and Australian systems, recognizing the crucial need for effective tracking in agriculture. Jiang et al. [119] developed a comprehensive agricultural product safety traceability platform, facilitating real-time automatic data collection, processing, and display to enhance traceability and reduce associated tracking costs.

### *Diseases Monitoring*

The integration of IoT for real-time and continuous monitoring offers farmers and relevant authorities the capability to identify diseases at an early stage and implement preventive

measures before they escalate. The farm's environment plays a pivotal role in disease occurrence. For example, the framework introduced in [121] integrates various sensor devices through wireless sensor networks for monitoring various environmental factors.

#### 1.6.4 Smart Home (SH)

In a smart home, various types of sensors are strategically deployed, each with its own specific function. Smart homes simplify daily tasks for users, proving especially beneficial for those prone to forgetting routine actions like locking doors or turning off appliances. From smart door locks to the maintenance of household items like coffee machines, heaters, and smart bulbs, and even the use of surveillance cameras for enhanced security, smart homes offer a wide range of possibilities. Furthermore, users can control these devices through voice commands and remotely monitor their home equipment. Smart homes contribute to improved energy efficiency by automatically turning off devices not in use and notifying users of any unusual incidents. MavHome [5], for example, employs prediction algorithms to perform various tasks in response to user-initiated events. As for energy conservation, an intelligent home achieves it through the utilization of sensors and the context-aware capabilities of IoT. Data gathered by these sensors is transmitted to a context aggregator, which then forwards the data to a context-aware service engine. This engine analyzes the data and determines appropriate actions. For instance, it may decide to turn off the air conditioning if the temperature is too cold, shut off the gas supply in case of a detected leak, or switch off the lights when there are no occupants at home [124].

#### 1.6.5 Smart Manufacturing System (SMS)

With the development and evolution of IoT, industrial IoT, artificial intelligence, and cyber-physical systems, many countries have opted to transform their manufacturing systems into smart manufacturing systems. Through the integration of smart technologies, these systems facilitate a rapid and extensive flow of data within and among manufacturing processes. Equipped with this data and employing advanced information and communication technology, smart manufacturing systems possess the capability to swiftly respond to global demands, efficiently utilise materials, energy, and labour resources, and deliver customised products on time [125]. What sets the smart manufacturing model apart from other manufacturing paradigms is its vision of the next generation of manufacturing with enhanced capabilities [126]. These systems adapt to new circumstances by leveraging real-time information for intelligent decision-making and by proactively predicting and preventing potential failures.

#### 1.6.6 Internet of Robotics Things (IoRT)

The Internet of Robotic Things is a concept that combines the principles of IoT and robotics. IoRT represents an emerging technology that incorporates robots within an IoT ecosystem as objects, enabling communication, collaboration, and automation. These robots seamlessly integrate into smart environments, performing a wide range of tasks. These tasks span from

personal activities within smart homes to applications in the healthcare industry. Furthermore, they extend to professional activities such as monitoring, delivery, and object control within manufacturing industries or warehouses.

### 1.6.7 Oil and Gas Industry

The oil and gas industry, facing substantial costs and safety risks, embraces IoT-based remote monitoring for real-time field equipment oversight and data-driven decision-making. These solutions allow for the remote monitoring of field equipment, the analysis of field data, collaborative data-driven decision-making, and the implementation of control commands to optimize asset performance while mitigating health, safety, and environmental (HSE) hazards [127]. Furthermore, IoT integration in the oil industry focuses on reducing human labor, minimizing time wastage, and improving accuracy through automation, as exemplified by Equinor’s well optimization system in the Bakken oil field [?]. By deploying IoT devices and ML algorithms in around 50 wells, Equinor achieved a 33% increase in oil production through optimized well operation and maintenance.

### 1.6.8 Smart Retail

The adoption of IoT in the retail industry has created a flexible environment that benefits both customers and sellers. This shift allows the entire retail sector to migrate from offline to online, enabling customers to independently conduct their shopping through self-service while facilitating smooth interactions between retailers and their customers. Furthermore, retailers can employ IoT technologies like RFID to monitor products and deploy sensors to collect customer data, which they can then utilize for analyzing customer buying behavior and enhancing business profitability [129, 130]. Additionally, customers have the option to make payments through online transactions and monitor their orders using online services [128].

### 1.6.9 Industrial Internet of Things (IIoT)

The IIoT holds significant potential, according to numerous market researchers, by serving as an extension of the IoT specifically customized for the industrial sector and its applications. It empowers industries and enterprises to enhance and optimize their operations by leveraging M2M communication, big data analytics, and ML. The scope of IIoT is extensive, encompassing a wide array of connected industrial devices and systems. Connected electric meters, wastewater systems, flow gauges, pipeline monitors, manufacturing robots, and various other types of industrial equipment and devices are included in this list [131]. One notable application of IIoT is in the mining industry, where companies like CISCO have implemented IIoT solutions to improve safety and efficiency in underground mines. These solutions involve connecting people, tracking the locations of miners and vehicles, monitoring vehicle statuses, and automating building controls.

### 1.6.10 Social Life and Entertainment

Several applications have been developed to monitor and enhance human social activities, in addition to work or professional activities, as social life and entertainment are integral parts of a person’s life. Portable devices such as mobile phones and tablets possess sensing capabilities and communication technologies that facilitate interactions between individuals. Integrating IoT into an individual’s social life can contribute to emotion detection, community building, and emotional support. CircleSense [134] is an application that analyzes a person’s social activities using various sensors to identify their social circle. It also tracks the person’s location via location sensors and employs Bluetooth technology to identify people in proximity. Camy, an artificial pet dog, expresses affection and empathy through the use of effective computing technology. This technology analyzes multiple aspects of a person’s behavior, such as facial expressions, speech, body gestures, hand movements, and sleep patterns, to identify and appropriately respond to their emotions [135]. A Table 1.8 has been provided for presenting information about relevant works in the aforementioned domains.

Table 1.8: Relevant works in other applications

Applications	Related Works	Applications	Related Works
Social Life and Entertainment	[134, 135]	Smart manufacturing system	[125, 126]
Internet of robotics things	[137, 138]	Oil and gas	[127]
Smart Retail	[129, 130]	Industrial IoT	[132, 133]
Smart home	[5, 136]		

## 1.7 Challenges and Future Directions

The remarkable position that IoT now occupies in today’s world was once only a dream a few years ago. Today, IoT has captivated the entire globe and continues to extend its reach into various domains. Nonetheless, IoT also grapples with numerous issues and challenges that pose hurdles to its seamless implementation and expansion. This section offers an in-depth exploration of the key challenges confronting the IoT.

### 1.7.1 Broad and Open Research Challenges

Broad and open research challenges refer to complex and critical challenges in the IoT system that do not have any straightforward or predefined solutions. These challenges require extensive research and exploration in order to propose efficient solutions. They are “broad” in the sense that they encompass a wide range of related issues and considerations, and they are “open” because they may not have clear-cut or definitive answers, leaving room for ongoing research, experimentation, and discovery. This subsection provides a comprehensive listing of challenges in the IoT domain.

### *Building Intelligent Environments based on IoT Paradigm*

Creating a smart environment requires a vast number of devices, sensors, and complementary technologies to facilitate their interconnectivity. Managing this large volume of objects constitutes the initial challenge in the realm of IoT and intelligent environments. Moreover, the substantial task of collecting, storing, and conducting efficient analyses on enormous amounts of data remains a significant concern and creates collision issues within the IoT framework [139]. Handling massive amounts of devices and data in the IoT requires. One approach is to employ decentralized systems instead of centralized ones, reducing the volume of data sent to the cloud for processing. Techniques like data filtering, compression, and load balancing can further minimize the size of the data. Utilizing IoT technologies with robust device management and maintenance capabilities is also beneficial. Additionally, leveraging big data technologies like Hadoop and Spark can efficiently handle the substantial IoT data volumes. This holistic approach ensures readiness for the expanding IoT landscape.

### *Privacy and Security Challenges of IoT Applications*

The heterogeneity of IoT devices and the diversity of various IoT applications result in various security and privacy issues. People are primarily concerned about potential privacy invasions and security threats when using these technological devices. More information is provided below.

1. Security: Different layers of the IoT are vulnerable to various kinds of attacks based on the technologies and protocols used in these layers. According to [140], IoT layers including *perception layer*, *network layer*, and *application layer* face various security attacks. As the major role of the *perception layer* is to collect data, the security challenges in this layer focus on falsifying the data and destroying perception devices. Attacks including *Node Capture Attacks*, *Malicious code Injection Attacks*, *False Data Injection Attacks*, *Replay Attacks*, *Cryptanalysis Attacks* and *Side Channel Attacks*, *Eavesdropping and Interference*, and *Sleep Deprivation Attacks* are faced by this layer [140].

Since the basic function of *network layer* is to transmit collected data, particularly using wireless technologies, security challenges in this layer revolve around the availability of network resources and the wireless network. Challenges at the Network Layer encompass *Denial-of-Service (DoS) Attacks*, *Spoofing Attacks*, *Sinkhole Attacks*, *Wormhole Attacks*, *Man-in-the-Middle Attacks*, *Routing Information Attacks*, *Sybil Attacks*, and *Unauthorized Access* [140]. *Application layer*, which focuses on providing user-requested services, challenges primarily revolve around *software attacks*, including *phishing attacks*, *malicious viruses/worms*, *malicious scripts* [140].

It is imperative to propose secure, robust, and reliable authentication schemes to detect and defend unauthorized access [141]. Virus detection techniques and script detection techniques such as honeypot techniques, static code analysis, and dynamic action detection must be implemented to defend against worms, viruses, and malicious scripts bridging firewalls. Furthermore, introducing secured routing protocols is essential to ensure secure routing.

2. Privacy: IoT devices continuously generate vast amounts of real-time data, which



undergoes three main stages: (1) Data Collection, (2) Data Aggregation, and (3) Data Mining and Analytics. While these processes enhance our lives by providing various services, they also raise concerns about data privacy in the IoT. Privacy breaches in IoT can have serious repercussions for both the IoT network and its users, including financial losses, property damage, and even risks to human safety and security [140, 142].

For instance, consider the smart grid, where adversaries can readily seize control of the smart metres, allowing them to access or manipulate the collected data. This could potentially compromise the confidentiality and privacy of energy consumption data. By using this altered data, utility providers may make inaccurate assessments of energy supply and demand within the grid, resulting in erroneous energy dispatch decisions. This, in turn, could lead to imbalances in energy supply and demand, potentially causing widespread power outages. In the healthcare industry, if an adversary manages to acquire a patient's health data, they could manipulate medication prescriptions or medical records, leading to significant health risks and potential insurance fraud. Therefore, it is imperative to deploy privacy preservation schemes to prevent data leakage and ensure that private data remains inaccessible to adversaries [140, 143].

There are three main groups for categorizing privacy-preserving mechanisms in the context of IoT data processing: (i) privacy preservation during data collection, (ii) privacy preservation during data aggregation, and (iii) privacy preservation during data mining and analytics. While various techniques, such as encryption and key management, can be applied to protect privacy in data collection, mining, and analytics, the majority of efforts in IoT privacy preservation have focused on data aggregation. Data aggregation involves processing relevant data in multiple locations, making it challenging to ensure privacy using traditional encryption methods. As a result, researchers have developed several privacy-preserving mechanisms specifically for data aggregation, which can be categorized as follows:

- (a) *Anonymity-based privacy preservation*, which employs techniques like K-anonymity, L-diversity, and T-closeness to protect the privacy of identification information during data aggregation.
- (b) *Encryption-based privacy preservation*, which prevents adversaries from eavesdropping on data during aggregation by utilizing encryption techniques such as homomorphic encryption, commitment mechanisms, secret sharing, and zero-knowledge proofs [144, 145].
- (c) *Perturbation-based privacy preservation*, where techniques such as data customization, data sharing, and random noise injection perturb raw data to ensure privacy during aggregation.

Among these, perturbation-based privacy-preserving schemes are popular in IoT due to their direct operation on raw data. However, many of these perturbation-based privacy-preserving schemes sacrifice data utility to achieve privacy. This reduction in data utility can hinder the support of services requested by IoT applications. Therefore, a significant challenge in the field of data privacy preservation in the IoT is designing

schemes that strike a balance between privacy and data utility, making it a crucial area for future research [21, 140]. In summary, safeguarding data privacy in the IoT is crucial to preventing these adverse outcomes and maintaining the security and integrity of both individuals and the IoT ecosystem.

### *Compatibility*

Interconnecting devices from various vendors in an IoT network can pose monitoring and management challenges. Different industries currently rely on a multitude of standards to support their applications. Given the vast amounts of data, diverse device types, and the presence of various entities, utilising standard interfaces becomes crucial. This importance is amplified, especially for applications that need to accommodate both cross-organisational collaborations and a wide array of system limitations. Addressing these issues requires all industries to adhere to specific standards, but achieving such universal compliance can be a daunting and impractical task.

### *Scalability*

In the future, heterogeneous devices are expected to continuously join the ever-expanding IoT network. As a result, as the number of devices increases, ensuring smooth connectivity, effective data management, and overall system performance on a small scale becomes increasingly challenging. Therefore, the scalability of IoT poses an ongoing challenge for the future of this technology. To effectively address scalability challenges, it is essential to construct a scalable architecture, utilizing technologies like modular components, load balancers, and distributed systems.

### *Energy Efficiency*

Small smart devices that comprise IoT systems often have limited battery power, which is not easily replaceable. This limitation can lead to a global energy crisis and high power consumption, as well as constraints on memory and processing capabilities. Consequently, routing processes and compute-intensive applications may not run efficiently on these devices. While some routing protocols do support low-power communication, they are still in the early stages of development, and the constrained energy of smart devices may not be sufficient to fully utilize these WSN routing protocols. To tackle these challenges effectively, it's essential to emphasize the creation of low-power hardware and the adoption of energy-efficient protocols like MQTT-SN or CoAP rather than relying on more power-intensive alternatives such as HTTP. Additionally, harnessing over-the-air (OTA) firmware updates can ensure devices remain optimized and bug-free, thus diminishing the necessity for physical maintenance visits. Duty cycling, as another viable approach, aids in curbing power consumption significantly.

### *Mobility Management*

Mobility management in the IoT refers to the ability to handle devices that move within the network seamlessly. It is a crucial aspect because many IoT devices are not stationary and need to communicate as they change locations. The presence of mobile devices in IoT setups can lead to challenges in how routing protocols and IoT networks work efficiently. The cur-

rent methods used for devices that move, like in sensor networks, mobile adhoc networks, and vehicular networks, can't effectively handle the various problems related to routing because these sensors have limited processing power and energy resources. To address these challenges, IoT systems employ various mobility management techniques and protocols, aiming to provide reliable and seamless communication for mobile devices in the IoT ecosystem.

#### *Cost of Maintenance and Services*

The IoT network consists of a vast number of devices, utilizing various costly communication technologies. This inevitably leads to increased maintenance and service costs for these numerous devices and connections. Hence, a significant challenge lies in addressing this issue by designing devices and sensors that demand minimal maintenance.

#### *Internet Disconnection Problem*

The disruption of internet connectivity, which is central to IoT operations, results in inferior performance from IoT applications and a decline in service quality. Furthermore, restrictions on the number of devices that can concurrently interact with the base station limit user access to these services. This issue is especially problematic in remote or unreliable network settings, where sustaining a consistent internet connection proves challenging. Consequently, addressing the problem of internet disconnections in IoT is imperative to maintain the reliability and efficiency of IoT systems.

#### *Processing, Analysis and Management of Data*

The procedure for processing, analysing, and managing data is tremendously challenging because of the heterogeneous nature of IoT devices and the large scale of data generation. Currently, most systems utilize the centralized cloud-based systems for performing computationally intensive tasks and delivering data. However, an ongoing concern revolves around the limitations of traditional cloud architectures when it comes to efficiently handling the vast amounts of data generated and utilized by IoT-enabled devices. Additionally, these architectures struggle to support the associated computational demands while also meeting precise timing constraints. To address this challenge, most systems are currently relying on existing solutions like mobile cloud computing and fog computing, both of which utilize edge processing [146].

#### *Other Challenges*

In addition to the previously mentioned challenges, IoT technology faces several other issues. The widespread adoption of IoT devices and technology, coupled with our increasingly reliant lifestyles, has led to users becoming highly dependent on IoT applications. This reliance is particularly critical in healthcare, where patients heavily depend on healthcare applications. Moreover, IoT devices can sometimes unexpectedly interfere with human activities, resulting in unanticipated and autonomous behaviors. The IoT network introduces ambiguity, making it challenging to distinguish between physical and virtual devices and even humans due to the ease of transformation between these categories. Quality and traffic control have become more complex due to the miniaturization and huge number of IoT devices. Managing unique identifications for each IoT device is also a growing concern. Furthermore, the IoT goes beyond geographical boundaries, with applications like healthcare offering services

internationally. Nations face challenges due to the global reach of IoT, as data generated within their borders can be collected and transmitted to service providers located anywhere in the world, giving rise to concerns regarding data privacy and jurisdiction. Addressing these multifaceted challenges will require careful consideration and international collaboration to ensure the effective and secure implementation of IoT technology.

### 1.7.2 Ethical Considerations

The term “ethical issue” pertains to a situation or quandary characterized by a clash of moral principles, values, or ethical norms [147]. The realm of IoT confronts these ethical quandaries, necessitating individuals or organizations to make challenging choices amidst conflicting interests. These decisions frequently revolve around determining what is ethically correct or incorrect. Figure 1.6 illustrates prevalent ethical dilemmas within the IoT domain.



Figure 1.6: Ethical Issues in IoT

Adapted from [148], the following outlines the five main categories that divide the ethical concerns related to IoT. The aim of putting forth these issues is to safeguard privacy rights by regulating how organizations manage information generated by IoT devices. These ethical standards, designed to establish guidelines for organizations, should also prompt individual concerns regarding privacy, as they serve as legal safeguards to protect individuals.

1. *Information privacy considerations*: Organizations must handle the produced data with both openness and transparency. Except in specific cases, they should offer choices to individuals, allowing them not to disclose their identity or to use a pseudonym.

2. *Information collection*: Organizations can gather requested data by implementing more stringent criteria for acquiring ‘sensitive’ information. Conversely, they should specify their approach to handling unsolicited information. In both situations, organizations are required to delineate the circumstances surrounding the collection of this information and provide prior notification to relevant parties.
3. *Managing data*: Organizations should specify the situations in which they might utilize or share the information they have gathered. Under specific conditions, an organization can employ personal data for direct marketing purposes. Nonetheless, they have the option of disclosing it internationally, but before doing so, they must set the safeguards that will be used to protect this information.
4. *Integrity of information*: Entities should gather and share precise, current, and comprehensive information. Reasonable precautions must be in place to prevent misuse, interference, loss, and unauthorized access, changes, or disclosure.
5. *Information rectification and availability*: When requesting access to their information, entities should clearly state their responsibilities for allowing access and making corrections to the information they possess. This involves the obligation to grant access and make necessary modifications, except in cases where a particular exception is applicable.

### 1.7.3 Legal and Regulatory Issues

After identifying the challenges and ethical concerns, there is a need to consider the legal aspects concerning the effectiveness of current laws in safeguarding users within this context. The significance of this concern arises from the increasing blurring of the boundary between the physical and virtual realms in IoT. The ensuing questions, depicted in Fig. 1.7, serve as examples of the issues that require discussion, as referenced in [147].

Considering the challenges mentioned in Section 1.7, it is evident that IoT faces several obstacles, including financial constraints, security vulnerabilities, and data privacy concerns, which can have life-threatening implications, especially in healthcare data breaches. To address these challenges effectively, a proactive approach involving extensive research is crucial. This research should focus on identifying IoT’s specific issues, followed by the implementation of robust technical solutions. Effective execution of this process will not only ensure a secure IoT system but also encourage user trust in enrolling themselves within the IoT network.

To mitigate ethical concerns, raising user awareness is essential, along with the integration of self-adaptive security policies and dynamically modifiable policies during IoT application development. The introduction of new laws and standards is also necessary, integrating existing regulations like HIPPA, FIPPS, the Electronic Communication Privacy Act, and others to comprehensively address security, privacy, and legal issues. Additionally, addressing technical challenges involves the introduction of adaptable and new standards as well as the implementation of standard address identification. Some examples of these technical solutions include advanced encryption techniques, electronic signatures, the integration of

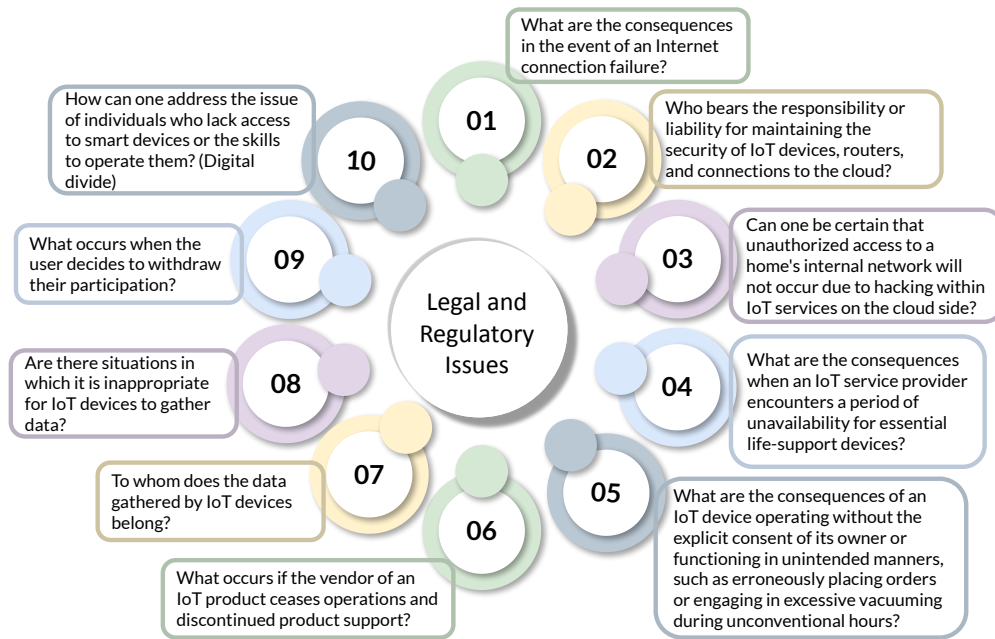


Figure 1.7: Legal and Regulatory Issues of IoT

standard protocols, and regulations to limit third-party data usage. This holistic approach aims to overcome the multifaceted challenges that the IoT faces.

## 1.8 Conclusions

The IoT has rapidly become an integral part of the 21<sup>st</sup> century, enhancing daily decision-making and ushering in innovative consumer services like pay-as-you-use. The seamless integration of smart devices and automation technologies has revolutionized every aspect of our lives. However, amidst this technological marvel, we must acknowledge significant concerns related to security, privacy, intellectual property rights, safety, and trust. These concerns continue to demand further investigation. This chapter has provided a comprehensive overview of IoT for newcomers seeking to explore this domain and gain a thorough understanding to make future contributions. The chapter covers fundamental IoT concepts, historical development, architectures, advantages, and technology taxonomy. It explores diverse applications in domains such as smart cities and healthcare while addressing challenges and providing possible future directions. This discussion serves as a solid foundation for researchers interested in developing practical IoT projects or pioneering new theoretical approaches within the IoT field, equipping them with a deep understanding of various aspects of IoT. This, in turn, provides a good ground for researchers who are interested in designing realistic IoT projects or developing novel theoretical approaches in the IoT field.



by acquiring deep knowledge in different IoT aspects.

## References

- [1] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, *et al.*, “Internet of things strategic research roadmap,” in *Internet of things-global technological and societal trends from smart environments and spaces to green ICT*, pp. 9–52, River Publishers, 2022.
- [2] I. Peña-López *et al.*, “Itu internet report 2005: the internet of things,” 2005.
- [3] W. Contributors, “Internet of things,” 2023. [Online; accessed September 16, 2023].
- [4] P. Sethi, S. R. Sarangi, *et al.*, “Internet of things: architectures, protocols, and applications,” *Journal of electrical and computer engineering*, vol. 2017, 2017.
- [5] D. J. Cook, M. Youngblood, E. O. Heierman, K. Gopalratnam, S. Rao, A. Litvin, and F. Khawaja, “Mavhome: An agent-based smart home,” in *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003.(PerCom 2003).*, pp. 521–524, IEEE, 2003.
- [6] P. Dalal, G. Aggarwal, and S. Tejasvee, “Internet of things (iot) in healthcare system: Ia3 (idea, architecture, advantages and applications),” in *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 2020.
- [7] D. Technologies, “Internet of things and data placement.” [Online; accessed October 02, 2023].
- [8] T. Kramp, R. Van Kranenburg, and S. Lange, “Introduction to the internet of things,” *Enabling things to talk: Designing IoT solutions with the IoT architectural reference model*, pp. 1–10, 2013.
- [9] K. Lakhwani, H. K. Gianey, J. K. Wireko, and K. K. Hiran, *Internet of Things (IoT): Principles, paradigms and applications of IoT*. Bpb Publications, 2020.
- [10] A. Nagaraj, *Introduction to sensors in IoT and cloud computing applications*. Bentham Science Publishers, 2021.
- [11] S. Greengard, “Internet of things,” 2023. [Online; accessed September 16, 2023].
- [12] W. Contributors, “Machine to machine,” 2023. [Online; accessed September 16, 2023].
- [13] V. of Humanity, “Iot technologies explained: History, examples, risks & future,” 2023. [Online; accessed September 16, 2023].

- [14] K. Rose, S. Eldridge, and L. Chapin, “The internet of things: An overview,” *The internet society (ISOC)*, vol. 80, pp. 1–50, 2015.
- [15] J. Romkey, “Toast of the iot: the 1990 interop internet toaster,” *IEEE Consumer Electronics Magazine*, vol. 6, no. 1, pp. 116–119, 2016.
- [16] M. Weiser, “The computer for the 21 st century,” *Scientific american*, vol. 265, no. 3, pp. 94–105, 1991.
- [17] R. Raji, “Smart networks for control,” *IEEE Spectrum*, vol. 31, no. 6, pp. 49–55, 1994.
- [18] K. D. Foote, “A brief history of the internet of things,” 2022. [Online; accessed September 16, 2023].
- [19] A. Schmidt and K. Van Laerhoven, “How to build smart appliances?,” *IEEE personal communications*, vol. 8, no. 4, pp. 66–71, 2001.
- [20] M. L. Nerkar, “Recognize human physical activity using smartphone sensors: A review,”
- [21] M. Saifuzzaman, T. N. Ananna, M. J. M. Chowdhury, M. S. Ferdous, and F. Chowdhury, “A systematic literature review on wearable health data publishing under differential privacy,” *International Journal of Information Security*, vol. 21, no. 4, pp. 847–872, 2022.
- [22] J. H. Gruzelier, “Eeg-neurofeedback for optimising performance. i: A review of cognitive and affective outcome in healthy participants,” *Neuroscience & Biobehavioral Reviews*, vol. 44, pp. 124–141, 2014.
- [23] P. K. Sekhar, E. L. Brosha, R. Mukundan, and F. Garzon, “Chemical sensors for environmental monitoring and homeland security,” *The Electrochemical Society Interface*, vol. 19, no. 4, p. 35, 2010.
- [24] S. Manna, S. S. Bhunia, and N. Mukherjee, “Vehicular pollution monitoring using iot,” in *International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)*, pp. 1–5, IEEE, 2014.
- [25] A. S. Gillis, “Iot gateway.” [Online; accessed October 03, 2023].
- [26] C. Point, “What is an iot gateway?.” [Online; accessed October 03, 2023].
- [27] daviteq, “Iot gateway – a key to connect the world,” 2020. [Online; accessed October 03, 2023].
- [28] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
- [29] Tisha, “What are the major components of internet of things (iot)?,” 2023. [Online; accessed October 03, 2023].

- [30] A. Junnila, “How iot works – part 4: User interface.” [Online; accessed October 03, 2023].
- [31] S. Sebastian, P. Ray, *et al.*, “Development of iot invasive architecture for complying with health of home,” *Proceedings of I3CS, Shillong*, pp. 79–83, 2015.
- [32] P. P. Ray, “A survey on internet of things architectures,” *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, 2018.
- [33] R. Sultania, “What are the characteristics of internet of things(iot),” 2023. [Online; accessed October 03, 2023].
- [34] S. Kuyoro, F. Osisanwo, and O. Akinsowon, “Internet of things (iot): an overview,” in *Proc. of the 3th International Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM)*, pp. 23–24, 2015.
- [35] N. Zubovich, “Advantages of internet of things: 10 benefits you should know,” 2023. [Online; accessed September 15, 2023].
- [36] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, “A review and state of art of internet of things (iot),” *Archives of Computational Methods in Engineering*, pp. 1–19, 2021.
- [37] G. Gimpel, “Bringing dark data into the light: Illuminating existing iot data lost within your organization,” *Business Horizons*, vol. 63, no. 4, pp. 519–530, 2020.
- [38] Y. Khan, M. B. M. Su’ud, M. M. Alam, S. F. Ahmad, A. Y. B. Ahmad, and N. Khan, “Application of internet of things (iot) in sustainable supply chain management,” *Sustainability*, vol. 15, no. 1, p. 694, 2022.
- [39] Impactmybiz, “5 benefits of the internet of things (iot) for smbs,” 2022. [Online; accessed October 03, 2023].
- [40] O. Elijah, T. A. Rahman, I. Oriikumhi, C. Y. Leow, and M. N. Hindia, “An overview of internet of things (iot) and data analytics in agriculture: Benefits and challenges,” *IEEE Internet of things Journal*, vol. 5, no. 5, pp. 3758–3773, 2018.
- [41] Y. Bo and H. Wang, “The application of cloud computing and the internet of things in agriculture and forestry,” in *2011 International Joint Conference on Service Sciences*, pp. 168–172, IEEE, 2011.
- [42] H. J. Marvin, Y. Bouzemrak, E. M. Janssen, H. v. van der Fels-Klerx, E. D. van Asselt, and G. A. Kleter, “A holistic approach to food safety risks: Food fraud as an example,” *Food research international*, vol. 89, pp. 463–470, 2016.
- [43] L. Manning, “Food fraud: Policy and food chain,” *Current Opinion in Food Science*, vol. 10, pp. 16–21, 2016.
- [44] D. Folinas, I. Manikas, and B. Manos, “Traceability data management for food chains,” *British Food Journal*, vol. 108, no. 8, pp. 622–633, 2006.

- [45] M. Asplund and S. Nadjm-Tehrani, “Attitudes and perceptions of iot security in critical societal services,” *IEEE Access*, vol. 4, pp. 2130–2138, 2016.
- [46] M. Selinger, A. Sepulveda, J. Buchan, *et al.*, “Education and the internet of everything,” *Cisco Consulting Services and Cisco EMEAR Education Team*, 2013.
- [47] R. Lutz, “The implications of the internet of things for education,” *Retrieved on*, 2014.
- [48] L. Barreto, A. Amaral, and T. Pereira, “Industry 4.0 implications in logistics: an overview,” *Procedia manufacturing*, vol. 13, pp. 1245–1252, 2017.
- [49] G.-H. Kim, O.-H. Kwon, and A.-S. Oh, “Design of warehouse management system using ips under bluetooth environment,” *International Journal of Multimedia and Ubiquitous Engineering*, vol. 11, no. 6, pp. 281–288, 2016.
- [50] W. Ding, “Study of smart warehouse management system based on the iot,” in *Intelligence Computation and Evolutionary Computation: Results of 2012 International Conference of Intelligence Computation and Evolutionary Computation ICEC 2012 Held July 7, 2012 in Wuhan, China*, pp. 203–207, Springer, 2013.
- [51] K. Rameel, A. Bhujbal, and M. Goudar, “Iot enabled automated robotic service for warehouses,” *Int. J. Eng. Technol. Sci. Res.*, vol. 4, pp. 588–592, 2017.
- [52] S. Liawatimena, B. Felix, A. Nugraha, and R. Evans, “A mini forklift robot,” in *The 2nd International Conference on Next Generation Information Technology*, pp. 127–131, IEEE, 2011.
- [53] S. Lu, C. Xu, R. Y. Zhong, and L. Wang, “A rfid-enabled positioning system in automated guided vehicle for smart factories,” *Journal of Manufacturing Systems*, vol. 44, pp. 179–190, 2017.
- [54] A. S. Alluhaidan, M. S. Alluhaidan, and S. Basheer, “Retracted article: Internet of things based intelligent transportation of food products during covid,” *Wireless personal communications*, vol. 127, no. Suppl 1, pp. 27–27, 2022.
- [55] F. Famá, J. N. Faria, and D. Portugal, “An iot-based interoperable architecture for wireless biomonitoring of patients with sensor patches,” *Internet of Things*, vol. 19, p. 100547, 2022.
- [56] Y. Song, F. R. Yu, L. Zhou, X. Yang, and Z. He, “Applications of the internet of things (iot) in smart logistics: A comprehensive survey,” *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4250–4274, 2020.
- [57] S. M. Nagarajan, G. G. Deverajan, P. Chatterjee, W. Alnumay, and V. Muthukumar, “Integration of iot based routing process for food supply chain management in sustainable smart cities,” *Sustainable Cities and Society*, vol. 76, p. 103448, 2022.
- [58] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

- [59] B. Varghese and R. Buyya, “Next generation cloud computing: New trends and research directions,” *Future Generation Computer Systems*, vol. 79, pp. 849–861, 2018.
- [60] M. Satyabrata, “Iot functional blocks,” 2023. [Online; accessed August 26, 2023].
- [61] L. Atzori, A. Iera, G. Morabito, and M. Nitti, “The social internet of things (sIoT)—when social networks meet the internet of things: Concept, architecture and network characterization,” *Computer networks*, vol. 56, no. 16, pp. 3594–3608, 2012.
- [62] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, “Internet of things (IoT) security: Current status, challenges and prospective measures,” in *2015 10th international conference for internet technology and secured transactions (ICITST)*, pp. 336–341, IEEE, 2015.
- [63] M. Leo, F. Battisti, M. Carli, and A. Neri, “A federated architecture approach for internet of things security,” in *2014 Euro Med Telco Conference (EMTC)*, pp. 1–5, IEEE, 2014.
- [64] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, “Research on the architecture of internet of things,” in *2010 3rd international conference on advanced computer theory and engineering (ICACTE)*, vol. 5, pp. V5–484, IEEE, 2010.
- [65] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, “Edge computing: Vision and challenges,” *IEEE internet of things journal*, vol. 3, no. 5, pp. 637–646, 2016.
- [66] B. Nour, S. Mastorakis, and A. Mtibaa, “Compute-less networking: Perspectives, challenges, and opportunities,” *IEEE network*, vol. 34, no. 6, pp. 259–265, 2020.
- [67] M. Murphy, “8 best IoT hardware platforms (2022 edition),” 2021. [Online; accessed October 03, 2023].
- [68] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, “IoT connectivity technologies and applications: A survey,” *IEEE Access*, vol. 8, pp. 67646–67673, 2020.
- [69] S. H. Shah and I. Yaqoob, “A survey: Internet of things (IoT) technologies, applications and challenges,” *2016 IEEE Smart Energy Grid Engineering (SEGE)*, pp. 381–385, 2016.
- [70] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” *IEEE Internet of Things journal*, vol. 1, no. 1, pp. 22–32, 2014.
- [71] A. Cenedese, A. Zanella, L. Vangelista, and M. Zorzi, “Padova smart city: An urban internet of things experimentation,” in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, pp. 1–6, IEEE, 2014.
- [72] J. P. Lynch and K. J. Loh, “A summary review of wireless sensors and sensor networks for structural health monitoring,” *Shock and vibration digest*, vol. 38, no. 2, pp. 91–130, 2006.

- [73] N. Maisonneuve, M. Stevens, M. E. Niessen, P. Hanappe, and L. Steels, “Citizen noise pollution monitoring,” 2009.
- [74] X. Li, W. Shu, M. Li, H.-Y. Huang, P.-E. Luo, and M.-Y. Wu, “Performance evaluation of vehicle-based mobile sensor networks for traffic monitoring,” *IEEE transactions on vehicular technology*, vol. 58, no. 4, pp. 1647–1653, 2008.
- [75] J.-W. Hsieh, S.-H. Yu, Y.-S. Chen, and W.-F. Hu, “Automatic traffic surveillance system for vehicle tracking and classification,” *IEEE Transactions on intelligent transportation systems*, vol. 7, no. 2, pp. 175–187, 2006.
- [76] W. Hu, X. Hu, J.-q. Deng, C. Zhu, G. Fotopoulos, E. C.-H. Ngai, and V. C. Leung, “Mood-fatigue analyzer: towards context-aware mobile sensing applications for safe driving,” in *Proceedings of the 1st ACM Workshop on Middleware for Context-Aware Applications in the IoT*, pp. 19–24, 2014.
- [77] A. O. Kotb, Y.-c. Shen, and Y. Huang, “Smart parking guidance, monitoring and reservations: a review,” *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 2, pp. 6–16, 2017.
- [78] L.-E. Y. Mimbela, L. A. Klein, *et al.*, “Summary of vehicle detection and surveillance technologies used in intelligent transportation systems,” 2007.
- [79] F. Al-Turjman and M. Abujobbeh, “Iot-enabled smart grid via sm: An overview,” *Future generation computer systems*, vol. 96, pp. 579–590, 2019.
- [80] J. Lin, W. Yu, and X. Yang, “Towards multistep electricity prices in smart grid electricity markets,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 1, pp. 286–302, 2015.
- [81] G. Hauber-Davidson and E. Idris, “Smart water metering,” *Water*, vol. 33, no. 3, pp. 38–41, 2006.
- [82] T. Wu, J.-M. Redouté, and M. Yuce, “A wearable, low-power, real-time ecg monitor for smart t-shirt and iot healthcare applications,” in *Advances in Body Area Networks I: Post-Conference Proceedings of BodyNets 2017*, pp. 165–173, Springer, 2019.
- [83] M. Bansal and B. Gandhi, “Iot & big data in smart healthcare (ecg monitoring),” in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, pp. 390–396, IEEE, 2019.
- [84] R. S. Istepanian, S. Hu, N. Y. Philip, and A. Sungoor, “The potential of internet of m-health things “m-iot” for non-invasive glucose level sensing,” in *2011 annual international conference of the IEEE engineering in medicine and biology society*, pp. 5264–5266, IEEE, 2011.
- [85] S. Sunny and S. S. Kumar, “Optical based non invasive glucometer with iot,” in *2018 International Conference on Power, Signals, Control and Computation (EPSCICON)*, pp. 1–3, IEEE, 2018.



- [86] H. Ota, M. Chao, Y. Gao, E. Wu, L.-C. Tai, K. Chen, Y. Matsuoka, K. Iwai, H. M. Fahad, W. Gao, *et al.*, “3d printed “earable” smart devices for real-time detection of core body temperature,” *ACS sensors*, vol. 2, no. 7, pp. 990–997, 2017.
- [87] I. Gunawan, D. Andayani, T. Triwiyanto, E. Yulianto, T. Rahmawati, L. Soetjatie, and S. Musvika, “Design and development of telemedicine based heartbeat and body temperature monitoring tools,” in *IOP conference series: materials science and engineering*, vol. 850, p. 012018, IOP Publishing, 2020.
- [88] Q. Xin and J. Wu, “A novel wearable device for continuous, non-invasion blood pressure measurement,” *Computational Biology and Chemistry*, vol. 69, pp. 134–137, 2017.
- [89] B. Pradhan, S. Bhattacharyya, and K. Pal, “Iot-based applications in healthcare devices,” *Journal of healthcare engineering*, vol. 2021, pp. 1–18, 2021.
- [90] Y. Fu and J. Liu, “System design for wearable blood oxygen saturation and pulse measurement device,” *Procedia manufacturing*, vol. 3, pp. 1187–1194, 2015.
- [91] L. Agustine, I. Muljono, P. R. Angka, A. Gunadhi, D. Lestariningsih, and W. A. Weliamto, “Heart rate monitoring device for arrhythmia using pulse oximeter sensor based on android,” in *2018 International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM)*, pp. 106–111, IEEE, 2018.
- [92] J. Kaur, N. Batra, and S. Goyal, “Smartemodetect: An internet of things based emotion monitoring wearable technology for drivers,” *Journal of Computational and Theoretical Nanoscience*, vol. 16, no. 9, pp. 3969–3973, 2019.
- [93] D. Kushawaha, D. De, V. Mohindru, and A. K. Gupta, “Sentiment analysis and mood detection on an android platform using machine learning integrated with internet of things,” in *Proceedings of ICRIC 2019: Recent Innovations in Computing*, pp. 223–238, Springer, 2020.
- [94] S. A. Bharadwaj, D. Yarravarapu, S. C. K. Reddy, T. Prudhvi, K. Sandeep, and O. S. D. Reddy, “Enhancing healthcare using m-care box (monitoring non-compliance of medication),” in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 352–356, IEEE, 2017.
- [95] D. Karagiannis and K. S. Nikita, “Design and development of a 3d printed iot portable pillbox for continuous medication adherence,” in *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pp. 352–353, IEEE, 2020.
- [96] Y. K. Lee, J. M. Lim, K. S. Eu, Y. H. Goh, and Y. Tew, “Real time image processing based obstacle avoidance and navigation system for autonomous wheelchair application,” in *2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, pp. 380–385, IEEE, 2017.
- [97] D. Kumar, R. Malhotra, and S. Sharma, “Design and construction of a smart wheelchair,” *Procedia Computer Science*, vol. 172, pp. 302–307, 2020.

- [98] C. Nave and O. Postolache, “Smart walker based iot physical rehabilitation system,” in *2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI)*, pp. 1–6, IEEE, 2018.
- [99] Y. Jiang, “Combination of wearable sensors and internet of things and its application in sports rehabilitation,” *Computer Communications*, vol. 150, pp. 167–176, 2020.
- [100] M. Sundholm, J. Cheng, B. Zhou, A. Sethi, and P. Lukowicz, “Smart-mat: Recognizing and counting gym exercises with low-cost resistive pressure sensing matrix,” in *Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing*, pp. 373–382, 2014.
- [101] D. R. Seshadri, R. T. Li, J. E. Voos, J. R. Rowbottom, C. M. Alfes, C. A. Zorman, and C. K. Drummond, “Wearable sensors for monitoring the physiological and biochemical profile of the athlete,” *NPJ digital medicine*, vol. 2, no. 1, p. 72, 2019.
- [102] M. Heshmat and A.-R. S. Shehata, “A framework about using internet of things for smart cancer treatment process,” in *Proceedings of the international conference on industrial engineering and operations management*, pp. 1206–1211, 2018.
- [103] D. d. A. Rodrigues, R. F. Ivo, S. C. Satapathy, S. Wang, J. Hemanth, and P. P. Reboucas Filho, “A new approach for classification skin lesion based on transfer learning, deep learning, and iot system,” *Pattern Recognition Letters*, vol. 136, pp. 8–15, 2020.
- [104] J. P. Rajan, S. E. Rajan, R. J. Martis, and B. K. Panigrahi, “Fog computing employed computer aided cancer classification system using deep neural network in internet of things based healthcare system,” *Journal of medical systems*, vol. 44, pp. 1–10, 2020.
- [105] K. Pradhan and P. Chawla, “Medical internet of things using machine learning algorithms for lung cancer detection,” *Journal of Management Analytics*, vol. 7, no. 4, pp. 591–623, 2020.
- [106] Z. Liu, C. Yao, H. Yu, and T. Wu, “Deep reinforcement learning with its application for lung cancer detection in medical internet of things,” *Future Generation Computer Systems*, vol. 97, pp. 1–9, 2019.
- [107] J. Cecil, A. Gupta, M. Pirela-Cruz, and P. Ramanathan, “An iomt based cyber training framework for orthopedic surgery using next generation internet technologies,” *Informatics in Medicine Unlocked*, vol. 12, pp. 128–137, 2018.
- [108] H. Su, S. E. Ovrur, Z. Li, Y. Hu, J. Li, A. Knoll, G. Ferrigno, and E. De Momi, “Internet of things (iot)-based collaborative control of a redundant manipulator for teleoperated minimally invasive surgeries,” in *2020 IEEE international conference on robotics and automation (ICRA)*, pp. 9737–9742, IEEE, 2020.
- [109] K. Bhatia and M. Singh, “Towards development of portable instantaneous smart optical device for hemoglobin detection non invasively,” *Health and Technology*, vol. 9, no. 1, pp. 17–23, 2019.

- [110] S. T. U. Shah, F. Badshah, F. Dad, N. Amin, and M. A. Jan, “Cloud-assisted iot-based smart respiratory monitoring system for asthma patients,” *Applications of intelligent technologies in healthcare*, pp. 77–86, 2019.
- [111] C. Yuanyuan and Z. Zuozhuang, “Research and design of intelligent water-saving irrigation control system based on wsn,” in *2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, pp. 695–697, IEEE, 2020.
- [112] Z. Li, J. Wang, R. Higgs, L. Zhou, and W. Yuan, “Design of an intelligent management system for agricultural greenhouses based on the internet of things,” in *2017 IEEE international conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC)*, vol. 2, pp. 154–160, IEEE, 2017.
- [113] X. Chen, “Study on growth condition monitoring and management techniques of millet field based on internet of things,” *Shanxi Agricultural University*, 2015.
- [114] F.-T. Lin, Y.-C. Kuo, J.-C. Hsieh, H.-Y. Tsai, Y.-T. Liao, and H.-C. Lee, “A self-powering wireless environment monitoring system using soil energy,” *IEEE Sensors Journal*, vol. 15, no. 7, pp. 3751–3758, 2015.
- [115] Q. Xie, M. Wu, J. Bao, P. Zheng, W. Liu, X. Liu, and H. Yu, “A deep learning-based detection method for pig body temperature using infrared thermography,” *Computers and Electronics in Agriculture*, vol. 213, p. 108200, 2023.
- [116] S. Porto, C. Arcidiacono, and G. Cascone, “Developing integrated computer-based information systems for certified plant traceability: Case study of italian citrus-plant nursery chain,” *Biosystems Engineering*, vol. 109, no. 2, pp. 120–129, 2011.
- [117] K. D. Sowjanya, R. Sindhu, M. Parijatham, K. Srikanth, and P. Bhargav, “Multipurpose autonomous agricultural robot,” in *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*, vol. 2, pp. 696–699, IEEE, 2017.
- [118] Y. Onishi, T. Yoshida, H. Kurita, T. Fukao, H. Arihara, and A. Iwai, “An automated fruit harvesting robot by using deep learning,” *Robomech Journal*, vol. 6, no. 1, pp. 1–8, 2019.
- [119] L. Jiang and K. Sun, “Research on security traceability platform of agricultural products based on internet of things,” in *2017 7th International Conference on Mechatronics, Computer and Education Informationization (MCEI 2017)*, pp. 146–150, Atlantis Press, 2017.
- [120] H. Gu, X. Zhang, X. Qin, *et al.*, “Construction of pork trace ability system,” *Heilongjiang Agric Sci*, vol. 2018, no. 05, pp. 46–49, 2018.
- [121] N. Materne and M. Inoue, “Iot monitoring system for early detection of agricultural pests and diseases,” in *2018 12th South East Asian Technical University Consortium (SEATUC)*, vol. 1, pp. 1–5, IEEE, 2018.

- [122] G. Nagasubramanian, R. K. Sakthivel, R. Patan, M. Sankayya, M. Daneshmand, and A. H. Gandomi, “Ensemble classification and iot-based pattern recognition for crop disease monitoring system,” *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12847–12854, 2021.
- [123] Y. Ma and X. Sun, “Intelligent agricultural machinery equipment and technology,” *Agri cultural Equipment & Technology*, vol. 46, no. 01, pp. 4–6, 2020.
- [124] D.-M. Han and J.-H. Lim, “Design and implementation of smart home energy management systems based on zigbee,” *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 1417–1425, 2010.
- [125] Y. Qu, X. Ming, Z. Liu, X. Zhang, and Z. Hou, “Smart manufacturing systems: state of the art and future trends,” *The International Journal of Advanced Manufacturing Technology*, vol. 103, pp. 3751–3768, 2019.
- [126] Y. Lu, K. C. Morris, S. Frechette, *et al.*, “Current standards landscape for smart manufacturing systems,” *National Institute of Standards and Technology, NISTIR*, vol. 8107, no. 3, 2016.
- [127] O. Alsaadoun, “A cybersecurity prospective on industry 4.0: Enabler role of identity and access management,” in *International Petroleum Technology Conference*, p. D031S058R001, IPTC, 2019.
- [128] S.-H. Liao and L.-L. Yang, “Mobile payment and online to offline retail business models,” *Journal of Retailing and Consumer Services*, vol. 57, p. 102230, 2020.
- [129] L. Liu, B. Zhou, Z. Zou, S.-C. Yeh, and L. Zheng, “A smart unstaffed retail shop based on artificial intelligence and iot,” in *2018 IEEE 23rd International workshop on computer aided modeling and design of communication links and networks (CAMAD)*, pp. 1–4, IEEE, 2018.
- [130] A. Jayaram, “Smart retail 4.0 iot consumer retailer model for retail intelligence and strategic marketing of in-store products,” *Proceedings of the 17th international business horizon-INBUSH ERA-2017, Noida, India*, vol. 9, 2017.
- [131] S. Munirathinam, “Industry 4.0: Industrial internet of things (iiot),” in *Advances in computers*, vol. 117, pp. 129–164, Elsevier, 2020.
- [132] C. Zhou, N. Damiano, B. Whisner, and M. Reyes, “Industrial internet of things:(iiot) applications in underground coal mines,” *Mining engineering*, vol. 69, no. 12, p. 50, 2017.
- [133] M. Javaid, A. Haleem, R. P. Singh, S. Rab, and R. Suman, “Upgrading the manufacturing sector via applications of industrial internet of things (iiot),” *Sensors International*, vol. 2, p. 100129, 2021.

- [134] G. Liang, J. Cao, and W. Zhu, "Circlesense: A pervasive computing system for recognizing social activities," in *2013 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 201–206, IEEE, 2013.
- [135] Y.-K. Row and T.-J. Nam, "Camy: applying a pet dog analogy to everyday ubicomp products," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp. 63–74, 2014.
- [136] M. Yu, A. Rhuma, S. M. Naqvi, L. Wang, and J. Chambers, "A posture recognition-based fall detection system for monitoring an elderly person in a smart home environment," *IEEE transactions on information technology in biomedicine*, vol. 16, no. 6, pp. 1274–1286, 2012.
- [137] D. Saravanan, G. Archana, and R. Parthiban, "Voice controlled humanoid robotic car for smart agriculture using arduino and android smart watch," *Int. J. Pure Appl. Math.*, vol. 119, no. 14, pp. 829–832, 2018.
- [138] M. Chen, J. Zhou, G. Tao, J. Yang, and L. Hu, "Wearable affective robot," *IEEE Access*, vol. 6, pp. 64766–64776, 2018.
- [139] W. Kassab and K. A. Darabkh, "A–z survey of internet of things: Architectures, protocols, applications, recent advances, future directions and recommendations," *Journal of Network and Computer Applications*, vol. 163, p. 102663, 2020.
- [140] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE internet of things journal*, vol. 4, no. 5, pp. 1125–1142, 2017.
- [141] S. Das, M. P. Singh, and S. Namasudra, "A lightweight authentication and key agreement protocol for iot-based smart healthcare system," in *2023 World Conference on Communication & Computing (WCONF)*, pp. 1–5, IEEE, 2023.
- [142] A. Singh, A. Kumar, and S. Namasudra, "Dnacds: Cloud ioe big data security and accessing scheme based on dna cryptography," *Frontiers of Computer Science*, vol. 18, no. 1, p. 181801, 2024.
- [143] S. Namasudra, D. Devi, S. Choudhary, R. Patan, and S. Kallam, "Security, privacy, trust, and anonymity," *Advances of DNA computing in cryptography*, vol. 1, pp. 138–150, 2018.
- [144] S. Das and S. Namasudra, "A novel hybrid encryption method to secure healthcare data in iot-enabled healthcare infrastructure," *Computers and Electrical Engineering*, vol. 101, p. 107991, 2022.
- [145] S. Das and S. Namasudra, "Macpabe: Multi-authority-based cp-abe with efficient attribute revocation for iot-enabled healthcare infrastructure," *International Journal of Network Management*, vol. 33, no. 3, p. e2200, 2023.

- [146] A. H. Hussein, “Internet of things (iot): Research challenges and future applications,” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 6, 2019.
- [147] S. G. Tzafestas, “Ethics and law in the internet of things world,” *Smart cities*, vol. 1, no. 1, pp. 98–120, 2018.
- [148] X. Carron, R. Bosua, S. Maynard, and A. Ahmad, “The internet of things and its impact on individual privacy: an australian privacy principle perspective,” *Computer Law & Security Review*, vol. 21, no. 1, pp. 4–15, 2016.