Discover Internet of Things

Review

Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions

Anita Choudhary[1]

Received: 1 June 2024 / Accepted: 19 November 2024
Published online: 19 December 2024
© The Author(s) 2024 OPEN

Abstract
In recent years, Internet of Things (IoT) evolved as a new paradigm and gained a lot of traction in the wireless telecommunications industry. It changed the traditional way of living into a high-tech lifestyle through the integration of intelligent devices, applications, and technologies that automate everything around us. The IoT is anticipated to connect physical objects to facilitate intelligent decision making in the future years. Several studies have been conducted to improve IoT technology. To fully realize the potential of IoT, numerous problems and issues remain to be addressed. IoT challenges and issues must be addressed from multiple perspectives, including applications, supporting technology, and social and environmental implications. This review paper aims to provide a full discussion from both technological and social perspectives. The paper highlights several challenges and critical aspects in IoT, architecture, and its application fields. A generic architecture of IoT is proposed with its enabling technologies to highlight the uses of each layer and technologies that implemented in it. Market opportunities are a highlight that helps to understand the growth of IoT. Further, the functional blocks and working of IoT is discussed, so the researchers take interest in its implementation. Also, a detailed discussion on IoT fields and it's uncovered challenges are highlighted. A brief overview of existing simulators and their functionalities is discussed, so that researchers can easily select the simulator as per their targeted objectives. In addition, major issues are highlighted that should be addressed by the scientific community. Finally, the significance of this research is to understand fundamentals of IoT architecture as well as a complete review in order to delve deeper into the difficulties and devise appropriate solutions.

Keywords Internet of Things (IoT) · IoT architecture · IoT applications · IoT simulation tools

1 Introduction

To make our lives easier, a new paradigm called the Internet of Things (IoT) allows connections between electrical devices and sensors to be made over the internet. IoT uses internet-connected smart devices to provide innovative global solutions to a range of business, governmental, and public/private industry-related issues. Wireless sensor network (WSN) technology-enabled ubiquitous sensing affects many aspects of day to days life by offering the ability to sense, infer, and understand environmental indicators, from ecological systems and natural resources to urban environments. IoT is a network of sensors, actuators, Radio Frequency IDentifications (RFIDs), software, storage, and links to gather data and analyze it in order to monitor and control the targeted environment. IoT is involved in every aspect of our daily lives and is quickly growing in all most all the fields. It seems as an innovation that unites a vast array of diverse intelligent device types, frameworks, and systems together for monitoring and controlling the environment. Furthermore, it leverages

✉ Anita Choudhary, anitach312@gmail.com | [1]Computer Science, Sri Karan Narendra Agriculture University, Jaipur, Rajasthan, India.

quantum and nanotechnology to achieve great improvements in processing speed, sensing, and storage capacity to the devices. To demonstrate the possible effectiveness and applicability of IoT transformations, extensive research has been done and it is still in continuity due to its increasing demand.

IoT is one of the important area for both academia and industry since it was proposed by K. Ashton in 1999 [1] in the context of supply chain management. Since IoT is a paradigm that aims to involve everything in the world, including social media, smart cities, health, transportation, health care, smart environments, agriculture, etc., it can never be an isolated field. Current Internet technology is constantly evolving into a network of interconnected objects with a variety of goals, including data collection from the target environment (sensing), interaction with the physical world (actuation/command/control), and use of existing Internet standards to provide services for data transfer, analytic, applications, and communications. Due to the involvement of people, computers, and smart objects all of which are omnipresent interconnected the potential of the IoT has yet to be fully realized. However, it can be expanded in a number of ways, one of which is involvement with already-existing network systems, such as Internet, smartphones, social networks, and industrial networks, cloud computing. A recent report [2], indicates that the global IoT connections increased by 18% in 2022, reaching a total of 14.3 billion active IoT endpoints. Projections suggest that by 2025, the number of connected IoT devices could rise to 27 billion. IoT devices that are used for sensing, acting, and monitoring are linked to the Internet using communication technologies like Wi-Fi, BLE, ZigBee, NFC, etc. These devices produce enormous amounts of data, which must be stored, processed, and served to users but IoT by itself is unable to process, store, or analyses enormous amounts of data gathered from trillions of sensors. Therefore, it requires storage and compute resources. This shortcoming is precisely the benefit of cloud computing, whose capacity for calculation and storage can be viewed as endless, making the integration of the IoT with the cloud advantageous for both parties.

Cloud computing has been conceived as an umbrella to delineate a grouping of complex on-ask computing service. The example of cloud service providers are Google App Engine [3], Amazon EC2 [4], Microsoft Azure [5], IBM Smart Cloud [6] etc. In a cloud, a user is facilitated to access its services from anywhere, anytime in the world and have to pay only for the accessed services that are based on the "pay-asyou-go" financial model [7]. Cloud computing technology seems to be a new era of computing in which resources are provided on-demand. This new era of computing shifts the location of hardware and software resources from local premises to the network that will reduce the management cost of the resources. The resource purchasing, provisioning, software development, and deployment is tedious job and because of that the application providers start uses of cloud data centers. It offers mainly three type of services: software, computing, and storage "as a service". It is simple for IoT applications to operate freely, to adapt and react intelligently to various scenarios, and to support for simple integration when using a cloud computing environment. The aforementioned issues persist due to the significant diversity and resource limitations of the participating devices.

Further, IoT is considered the fourth industrial revolution due to its extensive range of services worldwide, spanning from smart homes to AI-powered autonomous vehicles, Internet-connected medical devices, and more. This revolution has facilitated unprecedented levels of connectivity and speed among devices, creating an intelligent ecosystem [8]. The diverse applications of IoT come with unique requirements and constraints, resulting in a high degree of heterogeneity. Various studies, industries, and businesses are actively exploring different IoT capabilities to address the evolving technological landscape and meet the rising demands. Consequently, multiple protocols have been devised to cater to different needs, with each vendor striving to establish dominance in the market for their proposed devices and protocols. The original concept of IoT consisted of a three-layer structure, with sensors and actuators forming the foundational layer, and cloud computing serving as the top layer. Manufacturers face constant pressure to deliver their services quickly to meet market demands, necessitating rapid development to keep up with increasing requirements while addressing security concerns. These technologies are now integrated into various aspects of modern life, including residential spaces, critical infrastructure such as healthcare, transportation, and industrial sectors. Also, independent IoT devices find it challenging to implement power and bandwidth conservation due to the continuously growing number of devices connected in the IoT environment and also focus on exploring communication protocols for potential enhancements.

Various articles present comparative methodologies and examine different facets of the IoT, encompassing its diverse architectures and techniques. Recent research indicates a strong interest in the IoT and its related topics among scholars in academic and industries [9]. Recent publications in this field have been categorized into eight distinct groups: IoT applications, security, technologies, data, communication, communication networking, protocol standards, and development. Several potential applications utilizing IoT technology were explored in [10], shedding light on the diverse possibilities enabled by IoT innovations. Security is another significant challenge, with the potential to leverage sensor data to safeguard against intrusions or attacks on the sensors themselves. Additionally, various security concerns have been explored, alongside a brief exploration of potential IoT applications and their impacts across different domains.

The issue of bandwidth emerges as a critical concern, particularly as the number of sensor nodes grows, necessitating efficient resource utilization within constraints. An examination of IoT architectures and techniques is outlined in a comprehensive model in [11], emphasizing essential concepts and critical advancements in relevant studies and technological landscapes. Various IoT platform designs were assessed, leading to the development of a generic IoT standard paradigm in reference [12]. Another comprehensive overview of technologies was presented in [13], which delved into potential conceptual models, communication technologies, challenges, and unanswered questions. Furthermore, a novel six-layer design was introduced to safeguard the IoT infrastructure. The analysis of each protocol's specifications in [14] resulted in a comprehensive survey of application layer protocols, highlighting their distinct characteristics. The findings assessed how effectively each protocol catered to specific categories of applications and their corresponding communication requirements. Another study [15], provided a review of the fundamental aspects of the IoT ecosystem and communication protocols, primarily developed for IoT technology. Lastly, [16] offered an overview of current IoT models, techniques, and critical open-source platforms and applications.

In our work, we address the limitations of existing surveys [10–15, 17] and present comprehensive survey on state-of-the-art IoT technologies. Unlike other studies that only looked at one area, this survey provides a detail study about layered architecture of IoT, market opportunities, its applications, challenges, etc. Our major contributions in this paper can be summarized as follows:

- Comprehensive literature review of state-of-the-art solutions with respect to various aspects of IoT like automation system, environmental, security, data-centric IoT applications, and quality of services.
- Discussion on key aspects of IoT and its architectures. Proposed a novel architecture that represent the protocols used for its implementation.
- Discussion on various market opportunities of IoT are highlighted.
- Functional block of IoT devices and its working model is discussed in detail to highlight the uses of protocols.
- IoT fields such as industry automation, energy conservation, transportation, city, healthcare, supply chain, agriculture, traffic monitoring are discussed in detailed, in order to focus the challenges faces due to their growing demands.
- Brief overview about existing simulators and tools.
- Identification of specific gaps and research challenges to improve the performance of IoT systems.
- Highlight the future directions that needs to be considered by academia and industry.

The paper is organized as follows: "State-of-the-art" section, we have discussed the existing approaches and technologies that are evolved the IoT and highlight the existing issues that attracts the researchers attention. In "Background of IoT" section presents the background of IoT, its existing architectures (3-Layer, 5-Layer, 7-Layer) and vision of IoT. In "Market Opportunity" section, the demand of IoT in various fields is discussed. In next section "functional blocks of IoT" we have discussed components of IoT system, working model and technologies involved in working and implementation of IoT. In "IoT services and applications" sections, the involvement of IoT in the field of industry, energy, transportation, city, healthcare, supply chain, agriculture, and traffic monitoring discussed in detailed. In "IoT Simulators and Tools" sections, we have presented the brief introduction of existing tools that are used to focus on various fields of IoT like network connection (wired or wireless), device control, data management, measurement of performance metrics, etc. Specific research gaps and open challenges in IoT are described in "Research challenges" section. Then, in "Future direction" section, the existing gaps are highlighted that demands further research that improves the performance of IoT and able to deploy them on various fields for smooth working. Finally, "Conclusion" section, concludes the paper with key highlights.

2 State-of-the-art

The next phase of computing evolution can be seen as "Internet of Things" and take advantage of passes of evolution in computing starting from: Desktop → Distributed computing → Cluster computing → Grid Computing → Utility Computing → Cloud Computing → Fog and Edge Computing → Internet of Things.

Under the IoT paradigm, a large number of objects are kept in environment for monitoring and controlling purpose. These objects are connected by small range of frequency. RFIDs and sensor technologies are used to make connections between devices and send the data in the form of signal to the connected servers. The IoT devices continues sense the environment and generate huge amount of data, which needs to be handled, stored, and analyzed. The continuous

increase in the volume of generated information, coupled with the inability of traditional databases to manage various types of structured and unstructured data, presents significant challenges. Data gathered from diverse devices is being analyzed for various purposes to derive meaningful insights that inform critical decision-making. In order to take benefit of collected data for smart decision making, big data analytics is used because it examines and analyzes large and complex data sets. Big data involves the processing of large amounts of data to address specific queries and uncover trends or patterns. Mathematical algorithms are utilized to analyze the data, with the choice of algorithm depending on the nature of the data, the number of sources involved, and the objectives of the analysis. The challenge with big data lies in the substantial computing and networking infrastructure required to establish a big data facility. To address this issue, cloud computing is employed. Currently, many industries require robust cloud-based infrastructure as more operations are transitioning to the cloud due to its various advantages such as pay-per-use services, scalability, and accessibility.

In some applications (like traffic monitoring, transportation, healthcare, etc.) data generated from thousands of sensors, needs to be stored and analyed near to the application fields because of the quick decision making and low latency. In case of cloud computing the latency is high because data is stored and analzed at different geographical locations, so in order to take quick decisions fog computing is used. Fog Computing integrates the computational capabilities of smart devices located in proximity to the end user in order to support networking, processing, and storage at the edge. The primary objective of fog computing in conjunction with the IoT is to minimize the amount of data that needs to be transferred to cloud servers for tasks such as storage, analysis, and processing, thereby enhancing efficiency and performance. Consequently, data collected by sensor devices is sent to edge devices for temporary storage and processing instead of being directly transmitted to the cloud, resulting in reduced latency and network congestion. Still IoT uses the cloud computing for storage and analysis because in some applications like industry, agriculture, etc. the impact of past data play an important role in decision making. Further, intelligent connectivity with current networks and context-aware computing that makes use of network resources is main target of IoT. It is evident that 4G-LTE and wireless Internet connectivity are headed toward becoming the de-facto standard for networks uses for information and communication systems. If the IoT is to become a reality, the computing paradigm will have to evolve beyond traditional mobile computing scenarios that use smartphones and portables to connect all the objects and embed intelligence into our surroundings. For technology to disappear from a user's consciousness, the IoT needs that:

- a common understanding of the conditions encompassing its users and their appliances;
- pervasive communication networks and software architectures to process and deliver contextual information where it matters;
- IoT analytical tools that aim for intelligent and autonomous behavior.

Achieving smart connection and context-aware computing requires adherence to these three fundamental principles.

In a communicating-actuating network, where sensors and actuators seamlessly integrate with our surroundings and information is shared across platforms to create a common operational picture (COP), the proliferation of IoT devices gives rise to the IoT network. The IoT is poised to become the next big thing in technology and it becomes possible because of the adoption of various wireless technologies and its full potential. IoT is about to emerge from its early stages and transform the current static Internet into a Future Internet that is fully integrated [18]. Wireless technologies such as Bluetooth, Wi-Fi, RFID, and telephonic data services are examples of those that are supported.

In this section, we present an categorized review of existing approaches with respect to their applications. This review helps to understand how the IoT is involved in different areas and what are the critical factors which needs to be sensed and controlled. The critical factors of IoT are automation system, environmental, security & privacy, data-centric IoT applications, interoperability, and Quality of Services (QoS). All these factors are highlighted and reviewed below.

2.1 Automation system

Smart houses are well-known IoT application area for smart cities. To maximize comfort, security, and efficiency, a smart home's IoT-enabled appliances, air conditioning and heating system, television, audio and video streaming devices, and security systems all communicate with one another. Communication is done through a central control system that is web-based. Over the past ten years, the concept of a "smart city" has grown in popularity [19]. By 2022, the smart home industry is expected to generate over $100 billion in revenue [20]. Less energy usage will result in a relatively reduced electricity bill, thus a smart home not only offer comfort inside but also helps the homeowner cost cutting in other areas. In addition to smart homes, smart cities also include smart automobiles. Most of the components of modern cars,

including the engine and the headlights, are controlled by actuators and sensors [21]. IoT is dedicated for creating a new generation of smart automotive systems that include wireless connection between cars their drivers to enable predictive maintenance and comfortable & safe driving experience [22].

The problem of urbanization in cities was discussed by Alavi et al. [23]. Growing urban populations are a result of the migration of people from rural to urban environments. Smart solutions must therefore be offered for infrastructure, energy, healthcare, and mobility. For IoT developers, the smart city is one of the key application domains. It examines a number of challenges, including waste collection, parking, lighting, and management of the environment and air quality. IoT is continuously making a lot of effort to address such difficult problems. The expanding urbanization and the demand for better smart city infrastructure have made the market for smart city technology more accessible to entrepreneurs. The development of sustainable smart cities, according to the authors, depends heavily on IoT enabled technologies.

2.2 Environmental

Khajenasiri et al. [20] carried out a survey of IoT solutions for smart energy control to support applications for smart cities. They asserted that IoT is currently used in a small number of application areas to benefit both people and technology. The IoT has a very wide scope and has the potential to capture almost all application areas in the near future. Energy preservation is one of the important concern and IoT could contribute to the development of an intelligent energy management system that would save energy and money. The authors highlighted that the insufficient advancement in IoT hardware and software presents significant challenges in achieving this objective. They suggested that addressing these issues is essential to ensure the creation of an effective, reliable, and user-friendly IoT system.

Climate change driven by global warming poses a significant threat to public health worldwide. To establish an efficient system for environmental monitoring and management, Fang et al. [24]. developed an integrated information system (IIS) that merges the Internet of Things (IoT), geo-informatics, cloud computing, the Global Positioning System (GPS), geographical information systems (GIS), and e-science. Authors claimed that for climate control, the recommended IIS provides superior data collection, analysis, and smart decision-making is necessary for controlling the air pollution because it is major global issue again. To address air pollution issue, numerous tools and techniques have been proposed to monitor and control air quality. Cheng et al. proposed AirCloud, a cloud-based air quality and monitoring system [25].

2.3 Security and privacy

A significant concern in the domain of IoT that requires careful attention and thorough research in security and privacy. Weber [26] examined these critical issues and suggests that private organizations utilizing IoT should integrate data authentication, access control, attack resilience, and client privacy into their operational frameworks. To effectively address global security and privacy challenges, IoT developers must consider the geographical constraints present in different countries. A universal framework needs to be developed to satisfy the privacy and security needs of everyone. Prior to building an IoT framework that is fully operational, it is highly recommended that privacy and security issues be thoroughly investigated and identified with respect to applied field.

Heer et al. [27] discovered a security vulnerability in IP-based IoT systems. The internet plays a major role in the inter-device communication of the IoT. This makes security issues a big problem for IP-based IoT systems. When creating the security architecture, it is also important to consider the capabilities and life cycle of each IoT system object. Using security standards and a reliable third party are also included. If the security architecture could expand to support both smalland large-scale IoT devices, that would be ideal. According to the study, standard end-to-end internet protocols are unable to handle this communication since the IoT has created a new way for objects to communicate across networks. New protocols must be developed that take into consideration the translations at the gateways in order to achieve end-to-end security. Furthermore, every communication layer has unique security requirements and concerns. Because satisfying the requirements for just one layer will leave the system vulnerable, security needs to be ensured for all layers.

Authentication and access management is another IoT issue that needs promising solutions to improve security. Liu et al. offered a method for handling access control and authentication [28]. Authentication is essential to verify the communicating parties and prevent the loss of confidential information. The authors demonstrated an authentication method based on the Elliptic Curve Cryptosystem and evaluated its resistance to various security risks, such as replay attacks, eavesdropping, key control, and man-in-the-middle attacks. They claimed that their systems could enhance access control and authentication for IoT communication. Later, Kothmayr et al. [29]. introduced a datagram transport layer security (DTLS)-based two-way authentication technique for the IoT. Online thieves are constantly taking advantage

of the protected data. In addition to memory overhead and end-to-end latency, the proposed method can provide message security, integrity, authenticity, and confidentiality in the IoT-based communication network.

According to Luk et al. [30], a secure sensor network's (SSN) primary functions include authentication, data privacy, and defense against replay attacks. Authors discussed about ZigBee [31] and TinySec [32], two well-known SSN services. Although both SSN services are effective and dependable, they noted that TinySec uses less energy but is less secure than ZigBee in comparison, and that both SSN services are efficient and dependable. On the Telos platform, they proved the performance of another architecture, MiniSec, that supports great security and little energy use. IoT trust management is a crucial problem, according to Yan et al. [33]. According to Bao et al. (2013), trust management enables consumers to comprehend and have confidence in IoT services and applications without concern for uncertainty-related problems and hazards. Authors looked into various trust management problems and talked about why it's crucial for IoT consumers and developers.

Hasan et al. [34] provides a comprehensive review of protocols designed to ensure secure communication in IoT applications. The two main focus areas are key agreement and authentication crucial mechanisms for protecting IoT devices from unauthorized access and ensuring secure data exchange. Key agreement protocols allow IoT devices to establish a shared cryptographic key, ensuring that communication between them is encrypted. Authentication protocols verify the identity of devices to prevent unauthorized entities from gaining access to the network. The survey explores various existing protocols, such as public-key cryptography, symmetric key approaches, and lightweight protocols tailored to IoT's limited resource environments. The challenges in applying traditional security protocols to IoT, such as the need for lightweight and energy-efficient solutions due to the limited processing power and battery life of IoT devices. Finally, it reviews emerging techniques like blockchain-based authentication, post-quantum cryptography, and edge computing to enhance security in future IoT applications.

2.4 Data-centric IoT applications

For data-centric IoT applications with regard to cloud platforms, Li et al. [35] presented a dynamic strategy. The necessity for an adequate device, software configuration, and infrastructure require effective solutions in order to support large number of IoT applications that are running on cloud platforms. In order to develop solutions, IoT developers and academics are actively taking into account the diverse nature of IoT objects and devices. An architecture based on software defined networking (SDN) that functions well even in the absence of a clearly specified design was described by Olivier et al. [36]. Authors suggested that an SDN-based security architecture is more adaptable and effective for IoT.

2.5 Interoperability

According to Noura et al. [37], interoperability in the IoT is critical issue because it enables the integration of devices and services from various heterogeneous platforms to deliver efficient and dependable services. Several studies have underlined the difficulties that IoT interoperability faces and have emphasised the significance of interoperability [38–40]. An IoT-based ecological monitoring system was suggested by Kim et al. [41] to address the issue of climate change. The time-consuming and heavily labor-intensive nature of current methods was emphasized. The information from the sensors deployed at the investigation site must also be collected during a routine visit. Moreover, certain material was left out, which made the analysis less accurate. IoTbased frameworks can therefore address this issue and offer highly accurate analysis and prediction. For home waste water treatment is later demonstrated by Wang et al. [42]. Authors reviewed several problems with the dynamic monitoring system and waste water treatment process and offered workable IoT-based solutions. Therefore, IoT can be useful for process monitoring and waste water treatment.

2.6 Application-oriented

One of the key sectors around the world is agriculture. Many variables, including geographic and biological ones, affect agriculture. According to Qiu et al. [43], the technology being utilized to govern ecosystems is not fully trained and has low level of intelligence. Authors pointed that IoT researchers and developers would find this to be a useful application area. In order to manage the agriculture ecosystem, Qiu et al. [43], suggested a four-layer intelligent monitoring platform structure. The framework can provide a better ecosystem with less human intervention because each layer is in charge of a specific task.

KumarKasera et al. [44] examines the use of IoT and AI technologies in agriculture to improve efficiency, productivity, and sustainability at all phases of production. The survey divides applications into three stages: before harvest, during harvest, and after harvest. During the pre-harvest phase, IoT sensors and AI are used to monitor soil conditions, weather patterns, and crop health, allowing for precision farming and real-time decision-making to optimize water usage, fertilization, and pest management. During harvest, IoT-enabled technology and AI-powered automation increase harvesting efficiency by optimizing timing and resource management, lowering labor costs, and eliminating waste. In the post-harvest phase, IoT and AI play critical roles in storage, transportation, and supply chain management. These technologies enable to monitor storage conditions, track produce quality, and forecast market demand, resulting in less spoilage and more efficient distribution. The poll focuses on how IoT and AI contribute to more sustainable agriculture practices by improving resource management, reducing waste, and increasing production, which benefits both farmers and consumers.

Subashini et al. [45] presents a thorough examination of the use of IoT technologies in the healthcare industry. It investigates how IoT devices might improve patient monitoring, diagnosis, and treatment, hence enhancing overall healthcare delivery. The poll focuses on essential IoT technologies including as wearable devices, smart sensors, and telehealth platforms, which enable real-time data collecting and analysis to improve patient outcomes. The IoT has numerous uses in healthcare, including remote patient monitoring and chronic disease management, as well as smart hospital surroundings and better medical imaging. These technologies enable healthcare facilities to improve patient involvement, provide individualized treatment, and manage resources more efficiently. However, the poll also addresses important barriers to IoT integration in healthcare, such as data privacy and security concerns, interoperability issues between various devices and platforms, and the necessity for dependable communication networks. Furthermore, the paper underlines the significance of resolving regulatory compliance and providing user-friendly interfaces in order to encourage widespread use. Overall, the poll emphasizes the transformative potential of IoT in healthcare, as well as the need for effective solutions to address existing difficulties.

2.7 Quality of services (QoS)

Considering QoS as a major difficulty and a complex task in the evaluation and selection of IoT devices, protocols, and services was something that Temglit et al. [46] did. QoS is a very critical criterion to have in order to attract people and acquire their trust in IoT devices and services. They devised a novel method for the selection of distributed QoS that works quite well. The distributed constraint optimization issue and the multi-agent paradigm provide the foundation for this method. In addition, the methodology was assessed by conducting a number of experiments in distributed settings that were as realistic as possible. The applicability of the IoT to environmental and agricultural regulations is another essential facet of this technology. Talavera et al. [47] addressed the essential efforts of IoT for agro-industrial and environmental elements in a survey research that concentrated on this approach. They noted that it is obvious that attempts are being made to implement IoT in these sectors. The IoT is helping to advance existing technologies, which is to the advantage of both society and farmers. Jara et al. [48] emphasized the significance of IoT-based patient monitoring. Authors hypothesized that IoT devices and sensors, along with the assistance of the internet, could be useful in patient health monitoring. In addition to this, authors suggested a structure and a procedure that could help them accomplish their goal. Still, the protocols are developing and needs for revision in available technologies for performance improvement and availability of techniques in other demanding fields.

2.8 Energy

Energy efficiency represents a crucial field of study focused on developing sustainable and eco-friendly networks. As data traffic increases and network congestion becomes more prevalent, IoT devices, which often have restricted computational abilities and energy supplies, encounter difficulties in data analysis, processing, and storage. To mitigate these challenges, advancements in computing technology have proven to be a viable solution for enhancing energy conservation in IoT devices by offering robust computing power and efficient storage solutions to facilitate data collection and processing. Consequently, energy-efficient computing, commonly referred to as"green computing," has emerged as a primary area of interest for researchers aiming to implement extensive IoT networks. Alsharif et al. [49]. presents a comprehensive assessment of approaches and technology for lowering energy consumption in large-scale IoT implementations. It solves important difficulties to energy efficiency in IoT, such as device battery life, communication overhead, and processing restrictions. The survey emphasizes low-power hardware design, energy-efficient communication protocols (e.g., LPWAN, LoRa), and edge computing for optimizing energy utilization. It also covers energy harvesting techniques like solar and

thermal, as well as power management strategies like dynamic scheduling and sleep modes. The goal is to develop scalable IoT systems that reduce energy consumption while maintaining performance, hence ensuring the long-term viability of vast IoT networks.

3 Background of IoT

A brief history of the IoT components is provided in this section because the IoT spans a wide range of concepts.

3.1 What is IoT?

IoT's core tenet is the equipping of the physical things in our environment with sensors that allow them to detect their environment, communicate seamlessly, and provide contextual services. IoT is a network of networked objects that can gather and share data because they are embedded with sensors, software, network connectivity, and embedded devices. Applications like home automation, smart health monitoring, security, automated device monitoring, and job management are all made possible by the IoT. With this new paradigm, every industry will profit, including those in the fields of energy, computing, management, security, and transportation. There are number of definition accepted for the term "IoT", as definitions are presented from a variety of perspectives. The ensuing definitions originate from multiple scholars:

- Definition I: There are two terms in this expression: Things refers to all devices interconnected to a network relying on identical protocols, whereas the Internet is described as the global network of many networks [8].
- Definition II: The IoT concept is any device that is always available to be accessed by anyone, at any moment, from any location, via any application, and over any network [50].
- Definition III: The Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data [51].

According to the IoT vision, "things" can be categorized into three categories: humans, machines (sensors, actuators, etc.), and informational items (clothing, food, medicine, books, etc.) [52]. For the purpose of being able to address, communicate with, and verify each other's identities, these should be identified by at least one distinctive method of identification. In the IoT, the recognizable "things" are called "objects". The key attribute of IoT objects are [53]: (a) the capacity to scenes or actuate; (b) small in size; (c) limited capabilities; (d) small battery; (e) easy to deploy on field; (f) connectivity; (g) mobility; and (h) management by devices rather than people.

IoT makes it possible for physical objects to see, hear, think, and carry out activities by allowing them to communicate with one another, share information, and plan out actions [38]. It is now feasible to materialize the IoT and make it accessible from anywhere at any time over any network by means of the development of sensors, actuators, smart phones, and RFID tags. Objects can provide context and real-time environmental data through wireless sensor technologies. IoT makes it possible for objects to become more intelligent and to communicate with one another. Objects vary in size from tiny to large. It can be difficult to continuously connect moving objects to a power source. They therefore need a self-sustaining energy source in order to operate. As a result, IoT demands energy-efficient communication systems.

3.2 IoT architecture

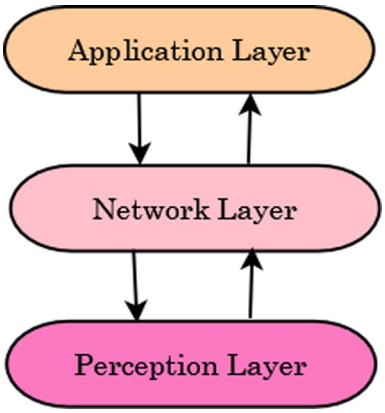
IoT protocol stack can be seen as an extension of TCP/IP protocol model. In this continuity some of the IoT architecture stack was proposed with different layers and features. In this section, some of the proposed IoT architecture with three layers, five layer, seven layer are discussed and presented [54–56].

3.2.1 The 3-layer architecture

When the IoT first began, it implemented with 3-layer architecture as shown in Fig. 1.

The 3-layer architecture contains: perception layer, network layer, and application layer. Description of all three layers are as follows:

Fig. 1 IoT 3-Layer Architecture



- Perception Layer: In the context of the IoT, the physical layer is also referred to as the "perception layer"or the "recognition layer". Each object in the IoT system is identified by the perception layer. This is accomplished by compiling data on each object. Sensing the physical properties of the objects in the environment is the physical layer's main purpose. This layer relies on various sensing technologies, such as RFID chips, barcodes, WSN, Global Positioning System (GPS) and other physical items. It is also responsible for converting the data into digital signals, which are simpler to send over a network. The physical layer depends on embedded intelligence and nanotechnologies [57]. The first creates chips that are smaller and embedded into commonplace items, like wearables with nano integration [58]. These devices collect data and forward it to the network layer.
- Network Layer: The network layer is the core element of the IoT. The information gathered by the perception layer is transmitted by it. It comprises the hardware and software instrumentation of the internet network, as well as the management and information centers. Data can be sent throughout the network as packets thanks to data routing channels provided by the network layer [59]. It comprises all network hardware, including switches and routers, required for the proper operation of WiFi, infrared technology, ZigBee, Third Generation (3G), Fourth Generation (4G), and Fifth Generation (5G), as well as communication and routing protocols.
- Application Layer: The majority of the technology's potential is realized at the application layer, which acts as the front end of the IoT architecture. The application layer's objective is to integrate industrial technology with IoT social demands; in other words, it can be thought of as a transitional layer between industry technologies and methods for controlling them to meet human needs [54]. It gives IoT developers access to the platforms, interfaces, and tools they require to create IoT applications, including those for intelligent transportation, intelligent homes, intelligent health, etc.

3.2.2 The 5-layer architecture

Due to the anticipated IoT development, the 3-layer architecture proved insufficient. Thus, a 5-layer architecture is suggested. The five key layers that make up IoT architecture describe all of the functionality of IoT systems. These layers are perception layer, transport layer, processing layer, application layer, business layer as shown in Fig. 2.

- Perception Layer: It is same as describing in 3-Layer architecture.
- Transport Layer: It appears to be the three-layer architecture's network layer. Information is sent and received from the processing layer to the perception layer and vice versa. It is equipped with numerous technologies, including Bluetooth, WiFi, and infrared. Additionally, this layer aims to use IPV6 to address every object in the system.
- Processing Layer: It is responsible to manage the data that the perception layer has collected. The two primary components of the handling process are analysis and storage. Because of the vast amount of system-related data that has been gathered, this layer's target is very challenging. As a result, it processes and stores information using a variety of methods, including database software, cloud computing, ubiquitous computing, and intelligent processing.
- Application Layer: Determining the type of applications that will be utilized in the IoT is the goal of this layer. Furthermore, it enhances the intelligence, authenticity, and security of IOT applications.

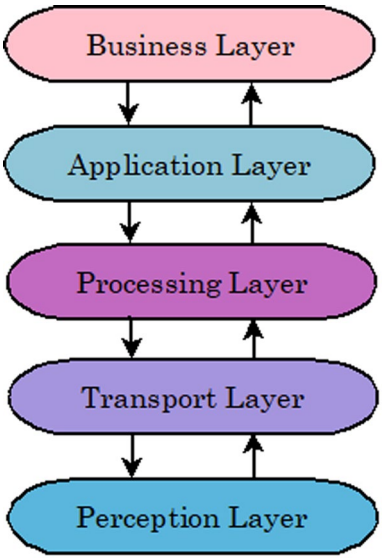


Fig. 2 IoT 5-layer architecture

- Business Layer: The work of this layer is to specify the charge and management of IOT applications. It is also in charge of all IoT application-related research as well as user privacy.

3.2.3 The 7-layer architecture

As the demand and applications are increasing, the IoT has undergone more design modifications. Early IoT scenarios used a three-layer paradigm with sensors and actuators as the base layer and cloud computing as the top layer [60]. The next practical approach to implement IoT turned out to be service-oriented architecture (SOA) [61]. A component-based model that may be built to connect various services through interfaces and protocols is the essence of SOA [11]. According to recent studies, CISCO's seven-layer approach is thought to be the most compatible and practical model for the IoT. The 7-layer approach is thoroughly explained, along with potential applications, in the early CISCO study [62] as shown in Fig. 3.

- Physical Devices and Controllers: Because it contains physical devices and controllers, the model refers to this layer as the "things" of the IoT. From the perspective of the system design, the sensors and other devices that are directly controlled by the IoT architecture are called "things". To enable distributed processing, high degrees of autonomy, and low latency responses to field events, Edge Intelligence is a key IoT concept that must be implemented at this layer.
- Connectivity: The layer that starts in the "middle" of an edge node device and goes all the way up to the point where data is transported to the cloud is known by this name. This layer comprises the back haul to the on-premises or cloud environment, Edge Computing, which comes after, and the mapping of field data to the logical and physical technologies that are employed. This layer represents just one of the numerous communication options available.
- Edge Computing: It is sometimes called "Cloud Edge" or "Cloud Gate-way" computing and is the next tier of the Global Forum Model architecture. Another name for this layer is "Edge Computing". All IoT systems require this layer, which connects the data and control planes to the higher cloud or business software layers, in one way or another. Protocol conversion, routing to higher layer software functions, and, if needed, fast path logic for low latency decision making will all be implemented by this layer.
- Data Accumulation: Gathering of Information It's Critical to Have Incoming Data Storage Given the Velocity, Volume, and Variety of Data. IoT systems can provide incoming data storage must be made available in order to process, normalize, integrate, and get ready for upstream applications later on. This is so that this data can be provided by IoT systems.

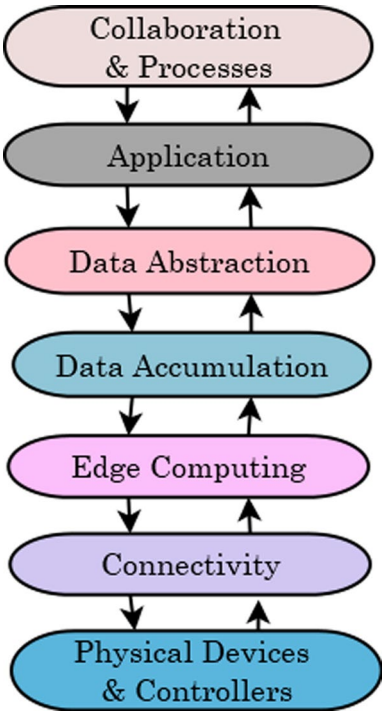


Fig. 3 IoT 7-layer architecture

- Data Abstraction: The data abstraction layer gathers like data from various IoT sensors or measurements, processes high-priority traffic or alarms quickly, and arranges incoming data from the data lake into flows and schema that are suitable for processing further upstream. Stated differently, we interpret the data.
- Application Layer: The layer that houses the application logic that drives both the control and data planes is known as the application layer. This layer should go without saying. Monitoring, process optimization, alarm management, statistical analysis, control logic, logistics, and consumer pattern analysis are a few IoT applications.
- Collaboration and Processes: Users are presented with application processing at this layer, and business applications incorporate data processed at lower layers. Additionally, this layer is in charge of enabling communication between various business applications. Human interaction with every other layer of the IoT system is the focus of this layer. Additionally, economic value is supplied at this layer. Using the value of the IoT and the tiers of infrastructure and services beneath it to promote economic growth, business optimization, and/or social good is the challenge at this layer.

3.3 Generic architecture of IoT

A flexible layered architecture is vital for the IoT, as it should be able to connect billions or even trillions of heterogeneous objects. There is still no consensus on a reference model among the countless architectures that have been proposed [63]. In order to helight and implement the IoT arecitecture their is a need to understand which layer implement which protocol or technology. For thus, we proposed an architecture that can be seen as the extended version of TCP/IP protocol stack. As IoT layers uses the TCP/IP protocols for processing and communication of data, from Fig. 4 it is easy to understand why particular layer implement specified protocol. The summarize representation of all the layers are:

3.3.1 Perception layer

The Perception Layer, also known as the Sensing Layer, is the foundational layer in IoT architecture. Its primary role is to collect data from the physical environment using a variety of sensors, actuators, and edge devices. This layer interacts directly with the physical world, enabling IoT devices to sense changes and gather critical information about their surroundings. Three main component of this layer are: (a) Sensors: these devices measure physical parameters such as temperature, humidity, motion, light, pressure, or sound. Different sensors are deployed depending on the type of data to be collected. (b) Actuators: these are mechanisms that can control or alter the physical environment based on the data

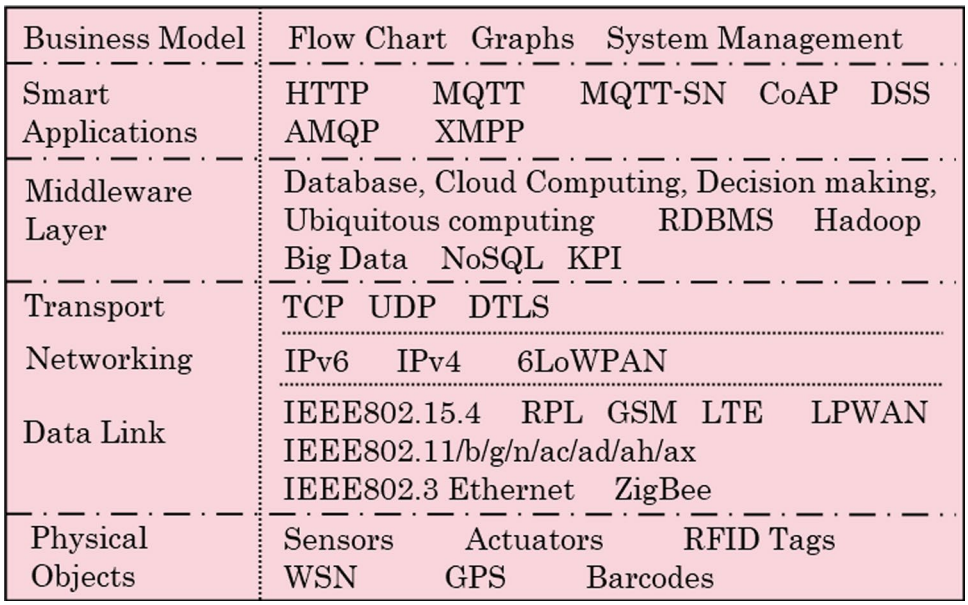


Fig. 4 Generic architecture of IoT

received. For instance, an actuator can turn on a fan when a temperature sensor detects that the room is too hot. (c) RFID Tags: it help in identifying and tracking objects, commonly used in logistics and inventory management.

This layer support a wide variety of sensors and devices exist to cover different use cases-enabling applications in smart homes, healthcare, agriculture, industrial IoT, and more. Also, the sensor technology is improved in many ways, such as miniaturization and low-power sensors, have enhanced the scalability and feasibility of IoT deployments in various fields. It support edge processing, so the data is prepossessed or filter, and that helps to reduce the burden on subsequent layers.

Still there are few challenges remains at this layer like: (a) Energy Consumption by devices: many IoT devices at this layer are battery-operated, making energy efficiency critical. Regular battery replacements or recharging can become a challenge, especially in large-scale deployments. (b) Security Vulnerabilities: devices in the perception layer are often vulnerable to physical tampering, data spoofing, or hacking. Attackers could compromise sensors to alter data, leading to incorrect system behavior. (c) Environmental sensitivity: sensors are subject to wear and tear, environmental changes (temperature, humidity), and interference from external factors, which can degrade their performance or cause them to malfunction. d) Data Quality: as the raw data comes from various devices in sometimes harsh environments, ensuring the quality, accuracy, and reliability of the data is challenging. Poor-quality data can affect the performance of the overall IoT system.

3.3.2 Data link layer

It includes and implement all necessary protocols that are require for hop to hop communications. The Data Link Layer in IoT architecture is a crucial layer responsible for establishing reliable communication between devices within a local network. It provides the necessary protocols and methods to ensure that data is transmitted correctly between connected devices, and it also manages how devices access the shared medium of communication, such as radio frequency or a wired connection. This layer is typically part of the Network Layer in a three-layer model or treated as a separate layer in more detailed IoT architectures. Key Protocols in this layer are same as TCP/IP protocol such as: (a) Ethernet: it is commonly used in wired IoT networks, Ethernet frames ensure reliable data transmission over a wired connection. (b) Wi-Fi (802.11): it is widely used wireless protocol, especially in home and office IoT networks, enabling data exchange over the air within short to medium-range distances. (c) Bluetooth: this short-range wireless protocol useful for low-power IoT devices such as wearables, smart home devices, and sensors. (d) Zigbee: a low-power, low-datarate wireless communication protocol used in home automation, smart lighting, and energy management systems. (e) LoRaWAN: it is used for long-range, low-power IoT applications in agriculture, smart cities, and environmental monitoring.

Data Link Layer support reliable data transmission via error detection and correction mechanisms which ensure that data corruption during transmission is minimized, leading to reliable communication, low power consumption

technologies through the use of Zigbee, LoRa, Bluetooth which is crucial for IoT devices operating on limited power resources, access control provided by MAC sublayer to efficiently manages shared communication mediums by avoiding collisions and transmit data seamlessly. This improves overall network efficiency. Still few challenges are still uncovered as limited coverage area by communication devices which may not be suitable for larger or more dispersed IoT systems, potential congestion in densely populated networks, such as in smart cities or large IoT deployments, there can be congestion on the communication medium, leading to delays and reduced data throughput, security risks because it support basic encryption which are often prone to security vulnerabilities like eavesdropping or man-in-the-middle attacks, making additional layers of security crucial.

3.3.3 Network layer

It define the addressing mode IPv4 and IPv6 used for communication between two devices. The Network Layer in IoT architecture is responsible for enabling data transmission between IoT devices and higher-level systems like servers, cloud platforms, and other devices across local or global networks. It handles the routing, forward-ing, and addressing of data packets, ensuring that data generated by IoT devices at the Perception Layer is properly transmitted to where it needs to go, whether that is another IoT device, an edge server, or a cloud-based service for further processing. Key protocols and technologies supported by this layer are: (a) IPv4/IPv6: Internet Protocol version 4 (IPv4) and version 6 (IPv6) are the core protocols for routing and addressing devices on the Internet. IPv6, with its vastly larger address space, is more suitable for the growing number of IoT devices. (b) 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks): A protocol that allows IPv6 packets to be transmitted over low-power wireless networks, such as those used by IoT sensors and actuators. (c) RPL (Routing Protocol for Low-power and Lossy Networks): A distancevector routing protocol specifically designed for wireless sensor networks and other IoT systems that operate in environments with limited power and unreliable communication links. (d) LoRaWAN/Sigfox: LPWAN protocols for long-range communication. (e) LTE-M/NB-IoT: Cellular protocols tailored for IoT. f) Wi-Fi/Bluetooth: Local area and short-range communication protocols.

Network layer support scalability, interoperability, facilitates communication across different protocols, efficiency, security to ensures data integrity and confidentiality during transmission. Still their are some challenges faced at this layer are network complexity latency, resource constraints, security threats as vulnerabilities to data interception and unauthorized access.

3.3.4 Transport layer

It define that which type of network connection is establish between end to end devices. The connection can be either connection less or connection oriented. The Transport Layer in IoT architecture is responsible for managing end-to-end communication between devices, ensuring reliable data transmission, error handling, and flow control. It operates above the Network Layer, managing how data is segmented, transferred, and reassembled on both ends of the communication channel. In the context of IoT, this layer is essential to maintaining communication integrity, especially for applications that require reliable and consistent data transmission across networks. In order to implements the functionalists TCP, UDP CoAP and SCTP protocols were kept same as in the Layered architecture of TCP/IP. Other then these, Message Queuing Telemetry Transport (MQTT) protocol is implemented to apply publish-subscribe messaging. It is lightweight and easy to implement for constrained devices with lowbandwidth networks. It operates over TCP and is commonly used in IoT applications for its efficient use of bandwidth and support for unreliable networks.

Transport layer optimizes the transmission of data, minimizing latency and overhead, which is critical for real-time applications in IoT. Also, scalability supports a growing number of connected devices by managing connections and data flow efficiently, enabling large-scale IoT deployments. It implements necessary security measures to protect data during transmission, ensuring the integrity and confidentiality of sensitive information. But there are some challenges faced at this layer which are: network reliability, resource constraints, heterogeneity among diverse range of IoT devices and communication technologies can lead to challenges in interoperability and protocol compatibility.

3.3.5 Middleware layer

It access and use the service provide by cloud provider and perform the computation for decision making. For data management and analysis Big data, Hadoop and NoSQL are used. The Middleware Layer in IoT architecture acts as a bridge between the lower hardware-centric layers (such as the Perception and Network layers) and the higher application-centric

layers (such as the Application and Business layers). This layer provides essential services such as data management, device management, communication, security, and interoperability. The goal of the middleware layer is to abstract the complexity of managing numerous heterogeneous IoT devices and networks, facilitating seamless communication, integration, and interaction between different IoT components and services. Middleware Platforms are: (a) Eclipse IoT Stack (Kura and Kapua): Provides IoT middleware components like Kura (for device management and communication) and Kapua (for data management and device integration). (b) OpenIoT: An open-source middleware platform that provides services for data integration, device management, and sensor virtualization. It is designed to handle large-scale IoT deployments. (c) FIWARE: A comprehensive middleware platform that provides a suite of tools for IoT device integration, data. (d) Amazon AWS IoT Core: AWS IoT Core offers a managed platform for connecting and managing IoT devices, enabling secure communication and integration with other AWS services for data storage, processing, and analytics.

Middleware Layer support simplified development by abstracts the complexities of device communication, data handling, and security, allowing developers to focus on building applications rather than managing low-level IoT infrastructure. Interoperability enables devices from different vendors, using different protocols, to communicate and work together seamlessly. Scalability supports the growth of IoT systems, ensuring that they can handle increased data and device numbers without compromising performance. Still their are some issue related to handling the wide variety of devices, protocols, and data formats remains a significant challenge, especially in large IoT systems with multiple vendors and standards. Latency to ensure real-time data processing and response, especially in critical applications like healthcare or industrial automation. Designing and maintaining middleware that supports a broad range of devices and services while ensuring security, scalability, and performance can be complex and resource-intensive.

3.3.6 Application layer

The Application Layer is the topmost layer in the IoT layered architecture, responsible for providing services and enabling the interaction between users and IoT devices or systems. This layer is where the data collected, processed, and transmitted by lower layers is transformed into meaningful insights, actions, and interfaces tailored to specific IoT applications. It connects IoT functionalities to real-world applications across various industries, such as smart cities, healthcare, industrial automation, and more.

Key technologies supported at application layer are:

- Web and Mobile Applications: Allow users to access and control IoT systems from anywhere using their smartphones or computers.
- Cloud Platforms: Cloud computing enables scalable and real-time data processing, which is crucial for large-scale IoT systems.
- APIs (Application Programming Interfaces): Through APIs, IoT applications can pull data from sensors, send commands to devices, or access external services like weather forecasts or mapping.
- Artificial Intelligence (AI) and Machine Learning (ML): Many IoT applications incorporate AI/ML algorithms for predictive analytics, anomaly detection, and decision-making. For instance, machine learning models can predict when a machine will fail, allowing proactive maintenance.
- Data Analytics Tools: IoT applications rely on real-time and batch processing tools to analyze large volumes of data generated by devices. These tools help identify trends, optimize processes, and provide actionable insights to users.

Application Layer support customization of applications as per service needs to provides flexibility for industry-specific solutions, enabling IoT systems to meet the specific needs of sectors like healthcare, agriculture, and smart cities. User interaction allows for seamless interaction between users and IoT devices, enhancing convenience and operational efficiency. Real-Time monitoring enables continuous tracking of environments, devices, or systems, providing up-to-date information and automated responses to changes or anomalies. Facilitates automation by using analytics and machine learning, allowing IoT systems to autonomously manage processes and respond to conditions without human intervention.

3.3.7 Business model

The data is analyzed and represented in the forms of graphs and flowcharts. It helps the IoT users for fast decision making and controlling of fields. The Business Model Layer is an optional but increasingly crucial layer in IoT architectures,

focusing on the economic and strategic aspects of IoT deployments. This layer defines how IoT systems create value, generate revenue, and align with the overall business strategy of organizations. It is the layer where the technical capabilities of IoT (provided by lower layers) are transformed into sustainable business models, addressing the needs of stakeholders like consumers, enterprises, and service providers.

The proposed IoT architecture includes all the necessary Layers and enabling technologies used in implementation of IoT.

3.4 Future vision of IoT

The IoT is currently a vision that is being developed, and depending on their areas of interest and how they plan to use it, there could be a large number of stakeholders in this development. The IoT is still in its infant stages, during which everyone is attempting to interpret it in accordance with their own requirements. In the current vision, there is a role for sensor-based data collection, as well as data management, data mining, and the World Wide Web. Obviously, hardware based on sensors also plays a role in this process. A straightforward and comprehensive definition of the IoT [64, 65] and the fundamental idea behind this concept is the pervasive presence around us of a variety of things or objects such as RFID tags, sensors, actuators, mobile phones, etc. able to interact with each other and collaborate with their neighbors to achieve common goals [60]. Zhao et al. [66] discuss three distinct visions of IoT. They are as follows:

- Things Oriented Vision: We can use sensors and ubiquitous technologies like RFID to track anything, which lends credence to this vision. The basic concept is to uniquely identify any object using Electronic Product Code (EPC) requirements. This approach is expanded by the use of sensors. It is critical to acknowledge that future vision will rely on sensors and their capabilities to achieve "thingsoriented"vision. By working together, we will be able to use embedded sensor systems and sensors to generate the data. In order to handle the integration of RFIDbased technologies with advanced sensing and computing devices as well as global connectivity, the condensed vision will rely on sensor-based networks in addition to RFID-based Sensor Networks.
- Internet Oriented Vision: The internet-focused vision has made it clear that connected smart objects are needed. Since IP is one of the most important protocols used on the Internet, the objects need to have IP-like properties. The sensor-based item can be translated into a format that is comprehensible, can be uniquely identified, and can have its characteristics continuously tracked. This creates the framework for intelligent embedded things, which can be imagined as little computers with processing power.
- Semantic Oriented Vision: This vision is made possible by the fact that we will have a huge number of sensors at our disposal and that the data they will collect will be very large. So, we'll have a lot of information, some of which may be redundant, that needs to be processed in a useful way. For better representations and understanding, the raw data needs to be managed, processed, and put out in a way that is easy to understand. If we can make sets of data into homogeneous and heterogeneous formats, then understanding the data will depend on the semantic technologies that are used to process the data. Here, we need a broad view of how to turn raw data into useful data and a clear separation between the data and how they should be interpreted.

4 Market opportunity

The IoT offers a significant market opportunity for equipment manufacturers, Internet service providers, and application developers. According to a report [2], for the first time, in 2020, there were more IoT connections than non-IoT connections (smartphones, laptops, and PCs). Examples of IoT connections include connected cars, smart home appliances, and connected industrial equipment. By the end of 2020, 11.7 billion (or 54%) of the 21.7 billion active connected devices globally were IoT connections. Over 30 billion IoT connections or nearly 4 IoT devices per person on average are predicted by 2025. Furthermore, it is anticipated that M2M traffic flows will contribute up to 45% of all internet traffic by 2022, as stated in reports by [67–69]. These predictions have been surpassed, as the number of connected devices has already experienced a remarkable 300% increase over the past five years, exceeding expectations outlined in a report by McKinsey Global Institute [70]. Additionally, a study on cellular network traffic in the United States revealed a substantial 250% surge in M2M traffic volume in 2011 [71]. Looking ahead, the IoT technology market is projected to witness substantial growth, with its market size expected to expand from USD 384.5 billion in 2021 to USD 566.4 billion by 2027 [72]. The global number of IoT devices is expected to nearly double, from 15.9

billion in 2023 to more than 32.1 billion by 2030. In 2033, China will have the most IoT devices, with approximately 8 billion consumer devices. IoT devices are used in a wide range of industry verticals and consumer markets, with the consumer segment accounting for approximately 60% of all IoT or connected devices by 2023 [73]. The potential economic impact and projected market share of dominant IoT applications by 2025 is shown in Fig. 5.

The economic growth of IoT-based services holds great importance for businesses. Particularly, the sectors of manufacturing and healthcare are expected to experience the most substantial economic impacts. By leveraging electronic media to provide efficient medical services such as wellness, prevention, diagnosis, treatment, and monitoring, healthcare applications and other IoT-based services like telecare and mobile health (m-Health) are projected to contribute between $1.1 and $2.5 trillion in annual growth to the global economy by 2025. By 2025, the total yearly economic impact of the IoT is projected to be between $2.7 trillion and $6.2 trillion [70]. Conversely, Wikibon projects that the industrial Internet will generate approximately $1279 billion in value by 2020, with a 149% increase in Return on Investment (ROI) from 13% in 2012 [74]. As per the World economic Forum 2022 report, 131.4 million households were uses smart speakers in 2022, and 335.3 million is predicted to use smart speakers by 2027 [75].

The growth of IoT market in various fields are as follows:

- Smart Home Automation: Growth in smart home devices like smart speakers, thermostats, and security systems. Market Size is expected to reach $174 billion by 2025 [76].
- Healthcare: Expansion of remote monitoring, telemedicine, and wearable health devices. In 2022, the Indian healthcare industry reached $372 billion. Market Size is expected to grow to $612 billion by 2025 [77].
- Industrial IoT (IIoT): Increased automation in manufacturing, predictive maintenance, and supply chain management. Market Size is projected to exceed $500 billion by 2025 [78].
- Smart Cities: Development of smart infrastructure, traffic management, and public safety solutions. Market Size is reach $1.8 trillion globally by 2025 [79].
- Agriculture: Use of IoT for precision farming, livestock monitoring, and resource management. Market Size is expected to grow to $26.52 billion by 2025.

Nevertheless, these statistics indicate that there is a strong possibility for substantial and swift growth in the IoT and its associated industries and services in the foreseeable future. This presents a unique opportunity for manufacturers of traditional appliances and equipment to transform their offerings into "smart devices" with the aid of this technological advancement. In order to foster the widespread adoption of the IoT and its related services globally, internet service providers (ISPs) must establish networks that can deliver QoS for various types of machine-to-machine, person-to-machine, and person-to-person traffic flows.

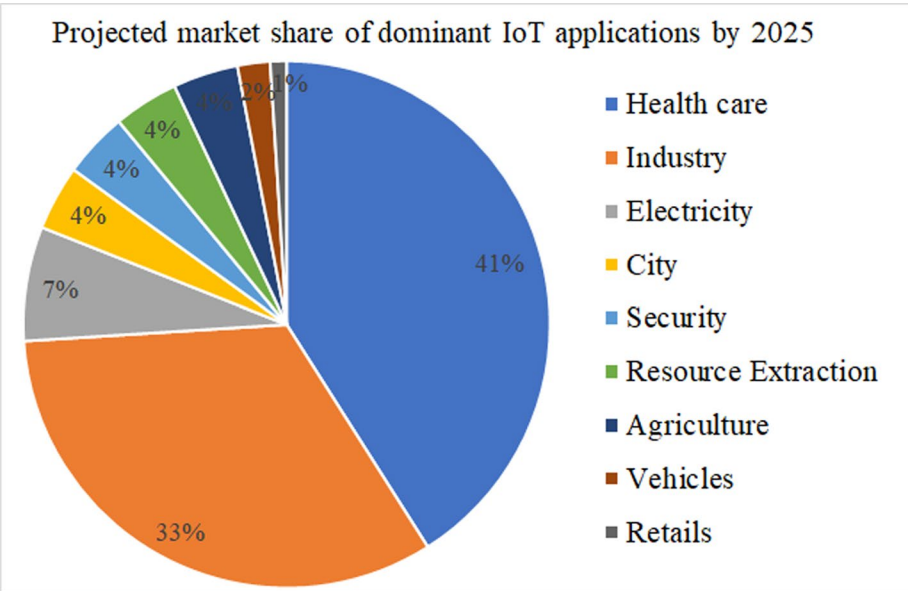


Fig. 5 Potential economic impact and projected market share of dominant IoT applications by 2025

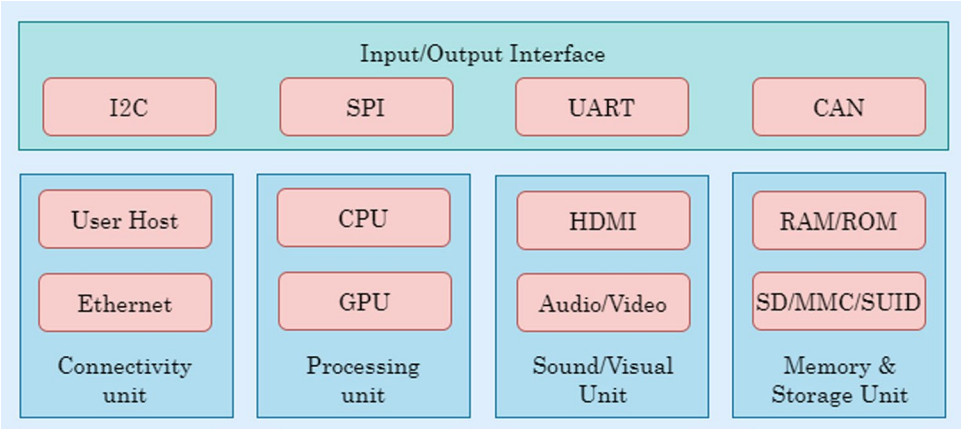


Fig. 6 Functional blocks of IoT system

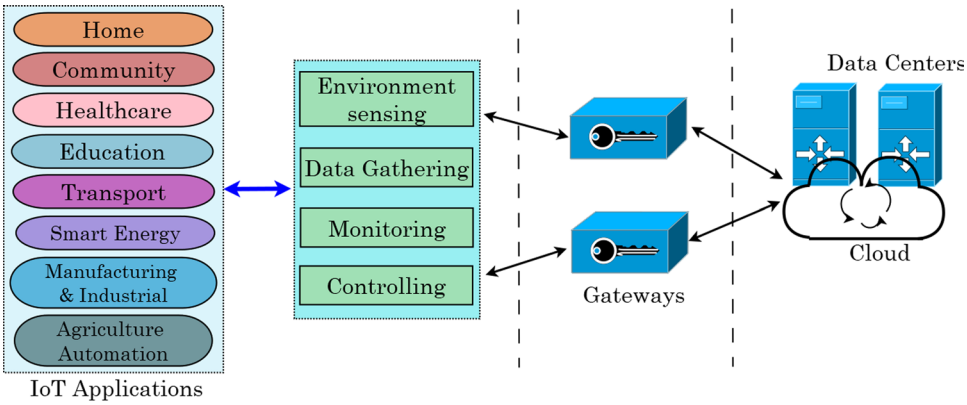


Fig. 7 Components of IoT system

5 Functional blocks of IoT system

The requirements and application domain can alter IoT designs [30, 37, 80]. An IoT system comprises several functional building blocks that facilitate various IoT activities, such as sensing mechanisms, authentication and identity, control, and management, in addition to a layered foundation. Figure 6 depicts these types of IoT architectural building elements.

Various essential functional components oversee input/output tasks, network concerns, data processing, audio/video surveillance, and storage administration. Optimal efficiency necessitates a well-functioning IoT framework comprised of these fundamental elements. Despite the existence of multiple proposed reference architectures with associated technical specifications, a universally accepted architecture tailored for the worldwide IoT environment remains elusive [81]. Consequently, the development of a suitable architecture capable of meeting all the requirements of IoT is still imperative.

5.1 Components of IoT system

IoT is made up of a wide range of gadgets that are interconnected based on how they are organized and configured functionally. To facilitate co-building and openness in IoT, a universal standard architecture for all kinds of applications is preferred. The functional processing of IoT system is shown in Fig. 7.

By dissecting the complex IoT system design into discrete phases, which collectively comprise the comprehensive IoT network architecture, the design can be made more understandable. These steps, which are frequently shown in an IoT architecture diagram, make sure that devices are capable of efficiently gathering, processing, and acting upon data. In the following steps, the elements of IoT systems are explain in detailed:

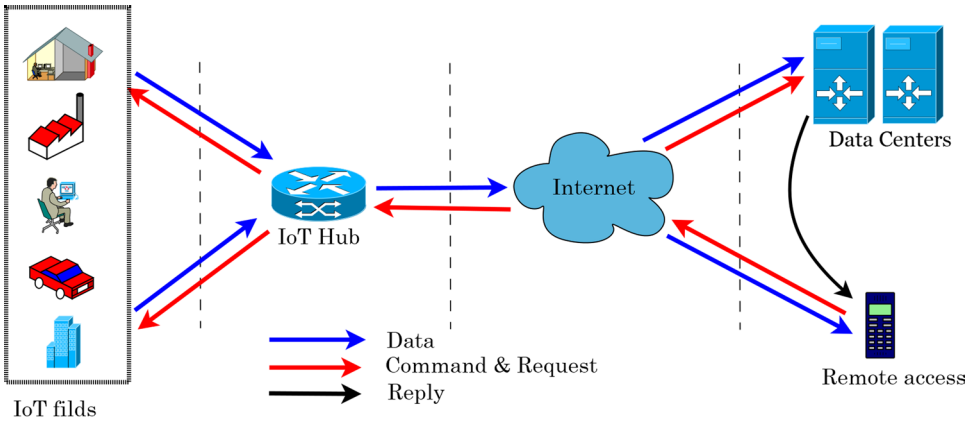


Fig. 8 Communication and data transfer in IoT system

Table 1 IoT Protocol stack

Layer	Protocols
Physical layer	802.15.4 [83], RFID, 802.11 g/ac/ad/ah [84], BLE [85], LTE-A [86], Z-Wave, NFC, ANT + [87], LoRaWAN [88], SigFox [89]
Network layer	6LoWPAN [83], 6TiSCH [90], IPv4, IPv6 [64], RPL [91], CoRPL [92], CRB-RPL [93], IETF ROLL
Application layer	CoAP [94], MQTT [90], SMQTT [95], XMPP [64], DDS [96], AMQP [97], IETF CORE, HTTP, SSH

- IoT applications: There are number of application areas like smart homes, smart city, logistics, etc. where there is a continues monitoring and sensing is required to take further actions for controlling the environment.
- IoT devices: In the IoT application areas we deploy IoT devices and these devices are responsible for capturing real-world parameters and interactions. The term "devices" envelops a plethora of gadgets, from simple temperature sensors to complex industrial machines. Through sensors and actuators embedded in these devices are used for continues monitoring and capturing of data.
- Internet Gateways: In the architecture of the IoT platform, gateways play the vital role of a bridge, making sure that data from devices finds its way to the larger Internet infrastructure. Their role as middlemen is to ease the transfer of data between local and wide-area networks. Modems, routers, and gateway devices work together to control and optimize data flow. Before data is sent forward, the Data Acquisition System (DAS) processes, filters, and aggregates it. In addition, it has a security function, ensuring data integrity and confidentiality throughout the IoT network architecture.
- Cloud date centers: After data passes through the gateway, the IoT cloud architecture is activated. This is where intensive analytics, storage, and processing take place. The main goal is to offer centralized processing, analytics, and storage for the massive volume of data that is coming in. At the center of the IoT system architecture is the cloud, which is made up of strong servers, databases, and analytical tools. The data is subjected to extensive processing, analytics, and storage procedures that transform unstructured information into insightful patterns and insights relevant to various IoT architecture types.

5.2 Working model of IoT and enabling technologies

An IoT system's general operating structure is shown in Fig. 8. Because they enable connectivity between IoT environment and IoT servers for a range of applications, IoT gateways are essential for IoT communication [82]. Designing an effective IoT architecture in a heterogeneous context requires careful attention to four main factors: openness, scalability, modularity, and interoperability.

In order to satisfy the needs of cross-domain interactions, multi-system integration with the potential for simple and scale-able administration features, big data storage and analytics, and user-friendly applications, the IoT architecture must be developed. The architecture must also be able to expand the functionality and give the system's IoT devices more automation and intelligence.

The protocols and technologies that are implemented at different layers of IoT architecture is mentioned in Table 1. Such protocols are used for sensing, capturing, communication, packet formation, routing, message passing, security, etc. The literature mostly covers data connection, network, and application layer protocols. The low weight of the protocols or technologies is their primary distinguishing feature, but they also place a strong emphasis on scalable, energy-efficient solutions for devices with limited resources (Table 1).

To distribute channels or medium to stations for coordinating data transfer among smart devices, data link layer protocols are utilised. Based on the IEEE 802.15.4 standard, ZigBee technology [98] aims to deliver a wireless data solution with dependable and secure wireless network designs. One of the most popular IoT protocol standards, ZigBee, allows smart items to communicate with one another. As opposed to Bluetooth devices, which take about 3 s to transition from passive to active mode, ZigBee devices have lower latency and are more responsive. BLE [85] is a short-range communication protocol that uses a contention-free MAC with minimal latency and quick transmission to save 10 times more energy than traditional Bluetooth. The existing IEEE 802.11 (Wi-Fi) standards' poor scalability, frame overhead, and high power consumption make them unsuitable for IoT applications. The IEEE 802.11 working group established a task group to create the 802.11ah standard [84], which provides minimal overhead and power-friendly communication and is appropriate for the IoT. In many instances, IoT uses RFID readers to gather environmental data through sensors. It is an identification system that, without human assistance, can use its radio frequency signal to autonomously identify target devices and collect data. It can manage the proper communications and information processing, and it has the capacity to uniquely identify things with the ability to provide position information.

The network layer protocols provide an abstract representation of the devices found in the smart world. Along with the established network layer protocols like IPv4 and IPv6 [64], a number of novel routing protocols are proposed for the IoT, such as 6LoWPAN [83, 92] and CRB-RPL [93]. For the Internet protocol to be implemented in so many resource-constrained devices, IPv6 is better than 6LoWPAN. In order to provide a suitable routing solution (RPLs), the Internet Engineering Task Force (IETF) Routing Over Low Power and Lossy Networks (ROLL) working group developed a new IPv6 Routing Protocol for Low power and Lossy networks. For multi-hop mesh technology, it offers effective routing routes in lossy, low-power networks. As a routing metric, RPL used node information and link costs. Node information includes workload, throughput, latency, dependability, and available energy resources. In CoRPL [92] and CRB-RPL [93], which employ Cognitive Radio (CR) for decision-making, the RPL is further changed.

A number of new protocols are being created at the application layer to accommodate the extensive and high volume IoT device network. Message Queue Telemetry Transport (MQTT) [99] is designed for IoT devices of small size that have low bandwidth, high costs, low processing power, and unstable networks so that they can communicate seamlessly among themselves. This allows for seamless communication between these devices. is designed for communication between machines (M2M). It provides a traditional one-to-one M2M IoT application. Some more appropriate protocols are the Constraint Application Protocol (CoAP) [94], the Advanced Message Queuing Protocol (AMQP) [97], the Extensible Messaging and Presence Protocol (XMPP) [64], and the Data-Distribution Service protocol (DDS) [96]. A web service oriented program called CoAP was developed to make it easier for low-resource electronic devices to communicate over the Internet. CoAP has low overhead, multicast capabilities, and is straightforward to transform into HTTP for simplification.

XML-based instance message oriented protocol named XMPP [64] is suggested to enable human-to-human (H2H) communication in the IoT. It is made to provide instant messaging connections between individuals. In addition to offering scalability and speed improvements for IoT applications, the DDS protocol [96], promotes interoperability across smart devices connected to the IoT. For high throughput and low latency, it supports numerous transport protocols, including multicast and TCP/IP and UDP/IP. Because to its distributed processing architecture, it can be directly connected to smart devices and sensors without the need for a centralised server. The IoT is created with the AMQP [97], which is primarily appropriate for server-based analysis and control plane. It offers compatibility and dependability for the servers' message queuing systems. AMQP can also be used for secure transactions, publish-subscribe messaging, and flexible routing.

6 IoT Services and applications

The IoT has a wide variety of possibilities for application development, but our culture is only able to take advantage of a very small fraction of those possibilities at the present time. New applications have the potential to improve the quality of our lives in a wide variety of contexts and settings, such as when we are at home, when we are traveling, when we are sick, when we are at work, when we are jogging, and in the gym, to name just a few examples. In these settings, the only form of intelligence present is rudimentary, and the majority of time, there is no way for individuals to communicate

with one another. Making it possible for these things to talk with one another and to process the information they gather from their surroundings necessitates the creation of distinct environments in which a very diverse set of applications can be used. When designing an application, some of the characteristics that should be taken into consideration are those outlined like network availability, coverage area, bandwidth, user involvement, redundancy, and effect analysis. Therefore in order to creating intelligent systems smart water, smart retail, smart offices, smart transportation, smart agriculture, smart healthcare, smart energy, etc. [100, 101]. Many of the IoT potential application domains are shown in Fig. 9.

A multidisciplinary vision for the environment, industry, public/private sector, healthcare, transportation, and other fields is provided by IoT. Different scholars have given different explanations of the IoT based on specific aspects and areas of interest. Numerous application domains show off the power and promise of IoT. A number of significant IoT initiatives have taken the market by storm in recent years. A selection of the notable IoT projects that have dominated the market are shown in Fig. 5. It is evident that, in comparison to other IoT projects, those centered around health care, industry, electricity hold a sizable market share.

The IoT is primarily concerned with the qualities of IoT services that are built on RFID, sensors, and 6LoWPAN communication networks. The 6LoWPAN communication can be utilized in a wide number of applications to collect sensor data and interpret the information, all of which will result in significant shifts in the ways in which we work and live. Many services and examples of common applications from a variety of fields have been discussed in this section.

6.1 Smart industry automation

In the workplace, the "Network of Things" is referred to as an enterprise-based application. Only the owners can use the information gathered from these networks, and it can be released in certain ways. The first widely used application to manage the building's utilities and keep tabs on the number of occupants is environmental monitoring (e.g., HVAC, lighting). Sensors have always been a crucial component of the automation, climate control, security, and other systems installed in factories. Eventually, a wireless system will take its place, providing the flexibility to adjust the configuration as needed. This is merely an IoT subnet for factory upkeep.

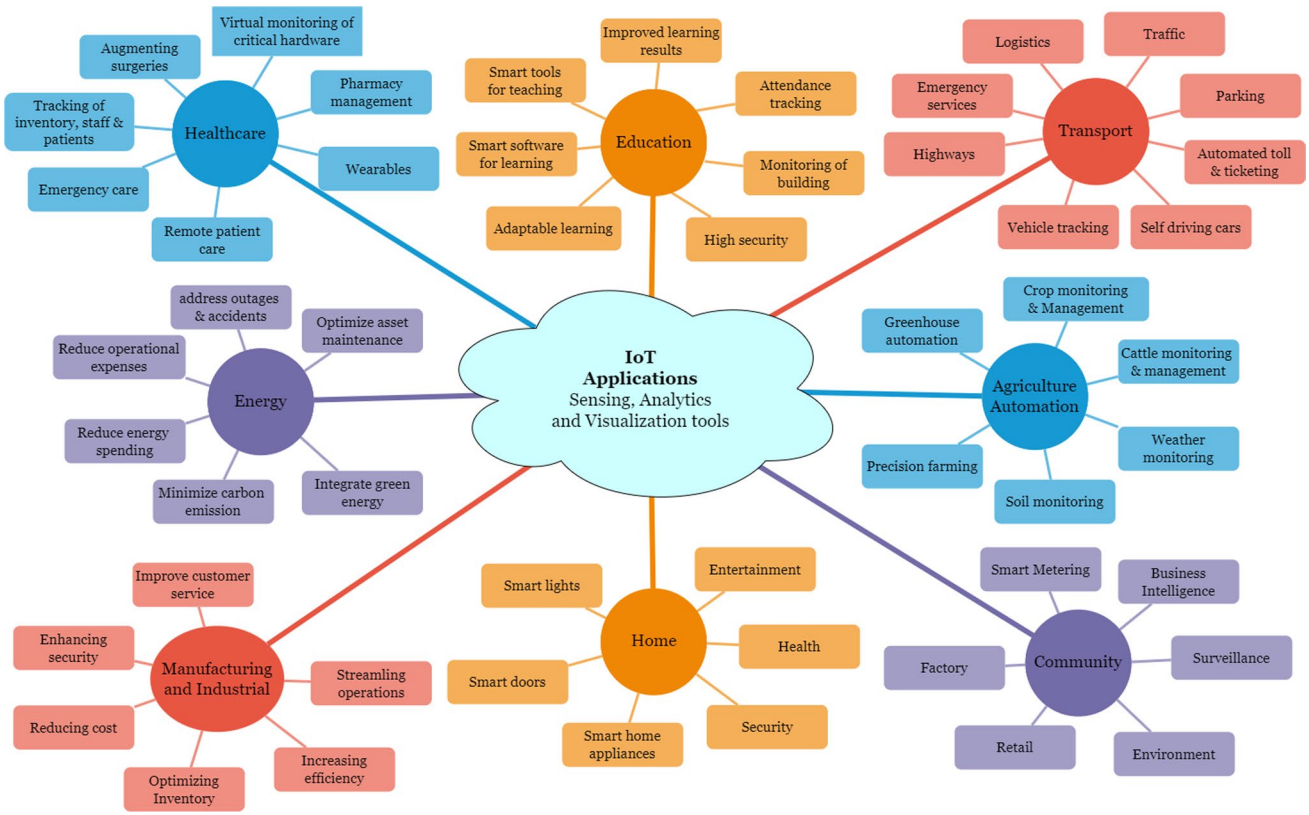


Fig. 9 Application domains of IoT

Table 2 IoT application domains

Factors	Industry	Energy	Transporta	tCiointy	Healthcare	Supply Chain	Agriculture
Users	Large, commu- nity level	general public, govern- ment	community level, gen- eral public	general public, policy makers,	general public, govern- ment	Few, com- munity level	Few, landown- ers, policy makers
Network size	Large	Large	Large	Medium	Small	Medium	Medium/Lar
Battery	Rechargeable battery, Energy harvesting	Rechargeable battery	Rechargeable battery, Energy harvesting	Rechargeable battery, Energy harvesting	Rechargeable battery	Rechargeable battery	Rechargeable battery, Energy harvesting
Internet connectiv- ity	Wifi, satellite communi- cation	Wifi, satellite communi- cation	Wifi, satellite communi- cation	Wifi, 3G, 4G LTE	Wifi, 3G, 4G LTE	Wifi, 3G, 4G LTE	Wifi, satellite communi- cation
Data man- agement	Shared server	Shared server	Shared server	Shared server	Local server	Shared server	Shared server
IoT devices	RFID, WSN, sin- gle sensor	RFID, WSN, sin- gle sensor	RFID, WSN, sin- gle sensor	RFID, WSN	RFID, WSN	RFID, WSN	WSN
Bandwidth	Large	Large	Large	Medium	Small	Medium	Medium
Example testbeds	Industry 4.0 [104, 105]	Smart energy meters (SEM) [106, 107, 108]	Intelligent trans- portation system [109 , 110]	Smart Santander [111]	AIoT-H [112]	production logistics andsup- ply chain system (PLSCS) [113, 114]	NodeMCU [115, 116]

Smart Environment IoT is one of the main IoT application areas that is already gaining popularity [102, 103]. A number of testbeds are currently in operation, and numerous more are scheduled for the upcoming years. Table 2 illustrates the subsystems that make up a smart environment, and a brief list of their technological attributes follows. It should be mentioned that data will be shared and that each subdomain covers a large number of focus groups. This covers the impact on citizens in terms of health and well-being issues; transportation in terms of mobility, productivity, and pollution; and services in terms of vital community services that are managed and offered to city dwellers by local government.

An enterprise-based application may, in any given setting of workplace activity, reveal the fact that it is built on a smarter environment. The individual or the business may, at its own discretion, release data to the outside world in this scenario. An additional benefit of IoT is the automation of industries. IoT has been offering revolutionary solutions for supply chain management and optimization, logistics, inventory control, quality control, and factory digitalization.

6.2 Smart energy conservation

The energy industry is expected to undergo a complete transformation with the advent of the IoT. It will revolutionize various aspects, ranging from the management of the electrical grid to energy production and enhancing energy efficiency. Through the utilization of data science and sensor-based technologies, solar and wind farms are becoming more automated and efficient. The applications of IoT extend across multiple sectors, including smart homes, smart grid systems, energy sustainability, auto-energy management, smart energy buildings, energy monitoring, energy harvesting, energy utilization and optimization schedules, energy internet, efficient data collection, and energy integration.

IoT advances contemporary technology. IoT technology makes it possible to connect every component involved in energy production and consumption. It also enhances operational visibility and offers significant leverage at every point in the energy flow process, from use to supply to end-user. The production of renewable energy and hydrocarbons both benefit economically from this partnership. IoT strategies for the power sector assist businesses in reducing maintenance and operating expenses by utilizing human labor and system optimization techniques. It is now feasible to optimize wind farm operations, maximize productivity, and drastically cut costs thanks to IoT and energy technology.

6.3 Smart transportation

One example of an IoT-based application that aims to enhance the concept of a smart city is a smart transportation system. The objective of a smart transportation system is to oversee smart cities through the utilization of advanced communication technologies. Inclement weather conditions such as dense fog and heavy rainfall can adversely affect conventional transportation systems that heavily rely on image processing. Consequently, the captured images may lack clarity. The implementation of an e-plate system [117] that incorporates RFID technology enables intelligent vehicle tracking, monitoring, and identification. Moreover, the incorporation of IoT into automotive technologies will enhance the management of traffic congestion, surpassing current capabilities. Through this technology, existing traffic systems can be optimized to facilitate efficient and automated communication among vehicles, eliminating the necessity for human intervention.

Real-time applications of satellite navigation systems and sensors are also possible for vehicles, ships, and aircraft. The majority of publicly accessible data, including delivery addresses, traffic jam locations, road conditions, weather forecasts, and gas station locations, can be used to optimize the routing of these vehicles. For instance, the updated data (route, cost) can be optimized, recalculated, and sent to drivers instantly in the event of a runtime address change. These vehicles' sensors can also provide real-time data to assess the condition of the engines, determine whether equipment needs maintenance, and forecast errors [118].

More sophisticated vehicles, including automobiles, trains, buses, and even bicycles, as well as roads and/or tracks, are being outfitted with sensors, actuators, and processing power. Roads themselves, as well as the goods that are being transported, are fitted with tags and sensors that transmit vital information to traffic control sites and transportation vehicles. This helps to improve the flow of traffic, contributes to the management of the depots, gives tourists access to information that is pertinent to their mode of transportation, and keeps track of the condition of the goods that are being transported.

Additionally, newly released vehicles with smart device integration are able to identify traffic jams and provide the driver with the best possible detour recommendation. This may lessen the amount of traffic in the city. Additionally, low-cost smart devices ought to be developed to be integrated into all range vehicles in order to track engine activity. IoT is also quite effective at preserving the health of the car. By using sophisticated sensors, self-driving cars may be able to

communicate with other self-driving cars. Compared to human-driven cars that used to drive in a stop-and-go manner, this would make traffic flow more smoothly. The global implementation of this procedure will require time.

6.4 Smart city

By introducing the concepts of smart homes, smart cities, and smart transportation and vehicles, the IoT is reshaping society's conventional civil structure into a hightech framework. Supporting technologies like machine learning and natural language processing are helping to make rapid progress in understanding the need for and usage of technology at home [119]. An efficient smart city requires the use of a number of technologies, including wireless sensor networks and cloud server technology, in conjunction with IoT servers. Consideration of the smart city's environmental aspects is another crucial matter. Therefore, when designing and planning the infrastructure of smart cities, energy-efficient and green technologies should also be taken into account. One further use of the IoT that is generating a lot of buzz is the smart grid and smart metering technology have been discussed in [60]. The consumption of energy can be effectively monitored in a number of different settings, including a locality, a small office, or even a smart home [66]. This model can be expanded to cover an entire city in order to more effectively balance load. The world is shifting at a rapid pace, and as a result, there is a growing demand for surveillance based on cameras. The processing of images and the use of computer vision will both be required for this surveillance. The IoT, which will be based on video processing [120], is a new technical challenge that aims to merge huge compute with small embedded devices. With technologies that enable sensors, it will be possible to create "smart homes" in which many items of daily usage will be monitored.

6.5 Smart healthcare monitoring

Imagine a scenario in a rural community in which people of all ages, including infants, pregnant women, elderly people, and others, all have RFID-enabled chips implanted in their bodies in order to monitor their key health data. Any behavior that is deemed strange on their behalf will cause an alarm to be raised or an alert to be issued in the nearby local medical assistance home. Patients, for instance, may have RFID chips implanted in their bodies in order to keep track of their medical history. Sensor technology has a number of applications, including those dealing with emergency response and health monitoring [60]. The information can be put to use to provide medical assistance to a person who requires it, and in the event of more severe abnormalities, it can be used to notify nearby hospitals that are well-equipped to handle the situation. As a result, the costs associated with hospitalization can be reduced through the utilization of early intervention and treatment [66, 121]. This is the benefit of utilizing the IoT in smart healthcare.

6.6 Smart supply chain

With the help of embedded sensor technologies, over a million elevators worldwide can be accessed remotely and communicate bidirectionally [71]. Both on-site and off-site technicians use the collected data to run diagnostics and repair options in order to make informed decisions that lead to increased improved customer service and machine uptime. In the end, big IoT data analytics gives a supply chain the ability to make decisions and manage the outside world. Factory equipment that is IoT enabled will be able to talk to each other about data parameters (such as temperature, machine utilization, etc.) and adjust settings or workflow to maximize efficiency [122]. Another use case that will be crucial to supply chains in the future when IoT infrastructure is present is in-transit visibility. RFIDs and cloud-based Global Positioning Systems (GPS), which offer location, identity, and other tracking data, are key technologies utilized by intransit visibility. The foundation of supply chains powered by IoT technologies will be these data. An item being shipped from a manufacturer to a retailer can be seen in great detail thanks to the information gathered by the equipment. Supply chain managers will be able to improve automated shipment and precise delivery information by predicting arrival time thanks to data gathered via RFID and GPS technologies. Managers will also have the ability to keep an eye on other data, like temperature control, which has an impact on the caliber of goods while they are in transit.

6.7 Smart agriculture and environment

By 2050, the world's population is predicted to grow to about 10 billion people. An important part of our lives is agriculture. To feed such a large population, we must improve the methods used in agriculture today. Therefore, in order to increase production in an efficient manner, agriculture and technology must be combined in effective manner. In this

regard, one potential strategy is greenhouse technology. It offers a means of regulating environmental factors to enhance productivity. On the other hand, manual control of this technology is less efficient, requires labor-intensive manual labor, costs money, and reduces production and energy loss. The development of IoT has made it simpler to monitor and regulate the environment inside the chamber, leading to increased productivity and energy savings (Fig. 10).

Technology with intelligently implanted sensors can be utilized to detect and transmit important aspects of the environment. Temperature, humidity, pressure, and other variables are all typical aspects of the surrounding environment. Singh et al. [123] reported that careful monitoring of soil parameters can facilitate the formulation of educated decisions regarding agriculture, which in turn can lead to an increase in the production of food grains and a reduction in crop loss. Wherever there is a high incidence of drought, water conservation should be a major issue of discussion. The application of intelligent technology in water conservation is one way to reduce the amount of water that is wasted.

In Agriculture, IoT-enabled devices and systems are used to monitor crops, soil conditions, weather, and other environmental factors in real-time, allowing for more efficient resource use, precision farming, and higher yields. The key applications of IoT in agriculture include smart irrigation systems, soil sensors, drone-based crop monitoring, and livestock tracking. These systems enable farmers to make data-driven decisions, optimize water and fertilizer usage, reduce waste, and improve crop health and productivity. Additionally, the challenges of integrating IoT in agriculture, such as the high cost of deployment, lack of technological infrastructure in rural areas, and data privacy concerns. Despite these challenges, IoT in agriculture holds great potential for increasing food production, sustainability, and efficiency, especially as global demand for food continues to rise.

6.8 Smart local, global and social sensing

Consider a situation in which every member of a household possesses a device that supports RFID and, as a result, object monitoring can lead to genuine person tracking. In the IoT, where regular mobile phones may be used to keep tabs on people, this is something that can easily take place. Devices based on sensors can come in a wide variety, and each one has the potential to be utilized for this kind of tracking. This complete process is referred to as local, global, and social sensing, respectively. The object can be tracked on a local, national, and even global scale at any given location, at any given time, and through any available network. RFID tags are indeed the foundation of this tracking system. These tags can be attached to anything objects, people, animals, logistics, etc. For the purpose of tracking anything that contains an RFID tag, an RFID tag reader may be utilized in any and all intermediate stages. An object's position can be identified, and that knowledge can then be utilized to intelligently trigger an alarm, an event, or a particular inference regarding a particular topic.

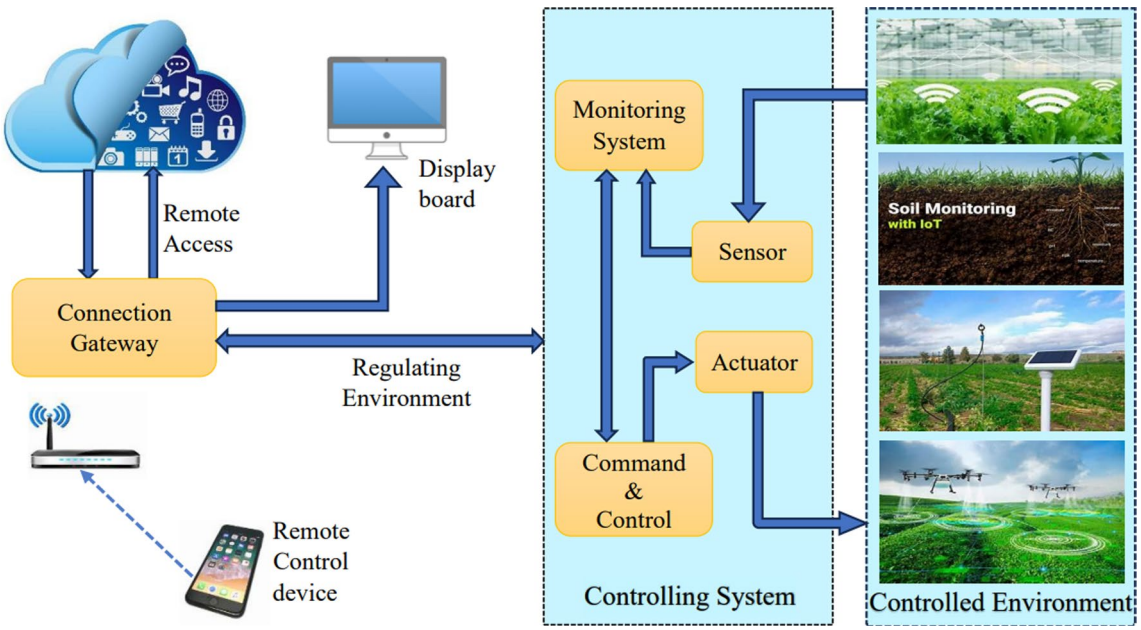


Fig. 10 A working structure of IoT system in agriculture production

6.9 Traffic monitoring

Monitoring the flow of traffic is an essential component of the infrastructure of any and every smart city in the globe. Regular traffic as well as highway traffic both require enough information regarding the support and logistics available on the highway, which in turn enables the system to become self-reliable and intelligent. Congestion on the roadways of any kind will inevitably result in wasted fuel and lost money in the long run. Any kind of foresight regarding traffic will always assist the overall system become better. There will be an increase in the amount of traffic caused by the number of WSN and sensor enabled communications. This will be known as the Traffic Internet of Things (TIoT). The information that is gathered from TIoT can be provided to travelers in the manner described by Zhang et al. [124]. The information about the traffic will be determined by the queuing model on the roadways and the infrastructure of the roads themselves. The user can be provided with information regarding the current status of traffic on all routes as well as the identification of crucial road points. Nonetheless, in order to forestall the kind of terrorist attacks that are common in big cities, the programme that monitors traffic needs to be safe. There are only a few prototype implementations of this kind can be found in [125, 126] and the Smart Santander EU project [127].

7 IoT simulators and tools

The IoT creates good society and well economy is critical and needs high requirements for different applications to guarantee that ideas are acknowledged with most significance factors. The IoT has excellent visions are formed into different measurements uses to utilize smart things, sensors and technologies with certifiable knowledge with correspondence system. In this way, the simulators play an important role to execute and analyze the performance of the proposed approach before deployed in actual environment because it very difficult to deploy and measure the performance in real environment as there are lots of overheads raised due to purchasing, provisioning, software development, and deployment of required resources in the fields.

Modern simulators are becoming more and more common as a result of growing interest in IoT and WSNs [128]. Choosing a trustworthy simulator is a difficult and time-consuming task, especially in the field of WSNs where a variety of complex scenarios and protocols call for network simulators with specialized features. NetworkSimulator-3 (NS-3), BevyWise, COOJA, IBM Bluemix, NetSim, OMNET + +, MATLAB, GloMoSim, and IoTIFY that have been developed to facilitate the simulation of IoT setups. The comparatitve analysis on the basis of their platform, programming language, scalability, network support, network topology, standards, etc. are done and represented in Table 3.

7.1 NS-2/NS-3

A free network simulator that mimics network topologies and communication protocols is called NS-2. Networks that are wired or wireless can be used. Users can use the network animator to play, pause, fast-forward, and end the simulation. Still, it is not a real-time simulation termed a virtual world [129]. NS-3 is an enhanced version of NS-2 and it includes more feathers like parallel and emulation simulation [130].

NS-2 is a widely used simulator for network simulation in various types of networks, including MANETs and VANETs. It offers simulation capabilities for both wired and wireless networks, specifically for routing and multicast protocols. NS-2 is licensed under version 2 of the GNU (General Public License) and is implemented as an object-oriented, discrete event-driven simulator written in C + + and Otcl/Tcl. This versatile tool enables the implementation and evaluation of network protocols like TCP and UDP, as well as the modeling of traffic source behaviors such as FTP, Telnet, Web, CBR, and VBR. Additionally, NS-2 supports the simulation of router queues management mechanisms like Drop Tail, RED, and CBQ, as well as routing algorithms and various other functionalities.

The NS-3 simulation core is a versatile tool that caters to research in both IP and non-IP based networks. However, it is worth noting that the majority of its user base is primarily interested in wireless/IP simulations. These simulations involve the utilization of models for Wi-Fi, WiMAX, or LTE at layers 1 and 2, as well as various static or dynamic routing protocols like OLSR and AODV for IP-based applications. Additionally, NS-3 offers support for a real-time scheduler, which proves beneficial for "simulation-in-the-loop" scenarios where users can interact with real systems.

Table 3 IoT simulations tools

Features	NS-3	BevyWis	eCOOJA	IBM Bluemix	NetSim	OMNET	+M+ATLA	BGloMoSi	MIoTIFY
License	Open	Open	BSD	IBM	Open	Academic	GPL	Open	GPL
Platform Support	Universal	Universal	Universal	Universal	Universal	Tiny OS	Universal	Universal	Universal
Programmi Language	nCg++and Python	C, Python & Java	Java	Java, Node. js, Swift, Go, PHP, Python, & Ruby	Java,HTM & XML	LC++,C	C/C++, HDL, PLC, GPU, .NET, & Java	C& Parsec	Java, Java Script
Scalability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protocol Optimization	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mobile Network Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Network topology	dynamic	dynamic	dynamic	dynamic	dynamic	static	dynamic	dynamic	dynamic
MAC, Routing support and Standards	802.11, LTE, DCF, LRWPAN Wifi, Wimax	MQTT	IPv4, IPv6, 802.15.4	MQTT, HTTP	802.11, CSMA, TDMA, Hybrid	RFID, L3, PHY, MANET	MQTT or REST APIs	CSMA, MACA, TSMA, 802.11, Telnet, FTP	MQTT, HTTP, CoAP, LWM2M
Network Support	6Low, WPAN, DSR, OLSR	Multiple Stipulated N/W	Multicast N/W	Cloud, gateways	Multicast N/W	Multipath ring, Simple tree routing, bypass routing	Multicast N/W	Bellman-Ford, FSR, OSPF, DSR, WRP, LAR, AODV	Cloud, gateways

This functionality allows users to transmit and receive NS-3-generated packets on actual network devices, while NS-3 itself can serve as an interconnection framework to introduce link effects between virtual machines.

7.2 BevyWise

Thousands of IoT devices can be simulated with BevyWise simulator and it is user friendly MQTT simulation tool [131]. It is powerful and simple user interface that makes it easy to add the required devices.

By leveraging the capabilities of Bevywise IoT Simulator, users can gain valuable insights into the performance levels of their MQTT/IoT Applications through comprehensive testing and analysis. The tool's user-friendly interface facilitates the creation of virtual IoT networks and devices, enabling users to simulate various scenarios and assess the behavior of their applications under different conditions. Furthermore, the ability to store simulation data in MySQL and SQLite databases, as well as FLAT files, enhances the versatility and functionality of the IoT Simulator, making it a valuable asset for developers and organizations seeking to optimize the performance of their IoT applications.

7.3 COOJA

COOJA, a network simulator based on the Contiki OS, enables the emulation of actual hardware platforms [132]. Focusing on network behavior, COOJA serves as an application of the Contiki OS. It has the ability to simulate wireless sensor networks without the need for specific motes. COOJA supports various standards including TR 1100, TI CC2420, Contiki-RPL, IEEE 802.15.4, uIPv6 stack, and uIPv4 stack.

The COOJA simulator has four different propagation models. The first model works with an ideal transmission range disk and is called the constant loss Unit Disk Graph Medium (UDGM). Data packets are sent to the motes inside this transmission disk; no packets are sent to the motes outside of it. An expansion of the constant loss UDGM, the second model, distance loss UDGM, accounts for radio interference. According to this model, there is a probability for packets to be transmitted (called success ratio TX) and received (called success ratio RX). Propagation delays are introduced for the radio links in the third model, called Directed Graph Radio Medium (DGRM). The fourth path loss model is the multipath Ray-tracer Medium (MRM), which computes receiver power using ray tracing techniques like the Friis formula. Diffraction, reflections, and refractions along the radio links can also be calculated by MRM.

7.4 IBM Bluemix

IBM created Bluemix, a platform as a service (PaaS) for creating, executing, deploying, and managing cloud applications. IBM Bluemix is a cutting-edge cloud platform that gives access of the company's IoT Platform without the need of a physical device [133]. Users can monitor and analyze simulated data using the built-in web console dashboards, and then use the information to create and improve already available applications. The program offers a number of features for working with, storing, and even interacting with social media data. IBM IoT platform facilitates the seamless communication and retrieval of data from interconnected devices, sensors, and gateways. Through the utilization of "recipes", the process of connecting devices to the IoT cloud is simplified. Applications are able to interact with IoT devices in realtime using REST APIs, enabling them to access and utilize the data collected based on user commands. This service offered by IBM IoT serves two primary objectives. Firstly, it ensures the secure connection of devices to the cloud by providing verified instructions, or "recipes", for establishing connections with devices, sensors, and gateways from various partners and individuals. Secondly, it enables the development of applications that can effectively communicate with devices. The communication between devices and the cloud is facilitated through the MQTT protocol, allowing for the seamless transmission of data. For instance, sensors can continuously gather and transmit humidity readings, which can then be accessed and analyzed through REST and real-time APIs for further processing.

7.5 NetSim

NetSim serves as a network simulation tool enabling the creation of network scenarios, traffic modeling, protocol design, and network performance analysis. It is a robust network simulator primarily utilized for modeling IoT systems. The sensors within NetSim are abstract, allowing for versatility in the type of sensor or embedded device used. These sensors are designed to detect physical properties or random fields such as temperature, pressure, etc. Once the sensors detect data, they transmit this information in the form of 'IP Packets' with user-defined sizes and interpacket arrival times. NetSim

encompasses various network technologies including 6LoWPAN gateway, 802.15.4 MAC/PHY, RPL, among others, to simulate the transmission of IP packets across an IoT network. Notably, the focus of NetSim lies in the transmission of IP packets rather than the actual application payload or sensed data being sent, excluding data storage and analytics of the payload.

NetSim represents IoT as a Wireless Sensor Network (WSN) connecting to an Internetwork through a 6LowPAN Gateway. The 6LowPAN Gateway features two interfaces: a Zigbee (802.15.4) interface for WSN wireless connectivity and a WAN Interface for external Internetwork connection. Within the WSN, sensors can generate measurement packets that are queued in a packet buffer before being transmitted wirelessly either directly or through hops to a gateway. The gateway then forwards the packet over the internet to a server. Wireless links in NetSim support various propagation models, with ad hoc routing facilitating multi-hop communication. The MAC/PHY layer protocol supported is 802.15.4, which operates in either Beacon Enabled or Disabled Mode for packet transmission. In Beacon Enabled Mode, nodes utilize a slotted CSMA/CA algorithm for packet transmission, while Unslotted CSMA/CA is used otherwise.

This simulation tool is scalable to accommodate hundreds of nodes and supports diverse sources and destinations. Through NetSim, users can analyze performance metrics such as loss, delay, and throughput, among others, to evaluate the efficiency of the simulated IoT network.

7.6 OMNET++

OMNeT++ is a versatile, modular, component-based C++ simulation library and framework designed primarily for constructing network simulators. It enables discrete event simulation of computer networks and other distributed systems [134]. The project, based on C++, aims to bridge the gap between research-focused simulation tools and costly commercial options like OPNET, now under Riverbed Technology [135]. One of the key features of OMNeT++ is its support for hierarchical organization of simulation models, with no restriction on the number of layers. This modular design enhances clarity and simplifies working with the simulation system. Additionally, the framework allows visualization of processes within the virtual network through a graphical user interface.

OMNeT++ facilitates the simulation of large networks and incorporates HiL integration by default. The primary challenge in connecting physical devices lies in integrating them with the simulation environment's scheduling mechanism. To address this, OMNeT++ offers a customizable real-time scheduler. An illustrative example is the socket demonstration included in the OMNeT++ installation, showcasing how external applications can interact with the simulation environment. By extending the real-time scheduler, a TCP/IP socket is opened on port 4242, enabling users to connect via a web browser. The GUI displays the corresponding HTTP request, demonstrating data transfer over the internet to the web server and back to the client. The use of simple TCP/IP sockets provides flexibility, with two Raspberry Pis serving as interfaces for communication on the sender and receiver ends. Each Raspberry Pi establishes a connection to the OMNeT++ simulation environment via Ethernet. Given its focus on modeling large networks, OMNeT++ is well-suited for simulating future smart environments.

7.7 MATLAB/Simulink

The MathWorks program MATrix LABoratory (MATLAB) has a graphical user interface. The interface is called Simulink [136]. The system has the capability to retrieve and preprocess both real-time and stored data by utilizing its integrated interfaces to cloud storage, relational and nonrelational databases, as well as protocols like REST, MQTT, and OPC UA. One interesting IoT module in MATLAB is to create and test smart devices in addition to gathering and analyzing IoT data on the cloud. IoT platforms gather information from smart devices, compile it online, and perform real-time analysis. Researcher can use this information to create prototype algorithms and run them in the cloud for extracting patterns and algorithms.

Simulink, an extension to MATLAB, offers a graphical interface for modeling and simulating systems. A key benefit of using Simulink is its capability to model nonlinear systems, a task that cannot be accomplished with a transfer function. Additionally, Simulink allows users to specify initial conditions, providing more flexibility in system analysis and design.

7.8 GloMoSiM

Software for parallel programming is commonly developed using C and Parsec. One such software is the Global Mobile Information System Simulator (GloMoSim) [137]. GloMoSim offers various MAC protocols, including CSMA, MACA, and

802.11, which can be utilized in simulations. The simulator is capable of emulating networks with up to a thousand nodes, connected through a diverse range of communication capabilities. The features include multicast, one-way communication via satellite broadcasts, multihop wireless communication with ad-hoc networking, and standard Internet protocols. There are three different routing protocols included in GloMoSim. Ad hoc OnDemand Distance Vector (AODV) is the first protocol, based on an earlier draft (draft-ietf-manet-aodv-03.txt) from the Internet Engineering Task Force [138]. When AODV detects a link break, it assumes that the MAC protocol notifies the routing protocol. MAC protocols with this feature include IEEE 802.11 and MACAW. In IEEE 802.11, for example, a signal is sent to the routing protocol if no Clear to Send (CTS) is received following a Request to Send (RTS) and no acknowledgement (ACK) is received following retransmissions of a unicasted packet. Fisheye State Routing, or FSR, is the second routing protocol used in GloMoSim. The foundation of FSR is the idea that as a router gets farther (in hops) from the network, its decision-making regarding packet forwarding is less affected by changes in the topology of the network region. FSR is a variation of GSR (Global State Routing), in which a node exchanges individual link state table entries at varying rates according to the link's distance from the source, as opposed to exchanging all of its information at regular intervals. As a result, not all nodes' information is contained in each update message. By giving closer nodes more information exchanged about them more often than farther nodes, it minimizes the size of update messages.

The third routing protocol in GloMoSim is WRP (Wireless Routing Protocol), which is a proactive protocol that maintains routing information through triggered and periodic updates. When a node successfully receives an update message, it transmits an acknowledgment back to the sender.

GloMoSim leverages Parsec's parallel discrete-event simulation capability. The integration of node aggregation technique in GloMoSim greatly enhances the simulation performance. Additionally, GloMoSim incorporates a platform-independent Visualization Tool developed in Java. This tool facilitates debugging and verification of models and scenarios, enables pausing, resuming, and stepping through execution, displays packet transmissions, showcases mobility groups in distinct colors, and presents statistical information.

7.9 IoTIFY

IoTIFY specializes in developing a cloud-based intelligent IoT system simulation platform. This platform allows for the simulation of large-scale and realistic deployments of IoT devices. With the increasing number of IoT devices being connected to the internet every day, IoT platforms are constantly evolving to provide more advanced features for data ingestion, analysis, and monetization. However, developing applications on different IoT platforms has become more challenging due to the complexity of devices and the introduction of concepts like digital twins.

To address these challenges, IoTIFY offers a scalable and flexible IoT device simulation platform that seamlessly integrates with IoT Application Ennoblement Platforms. This enables developers to rapidly create, test, and deploy IoT solutions that can handle millions of devices at scale. Additionally, IoTIFY supports a wide range of protocols, which are continuously updated to keep up with the evolving IoT landscape. The current version of IoTIFY's SaaS platform supports protocols such as MQTT, HTTP, CoAP, LWM2M, UDP, and TCP.

Scalability is a major concern in IoT, as millions of sensors and thousands of gateways can connect to an IoT platform at any given time. The dynamic nature of connectivity media introduces challenges such as packet loss, latency, and outoforder delivery. IoTIFY addresses these challenges by ensuring that its platform can handle such scenarios and is built on the same principles used to build scalable cloud platforms. Similar to real-world devices, each simulated IoT device in IoTIFY has its own temporary and persistent memory. These devices can store meta-information in their memories, which can be accessed and modified through external APIs or user interfaces.

The detailed analysis of aforementioned simulators are presented in Table 3. It helps in comparative study and analysis for selection of required simulator which can fulfill the researcher demands for their simulation.

Further, Cisco Packet Tracer [139] is an invaluable simulation tool for understanding and teaching IoT concepts, effectively bridging the gap between traditional networking and emerging IoT technologies. Its user-friendly drag-and-drop interface allows users to easily design and visualize complex network topological, integrating various IoT devices such as sensors and smart appliances. Packet Tracer supports key IoT protocols like MQTT and HTTP, enabling users to simulate real-world data flows and device interactions in a dynamic environment. The ability to engage with simulated devices in real time enhances the learning experience, providing immediate feedback that deepens understanding. While the tool excels in offering a hands-on learning experience, it does have limitations regarding the realism of complex IoT scenarios and lacks some advanced functionalities found in specialized IoT simulation

platforms. Nonetheless, Packet Tracer remains a vital resource for educators and professionals alike, fostering practical skills and knowledge essential for navigating the evolving IoT landscape.

ThingsBoard [140] is a powerful open-source IoT platform that facilitates the development and deployment of IoT applications through its robust simulation capabilities. Designed to handle device management, data collection, and visualization, ThingsBoard allows users to simulate various IoT devices and their interactions within a cohesive environment. The platform supports multiple communication protocols, including MQTT, CoAP, and HTTP, enabling seamless integration with real and simulated devices. Users can create dashboards to visualize real-time data, monitor device statuses, and analyze historical trends, making it an invaluable tool for both learning and practical applications. The ability to simulate device behavior and data flows helps developers prototype IoT solutions efficiently and test various scenarios before physical deployment. However, while ThingsBoard offers comprehensive simulation features, its complexity may present a learning curve for new users. Overall, ThingsBoard is an excellent resource for educators, developers, and researchers looking to explore IoT applications, providing a versatile platform for innovation and experimentation in the rapidly evolving IoT landscape.

Each simulator has its strengths and is suited for different IoT applications. NS-3 and OMNeT + + excel in network protocol simulations, while Cooja is better for low-power sensor networks. ThingsBoard is ideal for cloud-based, data-centric IoT applications. Choosing the right simulator depends on the the applied application.

8 Challenges

The integration of IoT-based systems into various aspects of human existence, coupled with the multitude of technologies facilitating data transfer among embedded devices, has presented a complex landscape fraught with concerns and challenges. These problems present a challenge for the developers of IoT in a society that has advanced in terms of its use of smart technology. Challenges and the requirement for more powerful IoT systems are developing in tandem with the advancement of technology. So, those who work on the IoT need to anticipate new problems and work to find solutions for them. From a long-term perspective, we identify the following challenges.

8.1 Resource management

The immense number of involved objects, the complexity and variety of deployment conditions, and the restricted object capacity are a few examples of the numerous aspects that contribute to the difficulties of management for the future IoT. It is required to establish comprehensive methods for analyzing resources, quantitative theories for assessing resources, and exact procedures for allocating resources and scheduling them.

8.2 Massive gathered information

It is expected that the IoT systems would have millions or even billions of objects. Every thing should give off a signal that conveys information about itself. It is important to obtain this information. The proliferation of IoT devices results in an enormous amount of data being collected as a result. As a result of the accumulation of a great deal of data, a number of issues have been brought to light. The issues at hand are those of transmission, storage, and processing. Because of transmission issues, it is necessary to send the data from all of the things in real time, and there is no assurance that this will be successful [141, 142]. This is because there may be a problem with the available bandwidth, which is essential for the transmission of this information but may not be available. It is common knowledge that the information moves along a path beginning with the items and ending with the web application that controls it. This journey takes place. There is a possibility that this journey will involve further bandwidth bottlenecks, which indicates that the requisite bandwidth will be unavailable for the majority of the trip. The number of media that is necessary to both store and back up this information is a challenge for data storage, as a result of which there is a problem with data storage. The processing operation indicates that the information pertaining to the things should be handled by IoT web apps in order to identify the control actions for each individual item. It is recommended that this handling procedure be performed in real time [143, 144].

8.3 Quality assurance

The evolution of the internet is expanding to encompass all aspects of the physical world, resulting in a wide range of applications with diverse needs in terms of bandwidth, security, timeliness, and reliability. For instance, consider the case of factory surveillance: to monitor a manufacturing process comprehensively, a combination of sensors and video cameras is utilized. Sensor networks demand precise data transmission with minimal bandwidth, while video streaming necessitates high bandwidth but can tolerate lower accuracy. Even seemingly simple tasks like synchronizing sensor data with video footage require a substantial level of coordination between wired and wireless communication systems.

8.4 IoT and TCP challenge

The infrastructure supporting the IoT is analogous to the backbone supporting the Internet. As a result, the transfer of the data will make use of either the TCP or UDP protocols as the transmission mechanism. The UDP protocol cannot be relied upon, which is precisely the reverse of what we want to achieve. As a result, TCP ought to be used as the transport layer for IoT systems. The TCP has a greater number of issues in relation to the IoT devices. These challenges include connection setup, congestion control, and data buffering. The necessity to send only a little amount of data from one device to another necessitates that most of the time in IoT systems the connection setup is not even taken into consideration. In addition, the majority of the communication resources in IoT are things like sensors, RFID tags, and personal digital assistants, all of which are unable to deal with the data necessary for setting up a connection. Congestion control is a difficult problem in wireless networks, which are also the medium for IoT devices. Also, in the event that only a little amount of information is being exchanged between two IoT items, the congestion management data is not obligatory. It is necessary for there to be data buffering in TCP both at the source, where the re-transmission process occurs, and at the destination, where the ordering process occurs. It is expensive for battery-free devices such as RFID tags to go through the processes of data buffering. As a result, the conclusion is that UDP is not appropriate, and that TCP has additional issues, despite the fact that it is typically unnecessary for IoT use cases. Several researchers investigated the properties and behaviors of the information that was transmitted inside IoT items such as WSN and RFID systems [141–143].

8.5 Real time objects detection

As we focus on the IoT system, we find two unclear questions: how we can define each thing, and how we can obtain the information about it. It is only logical for us to respond by employing the use of RFID, EPC, or UID technology. However, these technologies come with a number of drawbacks, the most notable of which being their radiation, privacy, and violation risks, as well as the inconvenient nature of their information update processes. In addition, defining all of these technologies in relation to the various objects in the world in such a short amount of time is not a simple task.

8.6 Extensive involvements

In contrast to the majority of devices on the Internet, which are owned by a few number of extremely large Internet service providers (ISPs), the majority of objects in the future smart universe will be held by relatively insignificant institutions and individuals. A user can serve in multiple roles simultaneously, including that of customer, object designer, and service provider. Due to the fact that the relationships between the many stakeholders will grow considerably more complex, and services will be supplied from a variety of locations, approaches for the sharing of information that are both resilient and flexible are required.

8.7 Energy efficient sensing

Multiple sensing modalities have competing demands that must be simultaneously met for efficient heterogeneous sensing of the urban environment. Network traffic, data storage, and energy use are all impacted by this. Significantly, this includes both stationary and mobile sensing infrastructure [145] in addition to random and continuous sampling.

For data collection and modeling that efficiently utilizes the temporal and spatial properties of the data, both in the transform domains that are related to the sensing domain, a generalized framework is needed.

As a crucial element for the residents' health and quality of life, urban noise mapping, for instance, requires the continuous collection of noise levels using batterypowered nodes, fixed infrastructure, and participatory sensing [145].

Reduced signal measurements are possible with compressive sensing, all without compromising the signal's precise reconstruction. From a limited number of projections onto a second basis that is incoherent with the first, a signal sparse in one basis may be recovered [146].

Finding the smallest l1-norm coefficient vector that agrees with the measurements allows us to reduce the problem to finding sparse solutions. This affects network traffic, sensor distribution, and data compression in the context of ubiquitous sensing. By using synchronous communication, compressive wireless sensing (CWS) lowers the transmission power of individual sensors [147] and sends noisy data sample projections to a central location for aggregation.

8.8 Incentive frameworks

Since most services are generated, shared, and purchased by individuals, the quality of those services will vary greatly due to the wide range of information, professional experience, and skill levels possessed by the individuals who develop them. It is vitally necessary to design suitable incentive frameworks in order to motivate individuals to build services that are of a high quality, share premium services on a large scale, and preserve the security and privacy of service customers.

8.9 Security and privacy

Security and privacy are significant obstacles that need to be overcome before there can be widespread application of IoT. Protecting the IoT, however, is a job that is nearly impossible to accomplish for the following reasons. A significant portion of IoT networks make use of lightweight wireless transmissions that are susceptible to attacks [148], and this is in addition to the fact that objects themselves are fragile gadgets. The fact that objects are dispersed across a variety of contexts and designed to interact with a variety of devices makes the design of protection mechanisms more difficult. Because global connectivity and navigability are essential components of IoT, attacks originating in local areas are likely to cause impacts on the system as a whole. There is a need for the development of innovative strategies that are appropriate for usage in IoT applications. These strategies should include user anonymity, failure recovery, attack resilience, access control, and data encryption.

8.10 Trust

It is unavoidable that conflicts and animosity in human civilization will have an impact on the way in which devices in the future IoT will interact with one another. It is necessary for there to be systems of trust in order for peers to be able to differentiate between potentially beneficial relationships and potentially harmful partners. Yet, this is not something that can be readily accomplished because there is the risk of having one's identify stolen, there is no way to know for sure what an object's status is, and there are conflicts among human communities.

8.11 Data confidentiality

Data confidentiality in IoT is crucial as these devices often collect and transmit sensitive information, such as personal, financial, and health data. Ensuring confidentiality involves protecting data from unauthorized access during transmission and storage. However, many IoT devices lack robust security measures like strong encryption, making them vulnerable to breaches and interception. To maintain confidentiality, secure communication protocols, proper encryption techniques, and strong authentication must be implemented across IoT networks, ensuring that only authorized users and systems can access sensitive data. Without these safeguards, IoT systems are at high risk of privacy violations and data theft.

Smart local, global, and social sensing in IoT faces a range of technical and ethical challenges. Solutions must focus on enhancing the integration and scalability of sensing devices, ensuring data privacy and security, improving data accuracy, and addressing energy constraints. Overcoming these challenges will unlock the full potential of IoT sensing for applications in industries like agriculture, healthcare, smart cities, and environmental monitoring.

9 Future directions

IoT networks may be able to reach every location by 2030 thanks to the 6G wireless communications standard [149]. Satellite-based communications are viewed as a fortunate means of satisfying the demands of IoT services in the 6G era. Seamless coverage and interconnection are essential for IoT applications like geo-location live tracking, eco-monitoring, and disaster prediction. Nevertheless, the requirements of 6G IoT for wide coverage and improved reliability are not met by geostationary IoT networks such as Sigfox, LoRa, and NB-IoT [150]. However, satellite-based systems are incredibly dependable, accessible from anywhere, and capable of functioning in any type of weather. Thus, in order to meet new IoT requirements, satellite systems must be integrated into 6G networks. It has also been suggested that hybrid satellite-terrestrial relay network (HSTRN) technology, which uses terrestrial stations as relays to forward and improve satellite messages to the recipients, can offer completely dependable communication in both highand remote-lying areas [151, 152].

To overcome the obstacles related to scalability, ultra-low-power consumption, minimal latency, privacy preservation, personalization, responsiveness, and universal coverage, even in the most isolated regions worldwide, the concept of 6G communications envisions a globally interconnected network of satellites and aerial platforms driven by AI and big data [153–155]. In this section, we present the forefront research directions that aim to address the aforementioned challenges.

The development of low-cost, dependable, and scalable networks is necessary to meet the demands for high spectral efficiency and wide connectivity [156]. Nextgeneration multiple access (NGMA) systems must be implemented because the multiple access techniques employed in these networks negatively affect their efficacy. In 1G to 4G cellular networks, orthogonal multiple access (OMA) systems will be insufficient to manage the expected surge in data traffic and device volume. Resource allocation should be done efficiently in order to overcome this obstacle. Optimizing resource allocation strategies contributes to improved network performance and coverage. To manage the rapidly increasing data traffic from IoT devices, numerous studies have concentrated on creating multiple access mechanisms [157]. Non-orthogonal multiple access (NOMA) has garnered a lot of attention as a multiple access strategy. Numerous factors indicate that NOMA is better than OMA, such as lower network latency, faster cell-edge performance, more relaxation at channel feedback, and higher spectrum effectiveness [158].

The fact that the upcoming wave of IoT requires a large number of wireless devices to be connected to a network creates numerous research and deployment challenges [159]. Since rate-splitting multiple access (RSMA) enables sequential decoding to realize the multiple access network's full capacity range, it is thought to be a workable approach. Compared to NOMA, it is a more adaptable and effective transmission method. RSMA is especially useful in reducing collisions in IoT sensor networks that employ random access (RA) techniques [160]. RSMA has the potential to be used in massive IoT scenarios with a large number of connected devices, in addition to its use in achieving high throughput [159].

Reconfigurable intelligent surfaces are another exciting technological advancement (RIS). RIS has emerged as a critical transmission mechanism for numerous IoT networks [161]. A vast array of low-cost passive antennas make up RIS. Pin-diodes or var-actors, which can intelligently arrange phase shifters and adjust incoming signals to desired frequencies, control the reflecting properties of antennas [162]. Through a different direction of reflection of the input electromagnetic wave, the phase is changed to affect the radio propagation conditions. The maximum user data rate may be raised by the RIS. Owing to these advantages, RIS-enhanced networks have been the subject of extensive research.

Unmanned aerial vehicles (UAVs) are among the technologies that have drawn a lot of attention in recent decades due to their potential to address long-distance and universal coverage challenges [163]. UAVs can establish better Line-of-Sight communication and avoid signal blocking and shadowing than cellular communications because they are more versatile, portable, and adaptable in three-dimensional space. In terms of technology, UAVs hold promise for realizing truly widespread connectivity for IoT systems. Nevertheless, the extensive cost and limited economic benefits associated with constructing infrastructure in remote and challenging locations pose significant challenges for terrestrial and UAV networks. Consequently, these networks are incapable of adequately providing coverage for the wide range of IoT devices (IoTDs) found in densely populated urban areas as well as remote and uninhabited regions. This coverage deficit affects various sectors such as smart cities, smart industries, emergency tracking, and environment management [164].

The satellite and aerial-integrated network (SAIN) paradigm holds the potential to utilize satellite and UAV networks as an interconnected solution, enabling universal coverage, a multitude of connections, and high-speed

communications for IoTDs. This approach aims to offer a diverse range of services to IoTDs by leveraging the capabilities of both satellite and aerial networks. By integrating these networks, SAIN can effectively address the challenges of providing widespread coverage, accommodating a large number of connections, and facilitating fast and reliable communication for IoTDs [157]. Furthermore, neither UAVs nor Low Altitude Platform Stations (LAPSs) in general are able to handle scenarios requiring extensive coverage. In the meantime, the wider coverage that the High Altitude Platform Station (HAPS) provides due to its elevated vertical position has made it more and more important. Its inexpensive cost, delay sensitivity, quick development and deployment, and massive capacity set it apart from other communication systems serving a wide area [165]. The XAPS paradigm, which employs a single HAPS as a macro aerial base station to provide broad coverage and several LAPSs as small aerial base stations to enhance connectivity in crowded areas, remote areas, and other difficult environments, is therefore being modified. Additionally, cluster-NOMA (C-NOMA) can be combined with the XAPS model, which divides HAPS terminals into multiple groups, to increase network capacity and performance. This allows for the application of C-NOMA within each cluster and OMA between them. When compared to NOMA, the decoding difficulty could be significantly reduced by using C-NOMA, which has fewer terminals in each cluster [166]. This simplifies the end-user experience and enables more efficient use of the available spectrum.

Fog computing offers distributed and real-time solutions that can be integrated into newly installed networks to address the low-latency challenge [167]. Research in this field may concentrate on creating techniques for distributed, real-time computing in fog environments and investigating new uses for fog computing [168]. Furthermore, to give the necessary awareness of the QoS, machine learning and optimization algorithms can be implemented at the edge nodes/gateways and servers. Due to the dynamic number of nodes accessing the system, particularly mobile nodes, the load on the computing servers is time-varying and nondeterministic. Determining when and how the nodes choose to shift the processing to the edge server in order to offload the task is a challenging problem [169]. Because edge computing installs smart services and on-edge nodes autonomously, it is frequently referred to as the "final mile"in AI. Numerous edge devices-miniaturized, dispersed, and low-power can perform precise artificial intelligence (AI) or work in tandem with other devices for a range of applications, including IoT node networks [170]. In order to meet the demands of data transfer over networks for reliability and minimal latency, the intelligence for such services can be dispersed to the edge.

The Space-Air-Ground IoT (SAG-IoT), where the advantages of aerial vehicles and satellite infrastructure are combined to improve network coverage, things get more complicated [171]. Task offloading and resource scheduling face greater challenges in this heterogeneous environment because the real SAG-IoT operates in non-deterministic spatiotemporal-dynamic scenarios [172]. Because of network variability and heterogeneity characteristics, the space–time-varying behaviors of the node task reception, transmission, and handling are random processes within a time slot rather than a snapshot of the system when looking at long-term performance.

Additionally, since offloading jobs depletes SAG-edge and cloud servers, it's critical to allocate them equitably because different network segments have distinct computational requirements and are subject to a variety of constraints [173]. Real-time optimization algorithms and reinforcement learning models have the potential to effectively manage the allocation of computing resources at the local level, aerial vehicles, and edge nodes. This coordination aims to gradually reduce the overall operating costs of the network [174, 175]. By decomposing the problem into its constituent elements and implementing strategies such as local resource allocation and channel reuse, the challenge can be successfully addressed through the utilization of Lyapunov optimization techniques [173, 176].

Kathole et al. [177] examine the distinct security challenges that arise with the advent of next-generation mobile networks. Among the critical issues identified are an expanded attack surface resulting from the increasing number of connected devices, intensified concerns regarding data privacy due to extensive data collection practices, vulnerabilities linked to network slicing, and risks associated with the complexities of supply chains. Moreover, the presence of insider threats is highlighted as a considerable risk, particularly given the growing number of stakeholders involved in the management of these networks. To address these challenges, the authors advocate for the adoption of advanced encryption methods to safeguard data transmissions, the utilization of artificial intelligence for real-time threat detection, and the implementation of rigorous access controls to mitigate insider threats. They also stress the necessity of collaboration among industry stakeholders to create standardized security frameworks and best practices. Ongoing risk assessments and proactive updates to security protocols are deemed crucial for adapting to the dynamic threat landscape presented by 5G and 6G networks.

The emergence of the IoT has ushered in a new age of unparalleled connectivity, with projections indicating that approximately 80 billion smart devices will be operational by the conclusion of 2025 [178]. These devices enable a wide array of intelligent applications, significantly improving quality of life and operational efficiency in numerous sectors. The

IoT encounters considerable challenges and critical issues concerning privacy and security, primarily stemming from the extensive network of interconnected devices that collect and transmit sensitive information. A significant issue is data privacy, as IoT devices frequently accumulate personal data without obtaining explicit consent from users, which raises the risk of unauthorized access and potential misuse of such information. Moreover, numerous IoT devices are deficient in robust security features, rendering them susceptible to various forms of attacks, including malware infiltration and data breaches. The lack of standardized security protocols across diverse IoT platforms further complicates the establishment of effective security measures. Ensuring the integrity of data is vital, as compromised information can lead to flawed decision-making in essential applications. The interconnected nature of IoT amplifies the attack surface, necessitating secure communication channels to safeguard against threats such as Distributed Denial of Service (DDoS) attacks. As IoT implementations expand, the complexity of managing security escalates, requiring adaptive and innovative solutions. Additionally, organizations must navigate a myriad of regulations pertaining to data protection and privacy, which can be particularly challenging in this swiftly changing environment. Addressing these concerns is crucial to safeguarding the safety and privacy of IoT systems, necessitating collaboration among manufacturers, developers, policymakers, and users.

Machine Learning (ML) is a powerful IoT and smart automation tool. Machine learning holds significant promise for enhancing enterprise systems that utilize the IoT through the facilitation of automation and informed decision-making. By integrating ML methodologies with IoT-generated data, organizations can uncover profound insights and derive valuable information from the extensive sensor data produced by IoT devices. The rapid processing capabilities of ML models equip IoT systems with enhanced knowledge, thereby optimizing their operational efficiency and practices. ML has emerged as a pivotal technological advancement in tackling various challenges associated with IoT, including the protection of smart systems and the identification of anomalous activities. The enhancement and automation of services provided by enterprise systems are crucial for addressing these challenges and attracting a broader customer base. Considerable advancements have been made in the research surrounding ML applications within enterprise architectures that incorporate IoT, highlighting the potential benefits of ML in various sectors. By utilizing ML within IoT-based enterprise systems, users can achieve comprehensive analytics and create highly sophisticated IoT applications. Future research is essential to develop an ML-driven security framework aimed at protecting enterprise architectures from potential vulnerabilities. By leveraging the complementary strengths of ML and IoT, organizations can unlock new avenues for establishing more efficient, secure, and adaptable enterprise ecosystems. Looking ahead, we intend to design and implement a machine learning-based Intrusion Prevention and Detection System (IPS/IDS) specifically for Industrial IoT environments.

10 Conclusion

In recent years, there has been a significant shift in the Internet paradigm. This transformation can be attributed to the remarkable progress in sensor and hardware technologies, which have facilitated the integration of sensors into various physical devices. Consequently, these devices able to communicate with one another and eliminating the need for human intervention. Thus, the growing use of IoT devices and technology has led to significant transformations in our daily lives. IoT innovations have attracted global attention among researchers and developers. IoT developers and academics collaborate to advance technology and benefit society. In this survey paper, we presented key components of the IoT paradigm, along with its protocols, technologies, and applications. A generic architecture is discussed in detail to highlight the layers and protocols applied at each layer. Further, important application areas are also highlighted, including those in which IoT developers and academics work. Challenges and future directions are briefed that help in improvement and evolution. The existing IoT fields has potential for significant improvements in semantics and security. Future works may explore the development of domain-specific or independent architecture. This initiative aims to establish a new IoT-based architecture and contribute to research in our IoT community.

Author contributions Anita wrote and reviewed the manuscript text.

Data availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Ashton, K.: That 'Internet of Things' Thing. RFID Journal 1999
2. Bru¨gge F, Hasan M, Kulezak M, Lueth KL, Pasqua E, Sinha S, Wegner P, Baviskar K, Taparia A. State of iot – spring 2023. Technical report 2023. https://iot-analytics.com/product/state-of-iot-spring-2023/
3. Choosing an App Engine Environment—App Engine Documentation—Google Cloud Platform. https://cloud.google.com/appengine/docs/the-appengine-environments Accessed 04 Nov 2016.
4. EC2 Instance Types – Amazon Web Services (AWS). https://aws.amazon.com/ec2/instance-types/. Accessed 27 Jan 2017.
5. Intro to Microsoft Azure — Microsoft Azure. https://azure.microsoft.com/en-in/documentation/articles/fundamentals-introduction-to-azure/. Accessed 04 Nov 2016.
6. IBM Cloud Computing for Builders & Innovators. http://www.ibm.com/cloud-computing/. Accessed 04 Nov 2016.
7. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Futur Gener Comput Syst. 2009;25(6):599–616.
8. Hendriks S. Internet of Things: how the world will be connected in 2025, 2016
9. Sadeghi-Niaraki A. Internet of Thing (IoT) review of review: bibliometric overview since its foundation. Futur Gener Comput Syst. 2023;143:361–77. https://doi.org/10.1016/J.FUTURE.2023.01.016.
10. Said O, Masud M. Towards internet of things: survey and future vision. International Journal of Computer Networks. 2013;5(1):1–17.
11. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of things: vision, applications and research challenges. Ad Hoc Netw. 2012;10(7):1497–516. https://doi.org/10.1016/J.ADHOC.2012.02.016.
12. Guth J, Breitenbucher U, Falkenthal M, Fremantle P, Kopp O, Leymann F, Reinfurt L. A detailed analysis of IoT platform architectures: Concepts, similarities, and differences. IoT 2018;9789811058608:81–101
13. C˘olakovi´c, A., Had˘zali´c, M.: Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Comp Netw 2018;144:17– 39. https://doi.org/10.1016/J.COMNET.2018.07.017
14. Wytrebowicz J, Cabaj K, Krawiec J. Messaging protocols for IoT systems—a pragmatic comparison. Sensors. 2021;21(20):6904.
15. Gerodimos A, Maglaras L, Ferrag MA, Ayres N, Kantzavelou I. IoT: communication protocols and security threats. IoT CyberPhys Syst. 2023;3:1–13. https://doi.org/10.1016/J.IOTCPS.2022.12.003.
16. Domınguez-Bolan˜o T, Campos O, Barral V, Escudero CJ, Garcıa-Naya JA. An overview of IoT architectures, technologies, and existing open-source projects. IoT 2022;20:100626. https://doi.org/10.1016/J.IOT.2022.100626
17. Abdulkareem NM, Zeebaree SRM, Sadeeq MAM, Ahmed DM, Sami AS, Zebari RR. IoT and cloud computing issues, challenges and opportunities: a review. Qubahan Acad J. 2021;1(2):1–7. https://doi.org/10.48161/QAJ.V1N2A36.
18. Yan L, Zang Y, Laurence TY, Ning H. The internet of things: from RFID to the next-generation pervasive networked systems, Auerbach Publications, 2008, p. 318.
19. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. IEEE Internet Things J. 2014;1(1):22–32. https://doi.org/10.1109/JIOT.2014.2306328.
20. Khajenasiri I, Estebsari A, Verhelst M, Gielen G. A review on internet of things solutions for intelligent energy control in buildings for smart city applications. Energy Procedia. 2017;111:770–9. https://doi.org/10.1016/J.EGYPRO.2017.03.239.
21. Technologies. https://www.ti.com/technologies/overview.html. Accessed 23 Nov 2022.
22. Liu T, Yuan R, Chang H. Research on the internet of things in the automotive industry. Proceedings 2012 International Conference on Management of e-Commerce and e-Government, ICMeCG 2012, 230–233. https://doi.org/10.1109/ICMECG.2012.80
23. Alavi AH, Jiao P, Buttlar WG, Lajnef N. Internet of things-enabled smart cities: state-of-the-art and future trends. Measurement. 2018;129:589–606. https://doi.org/10.1016/J.MEASUREMENT.2018.07.067.
24. Fang S, Xu LD, Zhu Y, Ahati J, Pei H, Yan J, Liu Z. An integrated system for regional environmental monitoring and management based on internet of things. IEEE Trans Indust Inf. 2014;10(2):1596–605. https://doi.org/10.1109/TII.2014.2302638.
25. Cheng Y, Li X, Li Z, Jiang S, Li Y, Jia J, Jiang X. AirCloud: a cloudbased air-quality monitoring system for everyone. In: Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems, Association for Computing Machinery (ACM), (2014), pp. 251–265.
26. Weber RH. Internet of Things—new security and privacy challenges. Comput Law Secur Rev. 2010;26(1):23–30. https://doi.org/10.1016/J.CLSR.2009.11.008.
27. Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K. Security challenges in the IP-based internet of things. Wireless Personal Commun. 2011;61(3):527–42. https://doi.org/10.1007/S11277-011-0385-5.
28. Liu J, Xiao Y, Chen CLP. Authentication and access control in the Internet of things. Proceedings 32nd IEEE International Conference on Distributed Computing Systems Workshops, ICDCSW 2012, 588–592, 2012. https://doi.org/10.1109/ICDCSW.2012.23
29. Kothmayr, T., Schmitt, C., Hu, W., Bru¨nig, M., Carle, G.: DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Netw **11**(8), 2710–2723 (2013). https://doi.org/10.1016/J.ADHOC.2013.05.003
30. Luk M, Mezzour G, Perrig A, Gligor V. MiniSec: a secure sensor network communication architecture, 2007.

31. Zigbee. https://csa-iot.org/all-solutions/zigbee/ Accessed 23 Nov 2022.
32. Karlof C, Sastry N, Wagner D. TinySec: a link layer security architecture for wireless sensor networks, 2004. https://doi.org/10.1145/1031495.1031515
33. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for Internet of Things. J Netw Comput Appl. 2014;42:120–34. https://doi.org/10.1016/J.JNCA.2014.01.014.
34. Hasan MK, Weichen Z, Safie N, Ahmed FRA, Ghazal TM. A survey on key agreement and authentication protocol for internet of things application. IEEE Access. 2024;12:61642–66. https://doi.org/10.1109/ACCESS.2024.3393567.
35. Li Y, Alqahtani A, Solaiman E, Perera C, Jayaraman PP, Buyya R, Morgan G, Ranjan R. IoT-CANE: a unified knowledge management system for data-centric Internet of Things application systems. J Parallel Distribut Comput. 2019;131:161–72. https://doi.org/10.1016/J.JPDC.2019.04.016.
36. Flauzac O, Gonzalez C, Nolot F. New security architecture for IoT network. Procedia Comp Sci. 2015;52(1):1028–33. https://doi.org/10.1016/J.PROCS.2015.05.099.
37. Noura M, Atiquzzaman M, Gaedke M. Interoperability in internet of things: taxonomies and open challenges. Mobile Netw Appl. 2019;24(3):796–809. https://doi.org/10.1007/S11036-018-1089-9/FIGURES/5.
38. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun Surveys Tutorials. 2015;17(4):2347–76. https://doi.org/10.1109/COMST.2015.2444095.
39. Palattella MR, Dohler M, Grieco A, Rizzo G, Torsner J, Engel T, Ladid L. Internet of things in the 5G era: enablers, architecture, and business models. IEEE J Sel Areas Commun. 2016;34(3):510–27. https://doi.org/10.1109/JSAC.2016.2525418.
40. Pereira C, Aguiar A. Towards efficient mobile M2M communications: survey and open challenges. Sensors. 2014;14(10):19582–608. https://doi.org/10.3390/S141019582.
41. Kim NS, Lee K, Ryu JH. Study on IoT based wild vegetation community ecological monitoring system. International Conference on Ubiquitous and Future Networks, ICUFN 2015-Augus, 311–316, 2015.
42. Wang JY, Cao Y, Yu GP, Yuan MZ. Research on application of IOT in domestic waste treatment and disposal. Proceedings of the World Congress on Intelligent Control and Automation (WCICA) 2015, 4742–4745. https://doi.org/10.1109/WCICA.2014.7053515
43. Qiu T, Xiao H, Zhou P. Framework and case studies of intelligence monitoring platform in facility agriculture ecosystem. 2013 2nd International Conference on Agro-Geoinformatics: Information for Sustainable Agriculture, Agro-Geoinformatics 2013, 522–525.
44. Kumar Kasera R, Gour S, Acharjee T. A comprehensive survey on IoT and AI based applications in different pre-harvest, during-harvest and post-harvest activities of smart agriculture. Comput Electron Agric. 2024;216: 108522. https://doi.org/10.1016/J.COMPAG.2023.108522.
45. Subashini, S., Kamalam, G.K., Vanitha, P.: A Survey of IoT in healthcare technologies, applications, and challenges. Artificial intelligence and machine learning: an intelligent perspective of emerging technologies, 136–144, 2023.
46. Temglit N, Chibani A, Djouani K, Nacer MA. A distributed agent-based approach for optimal QoS selection in web of object choreography. IEEE Syst J. 2018;12(2):1655–66. https://doi.org/10.1109/JSYST.2016.2647281.
47. Talavera JM, Tobon LE, Gomez JA, Culman MA, Aranda JM, Parra DT, Quiroz LA, Hoyos A, Garreta LE. Review of IoT applications in agroindustrial and environmental fields. Comp Electron Agric. 2017;142:283–97.
48. Jara AJ, Zamora-Izquierdo MA, Skarmeta AF. Interconnection framework for mHealth and remote monitoring based on the internet of things. IEEE J Sel Areas Commun. 2013;31(9):47–65. https://doi.org/10.1109/JSAC.2013.SUP.0513005.
49. Alsharif MH, Kelechi AH, Jahid A, Kannadasan R, Singla MK, Gupta J, Geem ZW. A comprehensive survey of energy-efficient computing to enable sustainable massive IoT networks. Alex Eng J. 2024;91:12–29. https://doi.org/10.1016/J.AEJ.2024.01.067.
50. Ray PP. A survey on Internet of Things architectures. J King Saud Univ Comp and Info Sci. 2018;30(3):291–319. https://doi.org/10.1016/J.JKSUCI.2016.10.003.
51. Ibmsmartcloudenterprise.http://www-935.ibm.com/services/in/en/managed-cloud-hosting/
52. The internet of things—concept and problem statement. aahttps://datatracker.ietf.org/doc/html/draft-lee-iot-problem-statement-00. Accessed 30 Nov 2022
53. Whitmore A, Agarwal A, Xu LD. The internet of things—a survey of topics and trends. Info Syst Front. 2014;17(2):261–74. https://doi.org/10.1007/S10796-014-9489-2.
54. Wu M, Lu TJ, Ling FY, Sun J, Du HY. Research on the architecture of Internet of Things. ICACTE 2010 2010 3rd International Conference on Advanced Computer Theory and Engineering, Proceedings 2010 https://doi.org/10.1109/ICACTE.2010.5579493
55. Zhang J, Liang M. A new architecture for converged internet of things. International Conference on Internet Technology and Applications, ITAP 2010 Proceedings 2010. https://doi.org/10.1109/ITAPP.2010.5566263
56. Grønbæk I. Architecture for the Internet of Things (IoT): API and interconnect. Proceedings 2nd Int. Conf. Sensor Technol. Appl., SENSORCOMM 2008, Includes: MESH 2008 Conf. Mesh Networks; ENOPT 2008 Energy Optim. Wireless Sensors Networks, UNWAT 2008 Under Water Sensors Systems, 802–807, 2008 https://doi.org/10.1109/SENSORCOMM.2008.20
57. Abdmeziem MR, Tandjaoui D, Romdhani I.: Architecting the internet of things: state of the art. In: Studies in Systems, Decision and Control 2016;36:55–75.
58. Verma D, Singh KR, Yadav AK, Nayak V, Singh J, Solanki PR, Singh RP. Internet of things (IoT) in nano-integrated wearable biosensor devices for healthcare applications. Biosensors Bioelectr X. 2022;11: 100153. https://doi.org/10.1016/J.BIOSX.2022.100153.
59. Farooq M, Waseem M, Mazhar S, Khairi A, Kamal T. A review on internet of things (IoT). Int J Comp Appl. 2015;113(1):1–7. https://doi.org/10.5120/19787-1571.
60. Compton M, Henson C, Lefort L, Neuhaus H, Sheth A. A survey of the semantic specification of sensors. In: International Workshop on Semantic Sensor Networks 2009
61. Atzori L, Iera A, Morabito G. The internet of things: a survey. Comput Netw. 2010;54(15):2787–805. https://doi.org/10.1016/J.COMNET.2010.05.010.
62. Farooq M, et al. Internet of Things (IoT) system architecture and technologies. internet of things from hype to reality: the road to digitization 2015;**5**(1):1–7. https://doi.org/10.1109/WF-IoT.2014.6803174

63. Krco S, Pokric B, Carrez F. Designing IoT architecture(s): a European perspective. WF-IoT. 2014. https://doi.org/10.1109/WF-IOT.2014.6803124.
64. Saint-Andre P. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. Technical report, RFC 3920. https://www.ietf.org/rfc/rfc3920.txt
65. Yun M, Yuxin B. Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid. 2010 International Conference on Advances in Energy Engineering, 2010; 69–72.
66. Zhao L, Yin S, Liu L, Zhang Z, Wei S. A crop monitoring system based on wireless sensor network. Procedia Environ Sci. 2011;11:558–65. https://doi.org/10.1016/J.PROENV.2011.12.088.
67. Evans D. The internet of things how the next evolution of the internet is changing everything. CISCO white paper. 2015. https://doi.org/10.1109/IEEESTD.2007.373646.
68. Gantz J, Reinsel D. The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east 2012. www.emc.com/leadership/digital-universe/index.htm.
69. Taylor S. The Next generation of the internet revolutionizing the way we work, live, play, and learn. Technical report 2013. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/disruptive-technologies
70. James M, Michael C, Bughin J, Dobbs R, Bisson P, Marrs A. Disruptive technologies: advances that will transform life, business, and the global economy—McKinsey. Technical report, McKinsey Global Institute 2013. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/disruptive-technologies
71. Shafiq MZ, Ji L, Liu AX, Pang J, Wang J. A first look at cellular machine-to-machine traffic Large scale measurement and characterization. Perform Eval Rev. 2012;40:65–76. https://doi.org/10.1145/2254756.2254767.
72. IoT Technology Market by Node Cpmponent (Sensor, Memory device, Connectivity IC), Solution (Remote Monitoring, Data Management), Platform, Service, End-use Application, Geography (2021–2027). Technical report, MarketsandMarket 2021. https://www.marketsandmarkets.com/Market-Reports/iot-application-technology-market-258239167.html
73. IoT connections worldwide 2022–2033—Statista. https://www.statista.com/ statistics/1183457/iot-connected-devices-worldwide/. Accessed 04 Oct 2024
74. Floyer,D.:DefiningandSizingtheIndustrialInternet theCUBEResearch2013.https://thecuberesearch.com/defining-and-sizing-the-industrial-internet/. Accessed 12 Mar 2024.
75. Internet of Thngs (IoT) Market Size, Share & Industry Analysis, By Component, By End-use Industry, and Regional Forecast, 2024–2032. Technical report, Global. https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307
76. Omdia report finds purpose-driven smart homes will lead to a market size of $178bn in 2025 Omdia. https://omdia.tech.informa.com/pr/2021/sep/omdia-report-finds-purposedriven-smart-homes-will-lead-to-a-market-size-of-178bn-in-2025 Accessed 04 Oct 2024.
77. IndiaDigitalHealthcare.https://www.trade.gov/market-intelligence/ india-digital-healthcare Accessed 04 Oct 2024.
78. AsiaPacificIndustrialIoTMarketPoisedtoReach.https://www.globenewswire.com/news-release/2024/06/10/2896145/0/en/Asia-Pacific-Industrial-IoT-Market-Poised-to-Reach-Valuation-of-USD-52-7-Billion-By-2032-Astute-A.html Accessed 04 Oct 2024
79. GlobalMarketOutlookforSmartCitiesto2025.https://www.businesswire.com/news/home/20200908005469/en/Global-Market-Outlook-Smart-Cities-2025-- Accessed 04 Oct 2024.
80. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): a vision, architectural elements, and future directions. Futur Gener Comput Syst. 2013;29(7):1645–60. https://doi.org/10.1016/J.FUTURE.2013.01.010.
81. Nicolescu R, Huth M, Radanliev P, De Roure D. Mapping the values of IoT. J Info Technol. 2018;33(4):345–60. https://doi.org/10.1057/S41265-018-0054-1/FIGURES/1.
82. Hu P, Ning H, Qiu T, Xu Y, Luo X, Sangaiah AK. A unified face identification and resolution scheme using cloud computing in Internet of Things. Futur Gener Comput Syst. 2018;81:582–92.
83. Montenegro G, Kushalnagar N, Hui J, Culler D. Transmission of IPv6 Packets over IEEE 802.15.4 Networks 2007. https://doi.org/10.17487/RFC4944
84. Sun, W., Choi, M., Choi, S.: IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz. J ICT Standard 83–108 (2013)
85. Nieminen J, Savolainen T, Isom¨aki M, Patil B, Shelby Z, Gomez C. IPv6 over BLUETOOTH(R) Low Energy. Technical report 2015. https://doi.org/10.17487/RFC7668.
86. Ghosh A, Ratasuk R, Mondal B, Mangalvedhe N, Thomas T. LTEadvanced: next-generation wireless broadband technology. IEEE Wirel Commun. 2010;17(3):10–22. https://doi.org/10.1109/MWC.2010.5490974.
87. ANT Basics THIS IS ANT. https://www.thisisant.com/developer/ant/ant-basics/. Accessed 04 Mar 2024
88. LoRaWAN Specification v1.0.3 LoRa Alliance
89. Mikhaylov K, Juha P, Haenninen T. Analysis of capacity and scalability of the LoRa low power wide area network technology. In: 22th European Wireless Conference, pp. 1–6. VDE VERLAG GMBH, 2016
90. Dujovne D, Watteyne T, Vilajosana X, Thubert P. 6TiSCH: deterministic IP-enabled industrial internet (of things). IEEE Commun Mag. 2014;52(12):36–41. https://doi.org/10.1109/MCOM.2014.6979984.
91. Systems C, Brandt A, Designs S, Hui J, Levis P, Pister K, Vasseur JP, Alexander R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. Technical report 2012. https://doi.org/10.17487/RFC6550 .
92. Aijaz A, Su H, Aghvami AH. CORPL: a routing protocol for cognitive radio enabled AMI networks. IEEE Trans Smart Grid. 2015;6(1):477–85. https://doi.org/10.1109/TSG.2014.2324022.
93. Yang Z, Ping S, Sun H, Aghvami AH. CRB-RPL: a receiver-based routing protocol for communications in cognitive radio enabled smart grid. IEEE Trans Veh Technol. 2017;66(7):5985–94. https://doi.org/10.1109/TVT.2016.2617874.
94. Shelby Z, Hartke K, Bormann C. The constrained application protocol (CoAP). Technical report 2014. https://doi.org/10.17487/RFC7252
95. Singh M, Rajan MA, Shivraj VL, Balamuralidhar P. Secure MQTT for Internet of Things (IoT). In: 2015 Fifth International Conference on Communication Systems and Network Technologies, pp. 746–751. Institute of Electrical and Electronics Engineers Inc., 2015. https://doi.org/10.1109/CSNT.2015.16
96. Ungurean I, Gaitan N. Data distribution service for realtime systems-a solution for the internet of things environments. Ann Univ Dunarea de Jos of Galati: Fascicle II Math Phys Theor Mech. 2015;38(1):72–6.

97. Vinoski S. Advanced message queuing protocol. IEEE Internet Comput. 2006;10(6):87–9. https://doi.org/10.1109/MIC.2006.116.
98. Lin MS, Leu JS, Li KH, Wu JLC. Zigbee-based Internet of Things in 3D Terrains. Comp Electr Eng. 2013;39(6):1667–83.
99. Gunner B. MQTT will enable the Internet Of Things 2013
100. Al Nuaimi E, Al Neyadi H, Mohamed N, Al-Jaroodi J. Applications of big data to smart cities. J Internet Serv Appl. 2015;6(1):1–15. https://doi.org/10.1186/S13174-015-0041-5.
101. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): a vision, architectural elements, and future directions. Futur Gener Comput Syst. 2013;29:1645–60. https://doi.org/10.1016/j.future.2013.01.010.
102. Gluhak A, Krco S, Nati M, Pfisterer D, Mitton N, Razafindralambo T. A survey on facilities for experimental internet of things research. IEEE Commun Mag. 2011;49(11):58–67. https://doi.org/10.1109/MCOM.2011.6069710.
103. Li X, Lu R, Liang X, Shen X, Chen J, Lin X. Smart community: an internet of things application. IEEE Commun Mag. 2011;49(11):68–75. https://doi.org/10.1109/MCOM.2011.6069711.
104. Matin A, Islam MR, Wang X, Huo H, Xu G. AIoT for sustainable manufacturing: overview, challenges, and opportunities. IoT. 2023;24:100901. https://doi.org/10.1016/J.IOT.2023.100901.
105. Li D, Jiang B, Suo H, Guo Y. Overview of Smart Factory Studies in Petrochemical Industry. Comp Aided Chem Eng. 2015;37:71–6. https://doi.org/10.1016/B978-0-444-63578-5.50009-8.
106. Singh PP, Khosla PK, Mittal M. Energy conservation in IoT-based smart home and its automation. Stud Syst Decision Control. 2019;206:155–77.
107. Balasubramanian C, Raja Singh RL. IoT based energy management system in smart grid. I-PACT. 2023. https://doi.org/10.1109/I-PACT58649.2023.
108. Allende C, Bannister P. International review of energy efficiency in data centres acknowledgements. Technical report, Australian Department of Industry, Science, Energy and Resources 2021
109. Zhang M, Yu T, Zhai G. Smart transport system based on "The internet of things". Appl Mech Mater. 2011;48–49:1073–6. https://doi.org/10.4028/WWW.SCIENTIFIC.NET/AMM.48-49.1073.
110. Lin HE, Zito R, Taylor M. A review of travel-time prediction in transport and logistica 2005
111. Hern´andez-Mun˜oz JM, Vercher JB, Mun˜oz L, Galache JA, Presser M, Hern´andez G´omez LA, Pettersson J. Smart cities at the forefront of the future internet. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2011;**6656**:447–462.
112. Pise A, Yoon B, Singh S. Enabling ambient intelligence of things (AIoT) healthcare system architectures. Comput Commun. 2023;198:186–94. https://doi.org/10.1016/J.COMCOM.2022.10.029.
113. Tu M, Lim MK, Yang MF. IoT-based production logistics and supply chain system – part 1 modeling IoT-based manufacturing IoT supply chain. Ind Manag Data Syst. 2018;118(1):65–95. https://doi.org/10.1108/IMDS-11-2016-0503/FULL/XML.
114. Alzahrani A, Asghar MZ. Intelligent risk prediction system in IoT-based supply chain management in logistics sector. Electronics. 2023;12(13):2760. https://doi.org/10.3390/ELECTRONICS12132760.
115. Raviteja K, Supriya M. IoT-based agriculture monitoring system. Adv Intell Syst Comp. 2020;1079:473–83.
116. Prathibha SR, Hongal A, Jyothi MP. IOT based monitoring system in smart agriculture. Proceedings 2017 International Conference on Recent Advances in Electronics and Communication Technology, ICRAECT 2017, 81–84. https://doi.org/10.1109/ICRAECT.2017.52
117. Evizal R, Rahim SKA. RFID vehicle plate number (e-plate) for tracking and management system. In: Proceedings of the International Conference on Parallel and Distributed Systems ICPADS, IEEE Computer Society, 2013. pp. 611–616. https://doi.org/10.1109/ICPADS.2013.109
118. Derawi M, Dalveren Y, Cheikh FA. Internet-of-things-based smart transportation systems for safer roads. In: IEEE World Forum on Internet of Things, WF-IoT 2020 Symposium Proceedings. Institute of Electrical and Electronics Engineers Inc., 2020. https://doi.org/10.1109/WF-IOT48130.2020.
119. Park E, Pobil AP, Kwon SJ. The role of Internet of Things (IoT) in smart cities: technology roadmap-oriented approaches. Sustainability (Switzerland). 2018. https://doi.org/10.3390/SU10051388.
120. Wei Y, Sukumar K, Vecchiola C, Karunamoorthy D, Buyya R. Aneka cloud application platform and its integration with windows azure. Cloud Comp. 2017. https://doi.org/10.1201/B11149-27.
121. Kumar P, Ranganath S, Weimin H, Sengupta K. Framework for real-time behavior interpretation from traffic video. IEEE Trans Intell Transp Syst. 2005;6(1):43–53. https://doi.org/10.1109/TITS.2004.838219.
122. Pettey C. Five ways the internet of things will benefit the supply chain 2. 2015. https://www.gartner.com/smarterwithgartner/five-ways-the-internet-of-things-will-benefit-the-supply-chain-2. Accessed 06 Mar 2024.
123. Singh D, Kew HP, Tiwary US, Lee HJ, Chung WY. Global patient monitoring system using IP-enabled ubiquitous sensor network. 2009 WRI World Congress on Computer Science and Information Engineering, CSIE 2009;1:524– 528. https://doi.org/10.1109/CSIE.2009.921
124. Zhang M, Yu T, Zhai G. Smart transport system based on "The internet of things". Appl Mech Mater. 2011;48–49:1073–6.
125. Internet of Things Architecture — IOT-A: Internet of Things Architecture. https://www.iot-a.eu/. Accessed 18 Nov 2022.
126. Kotis, K., Katasonov, A.: Semantic interoperability on the Web of things: The semantic smart gateway framework. Proceedings 2012 6th International Conference on Complex, Intelligent, and Software Intensive Systems, CISIS 2012, 630–635. https://doi.org/10.1109/CISIS.2012.200
127. Jara AJ, Varakliotis S, Skarmeta AF, Kirstein P. Extending the Internet of Things to the Future Internet through IPv6 support. 2014;**10**(1):3–17. https://doi.org/10.3233/MIS-130169
128. Zivkovic M, Nikolic B, Protic J, Popovic R. A survey and classification of wireless sensor networks simulators based on the domain of use Ad Hoc Sens. Wirel Networks. 2014;20:245–87.
129. Kumar S, Bansal A. Performance investigation of topology-based routing protocols in flying ad-hoc networks using NS-2. IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks, 2020, 243–267. https://doi.org/10.4018/978-1-7998-2570-8.CH013
130. Kim BS, Sung TE, Kim KI. An NS-3 implementation and experimental performance analysis of IEEE 802.15.6 standard under different deployment scenarios. Int J Environ Res Public Health. 2020;17(11):1–31. https://doi.org/10.3390/IJERPH17114007.

131. IoT Simulator to easily simulate real MQTT Devices Bevywise Networks. https://www.bevywise.com/iot-simulator/index.html. Accessed 05 Mar 2024
132. Mehmood T. COOJA Network simulator: exploring the infinite possible ways to compute the performance metrics of IOT based smart devices to understand the working of IOT based compression & routing protocols
133. Stifani, R.: IBM bluemix the cloud platform for creating and delivering applications. Int Tech Support Org, 2015
134. Barbecho Bautista PA, Urquiza-Aguiar LF, Cardenas LL, Igartua MA. Large-scale simulations manager tool for OmNet++: expediting simulations and post-processing analysis. IEEE Access. 2020;8:159291–306. https://doi.org/10.1109/ACCESS.2020.3020745.
135. Laliberte B. Enterprise environments are rapidly evolving riverbed: networkperformancemanagementsolutionsformodernbusiness. 2020. https://www.riverbed.com/riverbed-wp-content/uploads/2023/02/riverbednetwork-performance-management-solutions-modern-business-whitepaper. pdf
136. Chaturvedi DK. Modeling and simulation of systems using MATLAB® and simulink®. Modeling and Simulation of Systems Using MATLAB and Simulink, 2017, 1–709.
137. Nuevo J. A Comprehensible GloMoSim Tutorial, Universite du Quebec 2004
138. Perkins C, Belding-Royer E, Das S. Network Working Group 2003
139. PacketTracer.https://learningnetwork.cisco.com/s/packet-tracer-alternative-lab-solutions. Accessed 04 Oct 2024.
140. ThingsBoard Community Edition. https://thingsboard.io/docs/. Accessed 04 Oct 2024
141. Sibilla, G.: Intelligence for a safe city model. Information Security: An International Journal **30**(2) (2014)
142. Tan L, Wang N. Future internet: the internet of things. ICACTE 2010 2010 3rd International Conference on Advanced Computer Theory and Engineering, Proceedings 2010;5. https://doi.org/10.1109/ICACTE.2010.5579543
143. Haddara M, Staaby A. RFID applications and adoptions in healthcare: a review on patient safety. Procedia Comput Sci. 2018;138:80–8. https://doi.org/10.1016/J.PROCS.2018.10.012.
144. Lakshman TV, Madhow U. The performance of TCP/IP for networks with high bandwidth-delay products and random loss. IEEE/ACM Trans Netw. 1997;5(3):336–50. https://doi.org/10.1109/90.611099.
145. Kumar Rana R, Tung Chou C, Kanhere S, Bulusu N, Hu W. Ear-phone: an end-to-end participatory urban noise mapping system. Technical report 2009
146. Donoho DL. Compressed sensing. IEEE Trans Inf Theory. 2006;52(4):1289–306. https://doi.org/10.1109/TIT.2006.871582.
147. Bajwa W, Haupt J, Sayeed A, Nowak R. Compressive wireless sensing. In: Proceedings of the Fifth International Conference on Information Processing in Sensor Networks, IPSN '06, vol. 2006, 2006, pp. 134–142
148. Tan W, Xu K, Wang D. An anti-tracking source-location privacy protection protocol in WSNs based on path extension. IEEE Internet Things J. 2014;1(5):461–71.
149. Zong B, Fan C, Wang X, Duan X, Wang B, Wang J. 6G technologies: key drivers, core requirements, system architectures, and enabling technologies. IEEE Veh Technol Mag. 2019;14(3):18–27. https://doi.org/10.1109/MVT.2019.2921398.
150. Ye N, Yu J, Wang A, Zhang R. Help from space: grant-free massive access for satellite-based IoT in the 6G era. Dig Commun Netw. 2022;8(2):215–24. https://doi.org/10.1016/J.DCAN.2021.07.008.
151. Bankey V, Upadhyay PK. Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks. IEEE Trans Veh Technol. 2019;68(3):2488–501. https://doi.org/10.1109/TVT.2019.2893366.
152. Niu H, Lin Z, Chu Z, Zhu Z, Xiao P, Nguyen HX, Lee I, Al-Dhahir N. Joint beamforming design for secure RIS-assisted IoT networks. IEEE Internet Things J. 2023;10(2):1628–41. https://doi.org/10.1109/JIOT.2022.3210115.
153. Giordani M, Polese M, Mezzavilla M, Rangan S, Zorzi M. Toward 6G networks: use cases and technologies. IEEE Commun Magaz. 2020;58(3):55–61. https://doi.org/10.1109/MCOM.001.1900411.
154. Qadir Z, Le KN, Saeed N, Munawar HS. Towards 6G Internet of Things: recent advances, use cases, and open challenges. ICT Express. 2023;9(3):296–312. https://doi.org/10.1016/J.ICTE.2022.06.006.
155. Kok I, Okay FY, Ozdemir S. FogAI: an AI-supported fog controller for Next Generation IoT. Internet of Things. 2022;19: 100572. https://doi.org/10.1016/J.IOT.2022.100572.
156. Tegos SA, Diamantoulakis PD, Lioumpas AS, Sarigiannidis PG, Karagiannidis GK. Slotted ALOHA with NOMA for the Next Generation IoT. IEEE Trans Commun. 2020;68(10):6289–301. https://doi.org/10.1109/TCOMM.2020.3007744.
157. Lin Z, Lin M, De Cola T, Wang JB, Zhu WP, Cheng J. Supporting IoT with rate-splitting multiple access in satellite and aerial-integrated networks. IEEE IoT J. 2021;8(14):11123–34.
158. Lin Z, Lin M, Wang JB, De Cola T, Wang J. Joint beamforming and power allocation for satellite-terrestrial integrated networks with non-orthogonal multiple access. IEEE J Sel Top Sign Proces. 2019;13(3):657–70. https://doi.org/10.1109/JSTSP.2019.2899731.
159. Kumar A, L FY, Martinez-Bauset J. Revealing the benefits of ratesplitting multiple access for uplink IoT traffic. GLOBECOM, 2022;111–116 (2022)
160. Liu H, Tsiftsis TA, Kim KJ, Kwak KS, Poor HV. Rate splitting for uplink noma with enhanced fairness and outage performance. IEEE Trans Wireless Commun. 2020;19(7):4657–70. https://doi.org/10.1109/TWC.2020.2985970.
161. Agrawal N, Bansal A, Singh K, Li CP, Mumtaz S. Finite block length analysis of RIS-assisted UAV-based multiuser IoT communication system with non-linear EH. IEEE Trans Commun. 2022;70(5):3542–57. https://doi.org/10.1109/TCOMM.2022.3162249.
162. Bansal A, Singh K, Li CP. Analysis of hierarchical rate splitting for intelligent reflecting surfaces-aided downlink multiuser MISO communications. IEEE Open J Commun Soc. 2021;2:785–98. https://doi.org/10.1109/OJCOMS.2021.3070340.
163. Li B, Fei Z, Zhang Y. UAV communications for 5G and beyond: Recent advances and future trends. IEEE IoT J. 2019;6(2):2241–63. https://doi.org/10.1109/JIOT.2018.2887086.
164. Ruan Y, Li Y, Zhang R, Cheng W, Liu C. Cooperative resource management for cognitive satellite-aerial-terrestrial integrated networks towards IoT. IEEE Access. 2020;8:35759–69. https://doi.org/10.1109/ACCESS.2020.2975012.
165. Zhou D, Gao S, Liu R, Gao F, Guizani M. Overview of development and regulatory aspects of high altitude platform system. Intell Converged Netw. 2020;1(1):58–78. https://doi.org/10.23919/ICN.2020.0004.
166. Qin P, Zhu Y, Zhao X, Feng X, Liu J, Zhou Z. Joint 3D-location planning and resource allocation for XAPS-enabled C-NOMA in 6G heterogeneous internet of things. IEEE Trans Veh Technol. 2021;70(10):10594–609. https://doi.org/10.1109/TVT.2021.3109883.

167. Zare M, Elmi Sola Y, Hasanpour H. Towards distributed and autonomous IoT service placement in fog computing using asynchronous advantage actorcritic algorithm. J King Saud Univ Comp Info Sci. 2023;35(1):368–81. https://doi.org/10.1016/J.JKSUCI.2022.12.006.
168. Gomes E, Costa F, De Rolt C, Plentz P, Dantas M. A survey from real-time to near real-time applications in fog computing environments. Telecom. 2021;2(4):489–517.
169. Alghamdi I, Anagnostopoulos C, Pezaros DP. Data quality-aware task offloading in mobile edge computing: an optimal stopping theory approach. FGCS. 2021;117:462–79.
170. Zhang Y, Yu H, Zhou W, Man M. Application and research of IoT architecture for end-net-cloud edge computing. Electronics. 2022;12(1):1. https://doi.org/10.3390/ELECTRONICS12010001.
171. Zhang Z, Xiao Y, Ma Z, Xiao M, Ding Z, Lei X, Karagiannidis GK, Fan P. 6G wireless networks: vision, requirements, architecture, and key technologies. IEEE Veh Technol Mag. 2019;14(3):28–41. https://doi.org/10.1109/MVT.2019.2921208.
172. Zhou C, Wu W, He H, Yang P, Lyu F, Cheng N, Shen X. Deep reinforcement learning for delay-oriented IoT task scheduling in SAGIN. IEEE Trans Wireless Commun. 2021;20(2):911–25. https://doi.org/10.1109/TWC.2020.3029143.
173. Qin P, Fu Y, Zhao X, Wu K, Liu J, Wang M. Optimal task offloading and resource allocation for C-NOMA heterogeneous air-ground integrated power internet of things networks. IEEE Trans Wireless Commun. 2022;21(11):9276–92. https://doi.org/10.1109/TWC.2022.3175472.
174. Tang F, Hofner H, Kato N, Kaneko K, Yamashita Y, Hangai M. A deep reinforcement learning-based dynamic traffic offloading in spaceair-ground integrated networks (SAGIN). IEEE J Sel Areas Commun. 2022;40(1):276–89. https://doi.org/10.1109/JSAC.2021.3126073.
175. Al Ridhawi I, Otoum S. Supporting next-generation network management with intelligent moving devices. IEEE Network. 2022;36(3):8–15. https://doi.org/10.1109/MNET.009.2100585.
176. Liu J, Zhao X, Qin P, Geng S, Meng S. Joint dynamic task offloading and resource scheduling for WPT enabled space-air-ground power internet of things. IEEE Trans Netw Sci Eng. 2022;9(2):660–77. https://doi.org/10.1109/TNSE.2021.3130251.
177. Kathole AB, Kimbahune VV, Patil SD, Jadhav AP, Vhatkar KN. Challenges and key issues in IoT privacy and security. IoT Part. 2024;F2482:37–50. https://doi.org/10.1007/978-981-97-0052-33.
178. Liu C, Chen B, Shao W, Zhang C, Wong KKL, Zhang Y. Unraveling attacks to machine-learning-based IoT systems: a survey and the open libraries behind them. IEEE IoT J. 2024;11(11):19232–55. https://doi.org/10.1109/JIOT.2024.3377730.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.