SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper
Open Access

# A Comprehensive Review Of Architecture, Technologies, Characteristics, And Applications Of Internet Of Things

Maulik Dhamecha [1], Urvi Dhamecha [2], Aswathy R Nair [3], Hansa Vaghela [4], Ravi J. Khimani [5], Shyam Kotecha [6]

[1] Department of Computer Engineering, V.V.P. Engineering College, Rajkot, Gujarat. mvdhamecha@gmail.com
[2] Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, urvidarji17@gmail.com
[3] Department of Computer Engineering, Marwadi University, Rajkot, Gujarat. arn.aswathy@gmail.com
[4] Department of Computer Engineering, Marwadi University, Rajkot, Gujarat. vaghelahansa315@gmail.com
[5] Computer Engineering, Government Engineering College, Rajkot, Gujarat. ravikhimani.gec@gmail.com
[6] Computer Engineering, Government Engineering College, Rajkot, Gujarat. shyamkotecha.gec@gmail.com

**Abstract**
Internet of things (IoT) refers to an innovative concept used to link physical items through communication networks. IoT comprises of devices that contain sensors, embedded computational power, software and networking ability that allows collection, exchange and processing of data for provision of intelligent services. Though the name seems to indicate the dependency of IoT on the public internet, IoT devices can also function through private networks and communication infrastructures. IoT enables automation, monitoring and informed decision making through use of sensors, cloud computing, edge computing and artificial intelligence in fields such as health care, smart homes, industries, agriculture and transportation. Issues concerning security, privacy, interoperability and scalability should be taken into account while developing IoT systems.

**Keywords:** Communications networks, Internet of Things, Sensors, Processing ability.

## 1. Introduction

The advent of the Internet of Things (IoT) can be considered one of the greatest technological innovations in the current era [1], [2]. The basic principle of the Internet of Things involves the interconnection of physical objects or devices with each other via communication networks to facilitate data gathering, analysis, monitoring, and smart decision-making [1], [3]. In contrast to conventional computing systems which need a physical human intervention for their operation, IoT allows the devices to communicate in an autonomous manner and carry out certain functions using the gathered data [3], [4]. The result of this innovation has been the emergence of a new environment where the physical objects have become smart entities able to sense and react to the environment [2], [4].

The idea behind the Internet of Things and hence the term was initially brought up by Peter T. Lewis during a speech made at the 15th Annual Congressional Black Caucus Legislative Weekend in Washington D.C. in 1985 [5]. According to Lewis, IoT is about the combination of people, process, and technologies with devices and sensors in order to remotely monitor, identify, control, manipulate, and evaluate interconnected objects [5]. In his concept, he envisioned interconnected environments in which communication between devices and provision of useful data without any human involvement would be possible [5]. Although the technological infrastructure to support wide-spread use of IoT technology did not exist back then, the concept served as the basis for further development in the sphere of connected technologies [5].

Later in 1999, the notion of Internet of Things (IoT) was developed independently by Kevin Ashton who was involved in research at that time for Procter & Gamble and MIT Auto-ID Centre [6]. The concept involved utilization of Radio Frequency Identification (RFID) technology that would enable computers to automatically identify objects in order to gather information on them [6], [7]. The point was that computers must get the ability to collect information not only from the virtual world but also from the real world without any human assistance [6]. The development of Internet of Things concept marked a breakthrough from the classical notion of Internet that mainly focused on connecting people and computers to a new concept of Internet that allows hundreds of millions of devices to communicate with each other [1], [3]. The quick development of IoT is linked to the moment when the number of devices connected to the Internet surpassed the amount of people connected to it [8].

As a result of constant developments in the field of mobile computing and mobile devices, IoT technology has been successfully implemented in our daily activities [2], [4]. Modern mobile devices offer many features of sensing and communication, such as GPS tracking, gyroscope, accelerometer, brightness adjuster, voice recognition system, face recognition technology, and location services [2], [9]. All these devices serve unique functions, but when working together, they help create intelligent and customized user experience [2], [9]. For instance, the brightness of your smartphone screen can be automatically adjusted according to your location, environmental lighting conditions, or phone orientation. The same applies to location and motion sensors used in navigation apps, fitness tracking systems, and other context-aware applications [9].

The IoT ecosystem comprises numerous physical objects which are equipped with connectivity technologies, electronics, software applications, and sensors that help them collect and exchange data without requiring constant manual intervention [1], [3]. The objects in the context of IoT include numerous physical items such as household devices, industrial machinery, automobiles, health-related devices, wearables, agricultural equipment, and smart infrastructure components [2], [4]. These objects have unique identities and are able to communicate either by means of wired or wireless connections [1], [3]. Through connectivity, IoT allows for data exchange and automation opportunities [2], [4].

IoT is an automation and analysis model made up of several emerging technologies like artificial intelligence (AI), sensor technology, embedded systems, wireless communication, electronics, cloud computing, and data analytics [2], [4], [10]. All these technologies collaborate in such a way as to develop smart systems that monitor the physical environment, analyse data and make automatic decisions [2], [10]. Systems based on the Internet of Things (IoT) offer transparency, operational control, efficiency, and less human involvement through access to real-time information and management of connected devices [5]. The incorporation of the Internet of Things and artificial intelligence provides smartness to the system by learning from past data, forecasting future trends and doing autonomous activities [10].

The notable aspect about the Internet of Things is that it enables users to have a single platform for interconnecting and managing several devices or services [2], [4]. Much like the cloud system, the Internet of Things platform helps in collecting and analysing the information created by these devices [2]. The users can then control several systems via this single platform [2]. To take the example of a smart home system, it consists of various household appliances such as air conditioners, lights, security cameras, smart televisions, and home assistants [2], [4]. These devices can be managed from a distance by using smartphones and even voice commands [4].

Another significant application of IoT technology can be seen in the field of automobiles, wherein the vehicles use sensors and communication systems along with cloud-based computing to offer improved driving experiences [2], [4]. The modern-day vehicles that use IoT technology have the capability to monitor various parameters such as the fuel consumed, speed of the vehicle, performance of the engine, tire pressure, and location of the vehicle [2]. The driver has the facility of remotely accessing all this information related to the vehicle along with other advantages like better safety and fuel consumption [2].

Apart from being used for consumers, Internet of Things has shown substantial potential in several other areas such as industry, healthcare, agriculture, and urban development [2], [4]. In the industrial setting, the use of IoT has made it possible to achieve smart manufacturing by way of monitoring equipment, conducting predictive maintenance, and automating manufacturing processes [4], [11]. The application of Internet of Things in healthcare sector includes remote patient monitoring, smart wearable medical devices, and intelligent healthcare systems that increase access to healthcare services and enhance their quality [12], [13]. In agriculture, the use of sensors has helped monitor the condition of soil, weather, and crops [14].

Although there are many benefits to IoT, there are also some disadvantages associated with the quick growth of the Internet of Things that include security concerns, privacy issues, interoperability concerns, scalability challenges, and other problems [3], [4], [15]. As IoT devices generate vast amounts of data on an ongoing basis, it is important to ensure that the information cannot be stolen or tampered by hackers [15]. Moreover, the variety of devices and protocols used results in incompatibility problems for various platforms and vendors [3], [4]. Thus, creating secure communication channels and efficient architectures is crucial for future IoT ecosystems [15].

## 2. Literature Survey on Fundamental Architecture of IoT

The concept of IoT has become the focus of many research efforts because of the possibility of merging physical objects, communication infrastructures, computing environments, and intelligent processing systems within a single technological environment [16], [17]. The architecture of IoT is defined by the structure of the technological environment required for sensing, communication, data processing, and application services [16], [18]. Many architectures of IoT have been suggested to meet the needs for scalability, interoperability, security, and resource efficiency [17], [19]. While many architectures have been proposed, most of the IoT architectures include three basic layers: perception, network, and application layers [16], [20]. The advanced architectures also incorporate the layers of processing, middleware, security, and business [18], [20].

The initial basis of IoT architecture was laid down through the combination of sensor technologies, embedded systems, and communication networks [16], [17]. According to the initial ideas about IoT that were developed by Peter T. Lewis, the IoT was seen as an integrated space where people, processes, and technologies were interacting using intelligent devices and sensors [21]. The IoT architecture at that stage was centred around providing capabilities to remotely monitor, identify, and control physical objects [21]. In his turn, Kevin Ashton put emphasis on the use of RFID technology in IoT development by suggesting that computers could gather information from physical objects independently from the involvement of human beings [22]. These contributions defined the initial basis of IoT architectures based on the concept of uniquely identifiable objects that can communicate and share information [22], [23].

Generally, an architecture of the Internet of Things (IoT) starts from the perception layer, which is considered the physical layer for acquiring data from the environment [16], [20]. The perception layer comprises a variety of sensors, RFIDs, actuators, cameras, embedded controllers, smart objects, and other devices that acquire real-time information regarding temperature, humidity, position, motion, pressure, and other environment parameters [17], [20]. It serves as a connection link between the physical and digital worlds [16]. From research works conducted, it became clear that the efficiency and effectiveness of IoT systems greatly rely on the performance of the sensors since their malfunctioning may result in wrong and incomplete data acquisition [17], [24].

The second important element of the architecture of IoT is the network layer that acts as a communication layer responsible for the transmission of gathered data from the sensors to processing systems and application layers [16], [20]. The network layer consists of wired and wireless communication technologies, including Wi-Fi, Bluetooth, Zigbee, RFID, cellular networks, and advanced 5G communication technologies [17], [25]. Many scholars have highlighted the importance of communication protocols in the field of IoT due to the fact that the connected devices usually have low processing, memory, and energy capacities [17], [25]. Thus, lightweight communication techniques should be used for reliable data transmission [25], [26].

The processing layer, which is also referred to as the middleware layer, has been developed in sophisticated IoT architecture designs in order to deal with the shortcomings of the old three-layer design model [18], [27]. The processing layer is tasked with the responsibility of handling data storage, data analysis, device management, and service coordination [18], [27]. Cloud computing systems have been extensively applied in IoT architectures in order to offer large-scale computation and storage facilities that will help in dealing with the huge amount of data that is being generated by IoT systems [17], [28]. It has been found out that there are several challenges related to the use of cloud computing technologies in IoT systems; some of the challenges include the presence of high latencies, need for more bandwidth and reliance on central infrastructure [28], [29]. In order to address this challenge, IoT architectures can use edge computing and fog computing solutions [29], [30].

The application layer is referred to as the end-user layer, where the processed data is converted into services or applications [16], [20]. The application layer offers interfaces through which users can observe, control, and interact with the IoT systems [16], [17]. The different areas of applications include smart home, smart city, healthcare, industrial automation, agriculture, transportation among others [17], [20]. Several studies have shown that the specific IoT architectures for each application offer a great improvement in efficiency and the user experience through automated control mechanism [17], [31].

A number of scientists have suggested extending IoT architectures by adding extra layers to increase efficiency and improve security [20], [32]. One of the popular IoT architectures consists of five layers and involves the perception layer, the transport layer, the processing layer, the application layer, and the business layer [20], [32]. The business layer is responsible for managing the entire system, analytics, policy formulation, and business decisions [20], [32]. The business layer makes it possible for companies to analyse information received from IoT devices [32].

There has been increased emphasis on security and privacy issues in IoT architecture design since there is an increase in numbers of connected devices as well as sensitive data collected [19], [33]. There are studies from literature that show that traditional security methods cannot be used in IoT due to several reasons including the fact that most of these devices have processing limitations and are energy constrained [19], [33]. Different security approaches have been recommended which include encryption algorithms, authentication, access control, blockchain architecture, and AI-based intrusion detection system among others [19], [33], [34].
Another important issue in the context of IoT architecture which requires research attention is interoperability. The reason behind this problem lies in the heterogeneity of the components in IoT environment where communication standards used by various components differ [17], [18]. Several research efforts have attempted to design communication frameworks that can ensure communication between components from different vendors [18], [25]. These include MQTT, CoAP, and REST-based communication frameworks [25], [35].
Advances in the areas of artificial intelligence and machine learning have greatly contributed towards boosting the abilities of IoT architectures [36], [37]. AI-based IoT architectures are able to analyze massive amounts of data gathered through sensors, recognize patterns, detect abnormalities, and make predictive decisions [36], [37]. Increasingly machine learning algorithms are being used as part of the IoT process layer in order to implement functions like predictive maintenance, health diagnosis, smart surveillance, and energy management [36], [38]. With the help of IoT and AI, autonomous systems have been developed which can adapt to changing environments [36], [37].

In conclusion, from what is found in the literature, it can be seen that there have been developments in the IoT architecture model from basic three layers to multi-layer architectures including cloud computing, edge intelligence, artificial intelligence, and security aspects [16], [17], [29]. The basic IoT architecture forms the basis for the connection of the physical devices and communications, processing, and intelligent services provided [16], [18]. Despite the considerable advancements made, issues surrounding security, scalability, interoperability, and energy efficiency still affect research on IoT [19], [33]. The future IoT architectures will involve decentralized intelligence, secure communication, autonomous decisions, and compatibility with new technologies like 5G/6G networks, blockchain, and digital twin technologies [29], [34], [39].

## 3. IoT Architecture Components of IoT Architecture

The IoT architecture refers to the basic structure that enables the organization of a diverse range of hardware and software needed for facilitating communication between physical objects, networks, data processing system, and user applications. Through its architecture, IoT allows for a coherent approach to integrating heterogeneous devices, communication methods, and computing facilities in order to provide efficient intelligent services. The architecture enables IoT systems to be scalable, interoperable, and secured while providing automation and decision-making capabilities. As the complexity of IoT systems increases, it is important to have an established architecture [40], [41].
An IoT architecture is usually comprised of several layers where each layer carries out certain functions. Even though various architectural approaches have been suggested by scholars, four layers can be identified for any common IoT framework: Sensors/Devices Layer, Gateways and Network Layer, Cloud/Management Service Layer, and Application Layer. It is through the interaction of these layers that data collection, communication, data processing, analysis, and service provision take place [40], [42].

### 3.1 Sensors and Devices Layer

The Sensors and Devices Layer refer to the physical backbone of the IoT. The Sensors and Devices Layer comprise smart objects, sensors, actuators, embedded devices, and technologies for identifying devices to gather data from the environment. Sensors refer to electronic gadgets that measure physical phenomena such as temperature, humidity, pressure, movement, position, vibration, and chemical reactions and convert them to digital signals. However, actuators take action depending on the commands they receive, which involve physical activities such as turning devices on and off or changing temperature levels [40], [43].
For an IoT environment, the sensors and actuators can communicate and exchange data through communication techniques that use either wired or wireless connection. The technologies available for sensors include GPS technology, RFID, gyroscope, accelerometers, electrochemical sensors, biometric sensors, and environmental sensors. The sensors can work individually or exchange information through sensor networks. Due to the limitation

on energy, processing power, and memory available to some IoT sensors, proper communication and power management methods are necessary for their proper functioning [41], [44].
Sensors are usually interfaced with other IoT components using sensor gateways or local networks. Sensors may be included in various communication environments such as WSNs, LANs, PANs, and industrial communication networks. Accuracy of sensor data plays an important role in the efficiency of overall IoT system since all further processes and decision-making procedures depend on the data obtained at this level [43], [44].

### 3.2 Gateways and Data Acquisition Layer

Gateway and Data Acquisition Layer serve as a communication bridge between sensors or devices and processing layer. Due to the continuous generation of huge amounts of data by Internet of Things devices, it becomes inefficient to have direct communication between the sensors and the cloud platform. Gateways help in performing operations like data aggregation, protocol translation, data filtering, security management, and temporary storage of data [42], [45].
An IoT gateway acts as an interface between different types of devices and transforms protocols of different devices to standard protocols that can be transmitted on larger networks. IoT gateways minimize network traffic through filtering of unnecessary data and transmitting necessary data for further processing. IoT gateways also offer extra computing power for local computation [45].
The networks that can be used for communication within this layer could include both local networks as well as wide area networks. Short-range communication techniques include technologies like Wi-Fi, Ethernet, Bluetooth, and Zigbee, whereas long-range communication involves technologies like GSM, LTE, 5G, and upcoming 6G technologies. The choice of network technology is based on the application needs, which include communication range, bandwidth, energy usage, and latency [41], [46].
One of the major components related to this layer is Edge Computing, which is characterized by intelligence being brought close to the site of data generation. In edge computing, there are hardware and software solutions for the analysis and preprocessing of data prior to sending it into the cloud-based systems [14]. In case when the data collected by sensors is no different from the data received earlier, then an edge computing device can conclude that such information does not need to be sent to the cloud [47].

### 3.3 Cloud and Management Service Layer

Cloud and Management Services Layer enable powerful computation, storage, analysis, and management of IoT systems. Because IoT systems produce vast volumes of data, cloud platforms are able to provide scalable infrastructure that is capable of storing, processing, and analysing this data. Cloud IoT platforms enable significant operations, such as data management, device management, security management, service management, and intelligent analytics [42], [48].
The cloud layer analyses the collected data from the sensors by using sophisticated analysis techniques such as artificial intelligence, machine learning, and big data analytics. The insights from the analysis will assist organizations in making decision and automating many processes. In the case of the healthcare application, the cloud analysis the patient monitor data to aid in diagnosis and delivery of remote healthcare service, while in industrial applications it predicts equipment failures [48].
Another important task is security and device management. Cloud services have capabilities of providing authentication, authorization, access control, software updates, and monitoring mechanisms, thereby ensuring secure device operations. In addition, the cloud layer offers integration capabilities with a variety of domains of application such as retail, health care, emergency management, environment management, energy management, transportation, and smart cities [42], [48].

### 3.4 Application Layer

The Application Layer is the highest layer in IoT architecture and is used to provide services to users. It transforms processed data into usable applications that enable users to manage and control IoT systems. Services provided by this layer differ based on the specific domain and the needs of the user [40], [41].
Some of the areas where the application of IoT technology has been realized include smart homes, smart health care, smart farming, industry automation, smart transportation, and environmental monitoring. Some examples of smart home applications include control of lighting systems, home security systems, and household appliances using remote devices. Health care applications include remote patient monitoring through wearable devices. Industrial IoT applications entail the automation of industry processes [40], [42], [48].

In conclusion, IoT architecture involves interwoven layers that contribute towards making the sensing, communication, processing, and service delivery possible in the IoT system. The Sensors/Devices layer acquires data from the physical world while the Gateway & Network layer contributes towards facilitating communication. The Cloud/Management layer is responsible for data processing and security while the Application layer makes the intelligent solutions available to the end user [40], [41], [42].

## 4. Features of IOT

Internet of Things (IoT) has distinct features that differentiate it from the traditional networked technology. These features allow IoT systems to create intelligent communications among tangible items, gather and process huge amounts of data and provide automation services with little human involvement. The key features of IoT include connectivity, data analysis, integration, artificial intelligence, sensing, active participation and endpoint management. These features together help build intelligent systems that monitor, learn, adapt and make intelligent decisions [49], [50].

### 4.1 Connectivity

Connectivity is one of the basic characteristics of IoT because it facilitates the communication between physical devices, IoT platforms, cloud, and end-users. The key aim of connectivity is to ensure a reliable channel of communication between different IoT elements in order to allow an efficient exchange of data. IoT devices should be constantly connected to cloud services or servers in order to transfer their gathered data and get control commands [49], [51].

The current IoT systems employ different forms of communication technology like Wi-Fi, Bluetooth, Zigbee, RFID, Ethernet, cellular communications, LTE, and 5G. Once the IoT systems have been set up to be connected, they need to ensure secure and reliable two-way communications between the device and cloud services. Proper connectivity makes sure that information gathered from the sensors is relayed efficiently for analysis while enabling remote monitoring and management of the connected devices. Without proper connectivity, the IoT system will not be able to operate in real-time and automation [49], [52].

### 4.2 Data Analysis

Data analysis is yet another crucial aspect of IoT since data is constantly being generated from various sources due to the interconnection of the devices. However, it is not enough just to collect the data, since the essence of IoT lies in analysis of the collected data and gathering relevant information from it. IoT platforms employ different methods of data analysis such as machine learning, artificial intelligence, big data analytics, and predictive analysis [50], [53]. Analysis in real time of data collected provides means for organizations and their users to become more efficient as well as create smart services. Industrial IoT system analyses the performance data of machines to forecast any failure that is likely to take place, thereby saving cost on maintenance and increasing production. In the same manner, Healthcare IoT analyses the health data of patients and gives early warnings for medical care. As long as IoT system manages to comprehend and interpret the collected data, it becomes an intelligent system [53], [54].

### 4.3 Integration

Integration is a significant characteristic of IoT that enables different devices, platforms, applications, and technologies to work together as a unified system. IoT environments often involve heterogeneous devices manufactured by different organizations and operating through different communication protocols. Therefore, effective integration is required to ensure seamless communication and interoperability among various components [49], [55].

The combination of IoT along with other technologies such as cloud computing, artificial intelligence, blockchain, edge computing, and mobile applications increases the capacity of the system and provides a better experience to the user. For instance, in an intelligent home setup, lighting systems, surveillance cameras, smart devices, and environmental sensing equipment can all be integrated into a single system. The user is then able to manage different devices using one system only. Industrial systems also combine the use of IoT sensors with enterprise software [50], [55].

### 4.4 Artificial Intelligence

Artificial Intelligence (AI) is an important factor for the increase of intelligence and automation in IoT technologies. The integration of IoT with AI, termed as Artificial Intelligence of Things (AIoT), facilitates the devices in learning

through experience, making decisions and analysis of data. Through the use of AI algorithms, IoT devices can recognize patterns, predict events and react smartly to the environment [56], [57].
For instance, the intelligent coffee machine with IoT and AI functionality is able to keep track of the amount of coffee beans left in the machine, determine when they are going to run out, and place an order for their supply without human intervention. In addition, the AI-based smart cars are able to make decisions regarding the traffic conditions and routes to enhance safety while driving [56], [57].

### 4.5 Sensing Capability

Sense is among the main characteristics of the Internet of Things since the sensors play the role of the main tool that enables information collection from the surrounding environment. The Internet of Things sensors are responsible for detecting any changes in the environmental conditions and measuring physical parameters and then sending collected information to processing units [49], [50].
The sensoring feature is responsible for turning the conventional inert objects into interactive ones. In the absence of sensors, the Internet of Things environment cannot be able to sense and analyse what happens in reality. This can be seen through the environmental sensors which can sense air quality, smart agriculture sensors that can analyse soil moisture, and health sensors that can sense the health of humans [49], [58].

### 4.6 Active Engagement

The active interaction is yet another feature of the Internet of Things that facilitates constant interactions among the devices, services, and people. In contrast to traditional systems in which devices work independently, in the Internet of Things, devices actively interact with one another and adjust their actions to changes in situations [49], [50].
For instance, an intelligent thermostat can regulate room temperatures according to the preferences, environment, and energy consumption pattern. Similarly, smart cars can notify users about traffic, maintenance, and other safety issues in real time. The involvement of users makes the system more efficient as it eliminates the human intervention and allows the automation of connected devices [50], [59].

### 4.7 Endpoint Management

Endpoint management is crucial for the reliability, security, and efficiency of IoT systems. Because IoT systems may have thousands or even millions of connected devices, there must be effective endpoint management in order to guarantee smooth operation. Some of the components of endpoint management are authentication, updating, configuration management, monitoring, error checking, and security protection [60], [61].
Mismanagement of IoT end points may lead to various operational issues like failure, security risks, and even wrong functioning. Take the case of an automated coffee machine that orders coffee beans when there is a shortage of beans. In case of wrong detection of inventory or ordering of unnecessary beans when there are no users in the area for a few days, it will create difficulties and even cost money. It is thus important to have intelligent endpoint management tools for efficient functioning of IoT systems [60], [61].
Finally, the properties of the Internet of Things allow the creation of intelligent, automated, and connected systems. The connectivity property ensures that there is communication between the devices, the data analysis property provides insight from the collected data, the integration property allows different technologies to work together, and the artificial intelligence property improves decision-making. Likewise, the sensing, active participation, and endpoint management properties guarantee the proper functioning of the IoT elements during interaction [49], [50], [56], [60]

## 5. Applications of IoT

This IoT development has clearly been implemented in the current world by many industries. Due to its flexibility, it is favored by a large number of businesses and governments, and there is no reason not to implement it. These are some IoT applications [62], [63].

### 1. IoT Applications in Agriculture

The IoT system can help to measure the microclimatic conditions of the crops being grown indoors, resulting in increased production. As for outdoor cultivation, the IoT sensors, along with the weather details, will help to measure the required soil moisture and nutrients. With the help of smart irrigation systems, water is supplied to the required places and at the right time [64], [65].

**2. IoT Applications in Consumer Use**

Internet of Things gadgets available to citizens come in a portable variety and also the smart home varieties that make life convenient. These include wearable gadgets like Fitbit gadgets, smartphones, Apple Watches, health monitoring screens, and many others. These gadgets enhance entertainment, networking, health, and fitness [66]. Smart homes regulate functionalities that also have the capability of controlling the environment for comfort purposes once a person gets there. Functions like preparing food which uses the oven or the stove can be started remotely such that when one reaches there, the food is already prepared. This makes the security issue much easier as one will be in a position to start and stop the gadgets from afar and also start the smart lock system [63], [66].

**3. IoT Applications in Healthcare**

The objective of IoT mobile devices is to enable hospitals to monitor the health of patients even at their homes by shortening their stays in hospitals while receiving information that is vital to save lives. The smart beds at hospitals assist in giving information about bed Availability, thus minimizing the time taken for a patient to wait until getting admitted owing to lack of bed Availability. IoT sensors installation on complex devices makes them less prone to crashes and reliable [67].

Taking care of the elderly becomes much easier using IoT. Apart from this monitoring facility, the sensors are also capable of sensing adverse occurrences like falling of the patients or heart attacks [67].

**4. IoT Applications in Insurance**

The revolution of the Internet of Things will positively impact the insurance industry. Insurance companies can give discounts to their customers in accordance with the statistics provided by the Internet of Things, including the data generated by Fitbit devices. In such instances, by incorporating the idea of health tracking, insurance companies can offer customized insurance policies [68].

**5. IoT Applications in Manufacturing**

Manufacturing and industrial automation industry becomes second biggest winner in the draws of IoT. Technology like RFID and GPS could help to monitor the whole supply chain from beginning to end on the factory floor, from installation till delivering the products in the destination store. subject to production of data, information could be obtained by the sensors concerning environmental conditions, state of the product and its delivery time [69]. The sensors installed to the equipment in the factory could help to identify the breakdowns in the process of product manufacturing, thus saving time and energy. Other sensors installed to the same machines could help to control the work of the machine and predict the moments when the unit would need repair [69].

**6. IoT Applications in Retail**

IoT technology can be of great use in retail industry. The statistics of sales made both online and, in the shop, can evaluate the automation and robotics in the warehouse, the information collected from IoT sensors. All of it is done with the help of RFIDs, which are already used in many countries worldwide [70].

Trademark sites are things'; Companies are changing and the arrival of online shopping has decreased the number of brick-and-mortar sites. But IoT can provide analysis of the traffic in the shopping mall so that the shops could make the necessary changes to provide better customer experience and lower costs [70]. As far as customer engagement goes, based on the previous purchases, IoT helps to target customers. Provided with information gathered by IoT, retailers are able to make personalized offers for the customers, who do not require costly bulk marketing promotions, which bring less chances of success. The majority of such offers can be made using the smartphones of customers, even if they have the application of the right store [70].

**7. IoT Applications in Transportation**

However, by this time, people are aware of achievements in the field of autonomous vehicles. Yet this is not even half of the possibilities in transport. GPS, as we think about it, is another example of the Internet of Things application, helping transport companies design faster and more efficient routes for their trucks, making deliveries faster [71].

Quite a lot of developments have already been achieved in the sphere of navigation, once again reminding us of GPS in our phones or cars. However, city planners could also take advantage of this information to improve traffic flow, parking and construction and road maintenance [71].

If the driver finds himself in a situation similar to dunked, then apps can stop your car from moving, which is also possible in this situation.

**8. IoT Applications in Utilities/Energy**

The IoT sensors can be deployed for monitoring the environmental factors like humidity, temperature, and lighting levels. The information gathered from IoT sensors can be utilized for developing algorithms to regulate energy usage and make the required modifications without resorting to any human equations [72].

Utilization of IoT-based environmental regulation helps organizations and individuals save on energy costs and in turn contributes to the betterment of all, even the environment [72].

The data gathered through the Internet of Things can be analysed with the help of factors like usage and help in making the municipal power grid work effectively. The sensor can aid in identifying any malfunction and increase the response time of the repair shop and reduce the blackout period [72].

## 6. Conclusion

The advent of the Internet of Things (IoT) is revolutionizing workplaces and personal lives with intelligent connectivity, automation, and effective decision-making through big data. The development in areas like sensors, communication, cloud computing, and artificial intelligence has made IoT an indispensable technology in industries like healthcare, industry, transport, agriculture, and even smart home devices. There are many IoT applications that have already become an integral part of our day-to-day activities providing efficiency, remote monitoring, and control. Despite limitations like security, privacy, and interoperability, technological developments are constantly overcoming these limitations. The growth in IoT is unstoppable and will continue to be an indispensable technology in the future.

## References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.

[3] G. Godhani and M. Dhamecha, "A Study on Movie Recommendation System Using Parallel MapReduce Technology,", Vol.5, Issue 1, page no.375-378, IJEDR – 2017. https://rjwave.org/IJEDR/papers/IJEDR1701058.pdf

[4] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, Sep. 2012, doi: 10.1016/j.adhoc.2012.02.016.

[5] M. Dhamecha, A. Ganatra, and C. K. Bhensadadiya, "Comprehensive Study of Hierarchical Clustering Algorithm and Comparison with Different Clustering Algorithms," CiiT Int. J., 2011.

[6] K. Ashton, "That 'Internet of Things' thing," RFID Journal, Jun. 22, 2009. [Online]. Available: RFID Journal.

[7] S. Sarma, D. L. Brock, and K. Ashton, "The networked physical world," MIT Auto-ID Center, Cambridge, MA, USA, Tech. Rep. MIT-AUTOID-WH-001, 2000.

[8] D. Chandarana and M. Dhamecha, "A Survey for Different Approaches of Outlier Detection in Data Mining," in Proc. IEEE, 2015. doi: 10.1109/EESCO.2015.7253811

[9] J. Qi, P. Yang, G. Min, O. Amft, F. Dong, and L. Xu, "Advanced internet of things for personalised healthcare systems: A survey," Pervasive and Mobile Computing, vol. 41, pp. 132–149, Oct. 2017, doi: 10.1016/j.pmcj.2017.06.018.

[10] K. Parmar, N. Limbasiya, and M. Dhamecha, "Feature-based Composite Approach for Sarcasm Detection Using MapReduce," in Proc. IEEE, 2018. DOI: 10.1109/ICCMC.2018.8488096.

[11] A. K. S. Al-Fuqaha et al., "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, Fourth Quarter 2015, doi: 10.1109/COMST.2015.2444095.

[12] Y. Yin, Y. Zeng, X. Chen, and Y. Fan, “The internet of things in healthcare: An overview,” Journal of Industrial Information Integration, vol. 1, pp. 3–13, Mar. 2016, doi: 10.1016/j.jii.2016.03.004.
[13] M. Dhamecha, “Improve K-Mean Clustering Algorithm in Large-Scale Data for Accuracy Improvement,” AISC, 2021. https://doi.org/10.1007/978-981-15-9516-5_5.
[14] Urvi Darji, Shruti Oza, Kruti P. Thakor “Design Of PFD With Charge Pump For DPLL In 0.18μm CMOS Technology”, NCAET (2012)
[15] K. Boeckl, M. Fagan, B. Fisher, N. Lefkovitz, K. Megas, E. Nadeau, B. Piccarreta, D. O'Rourke, and K. Scarfone, “Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks,” NIST Interagency/Internal Report NISTIR 8228, National Institute of Standards and Technology, Gaithersburg, MD, USA, Jun. 2019, doi: 10.6028/NIST.IR.8228.
[16] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.
[17] M. Dhamecha, “An Efficient Comparison between Structured Analysis and Object-Oriented Analysis,” IJSRCSEIT, 2021. https://doi.org/10.32628/CSEIT217369
[18] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, Fourth Quarter 2015, doi: 10.1109/COMST.2015.2444095.
[19] A. A. A. Soltan, M. H. Alshamrani, and A. M. Alghamdi, “A survey on Internet of Things security: Requirements, challenges, and solutions,” Internet of Things, vol. 11, Art. no. 100284, Sep. 2020.
[20] M. Dhamecha, “Plant Recommendation System with the Use of Weather Forecasting,” CEUR Workshop Proc., 2021.
[21] C. Sharma, “Correcting the IoT history,” Chetan Sharma Consulting, 2020. [Online]. Available: https://www.chetansharma.com/publications/correcting-the-iot-history/
[22] K. Ashton, “That ‘Internet of Things’ thing,” RFID Journal, Jun. 22, 2009. [Online]. Available: https://www.rfidjournal.com/expert-views/that-internet-of-things-thing/
[23] M. Dhamecha, “Optimize Ant Colony Algorithm with Relation of Efficiency and Performance for the Traveling Salesman Problem,” GRADIVA, 2021.
[24] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, “Middleware for Internet of Things: A survey,” IEEE Internet of Things Journal, vol. 3, no. 1, pp. 70–95, Feb. 2016, doi: 10.1109/JIOT.2015.2498900.
[25] A. Čolaković and M. Hadžialić, “Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues,” Computer Networks, vol. 144, pp. 17–39, Oct. 2018, doi: 10.1016/j.comnet.2018.07.017.
[26] A. Banks and R. Gupta, “MQTT Version 3.1.1,” OASIS Standard, Oct. 29, 2014.
[27] M. Dhamecha, “Fundamentals of ANN and Basic Algorithm of Neural Network in Data Analytics,” MOENIA, 2021.
[28] M. Botta, W. de Donato, V. Persico, and A. Pescapé, “Integration of cloud computing and Internet of Things: A survey,” Future Generation Computer Systems, vol. 56, pp. 684–700, Mar. 2016, doi: 10.1016/j.future.2015.09.021.
[29] P. Bellavista, J. Berrocal, A. Corradi, S. K. Das, L. Foschini, and A. Zanni, “A survey on fog computing for the Internet of Things,” Pervasive and Mobile Computing, vol. 52, pp. 71–99, Jan. 2019, doi: 10.1016/j.pmcj.2018.12.007.
[30] M. Dhamecha, “Study of Search Engines with the Paradigm of Machine Learning,” SAMRIDDHI – J. Phys. Sci. Eng. Technol., 2022.
[31] M. Dhamecha, “Literature Survey of Basic Methodologies in Cloud Computing,” SAMRIDDHI – J. Phys. Sci. Eng. Technol., 2022.
[32] M. S. Al-Khafajiy, T. Baker, A. Al-Libawy, A. Maamar, M. Aloqaily, and Y. Jararweh, “Improving fog computing with multi-agent systems,” IEEE Access, vol. 7, pp. 16426–16445, 2019, doi: 10.1109/ACCESS.2019.2893207.
[33] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations,” IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702–2733, Third Quarter 2019, doi: 10.1109/COMST.2019.2910750.
[34] M. A. Ferrag, L. Maglaras, H. Janicke, J. Jiang, and L. Shu, “Authentication protocols for Internet of Things: A comprehensive survey,” Security and Communication Networks, vol. 2017, Art. no. 6562953, 2017, doi: 10.1155/2017/6562953.

[35] M. Dhamecha, "Fundamental Study of Chatbot with the Use of Artificial Intelligence," SODHASAMHITA, 2022.
[36] M. A. A. Alahi, S. Mukhopadhyay, L. Sharma, and S. Mukhopadhyay, "Artificial intelligence and machine learning in Internet of Things: A systematic review," Internet of Things, vol. 19, Art. no. 100552, Oct. 2022.
[37] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/j.comnet.2014.11.008.
[38] M. Dhamecha, "Literature Survey for Outlier Detection Methods in Data Analytics," TANZ Res. J., vol. 9, no. 12, pp. 139–142, 2023, doi: 10.6084/doi.23.9.11.TANZ21837.
[39] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital twin: Enabling technologies, challenges and open research," IEEE Access, vol. 8, pp. 108952–108971, 2020, doi: 10.1109/ACCESS.2020.2998358.
[40] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.
[41] M. Dhamecha and U. Dhamecha, "Prediction of Air Quality Index Affected by Vehicle Emissions Using Machine Learning," Int. J. Environ. Sci., vol. 11, no. 21, pp. 1566–1571, 2025, doi: 10.64252/r2d6a722.
[42] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.
[43] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A survey," IEEE Internet of Things Journal, vol. 3, no. 1, pp. 70–95, Feb. 2016, doi: 10.1109/JIOT.2015.2498900.
[44] M. Dhamecha and U. Dhamecha, "Behavioral Detection of Ransomware and a Comprehensive Approach to Ransomware Prevention," IEEE Commun. Standards Mag., vol. 11, no. 21, pp. 1–7, 2025, doi: 10.1109/MCOMSTD.2025.3616108.
[45] A. Gluhak, M. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. R. Razafindralambo, "A survey on facilities for experimental Internet of Things research," IEEE Communications Magazine, vol. 49, no. 11, pp. 58–67, Nov. 2011, doi: 10.1109/MCOM.2011.6069713.
[46] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," Computer Networks, vol. 144, pp. 17–39, Oct. 2018, doi: 10.1016/j.comnet.2018.07.017.
[47] Urvi Darji, Shruti Oza, Kruti P. Thakor "Low power and low jitter phase frequency detector for dpll using 0.18µm cmos technology", ICIKR-ETS (2012)
[48] M. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," Future Generation Computer Systems, vol. 56, pp. 684–700, Mar. 2016, doi: 10.1016/j.future.2015.09.021.
[49] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.
[50] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.
[51] V. Vyas, M. Dhamecha and U. Dhamecha, "Performance Evaluation of Hashgraph Algorithm in IoT: Execution Time and CPU Usage in DLT Systems" Advances in Nonlinear Variational Inequalities, vol. 27, no. 4, pp. 606–617, 2024, doi: https://doi.org/10.52783/anvi.v27.6397.
[52] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," Computer Networks, vol. 144, pp. 17–39, Oct. 2018, doi: 10.1016/j.comnet.2018.07.017.
[53] M. Chen, S. Mao, and Y. Liu, "Big data: A survey," Mobile Networks and Applications, vol. 19, pp. 171–209, Apr. 2014, doi: 10.1007/s11036-013-0489-0.
[54] J. Qi, P. Yang, G. Min, O. Amft, F. Dong, and L. Xu, "Advanced internet of things for personalised healthcare systems: A survey," Pervasive and Mobile Computing, vol. 41, pp. 132–149, Oct. 2017, doi: 10.1016/j.pmcj.2017.06.018.
[55] V. Vyas, M. Dhamecha and U. Dhamecha, "Cognitive Storage Techniques Using Popularity Heuristics in Big Data Frameworks" Communications on Applied Nonlinear Analysis, vol. 31, no. 8, pp. 1262–1276, 2024, doi: https://doi.org/10.52783/cana.v31.6392.
[56] A. S. D. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, Fourth Quarter 2015, doi: 10.1109/COMST.2015.2444095.
[57] X. Liu, X. Zhang, and W. Sun, "Artificial intelligence of things: A survey," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9447–9463, Jun. 2021.

[58] A. Ray, M. Chowdhury, and S. Neogy, "IoT-based smart agriculture: A comprehensive review," IEEE Access, vol. 9, pp. 123456–123475, 2021.

[59] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.

[60] B. Kathiriya, V. Vyas, M. Dhamecha, "Optimizing Fuzzy Decision Systems with the Jaya Algorithm for Enhanced Data Transfer in Multi-Hop CRNs" Franklin Open, Elsevier, vol. 16, 2026, doi: https://doi.org/10.1016/j.fraope.2026.100722.

[61] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702–2733, Third Quarter 2019, doi: 10.1109/COMST.2019.2910750.

[62] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[63] C. Perera, C. H. Liu, and S. Jayawardena, "The emerging Internet of Things marketplace from an industrial perspective: A survey," IEEE Trans. Emerging Topics Comput., vol. 3, no. 4, pp. 585–598, Dec. 2015, doi: 10.1109/TETC.2015.2390034.

[64] M. N. Mowla, N. Mowla, A. F. M. S. Shah, K. M. Rabie, and T. Shongwe, "Internet of Things and wireless sensor networks for smart agriculture applications: A survey," IEEE Access, vol. 11, pp. 145813–145852, 2023, doi: 10.1109/ACCESS.2023.3346299.

[65] H. Hammouch, M. A. El-Yacoubi, H. Qin, and H. Berbia, "A systematic review and meta-analysis of intelligent irrigation systems," IEEE Access, vol. 12, pp. 128285–128304, 2024, doi: 10.1109/ACCESS.2024.3421322.

[66] F. J. Dian, R. Vahidnia, and A. Rahmati, "Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A survey," IEEE Access, vol. 8, pp. 69200–69211, 2020, doi: 10.1109/ACCESS.2020.2986329.

[67] M. Dhamecha, U. Dhamecha, "Survey of Allaying Vulnerabilities for Cloud based Security in Zero Trust Architecture" International Journal of Computer Information Systems and Industrial Management Applications, vol. 18, pp. 1046–1055, 2026, doi: https://doi.org/10.70917/ijcisim-2026-3695.

[68] B. Chakraborty and S. S. S. S. Kumar, "The adaptation of Internet of Things in the Indian insurance industry—Reviewing the challenges and potential solutions," Electronics, vol. 11, no. 3, Art. no. 419, 2022, doi: 10.3390/electronics11030419.

[69] M. Boyes, B. Hallaq, J. Cunningham, and A. Watson, "The industrial internet of things (IIoT): An analysis framework," Comput. Ind., vol. 101, pp. 1–15, Oct. 2018.

[70] C. Perera, C. H. Liu, and S. Jayawardena, "The emerging Internet of Things marketplace from an industrial perspective: A survey," IEEE Trans. Emerging Topics Comput., vol. 3, no. 4, pp. 585–598, Dec. 2015, doi: 10.1109/TETC.2015.2390034.

[71] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of wireless sensor networks towards the Internet of Things: A survey," in Proc. 19th Int. Conf. Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2011, pp. 1–6.

[72] S. M. A. Abir, A. Anwar, J. Choi, and A. S. M. Kayes, "IoT-enabled smart energy grid: Applications and challenges," IEEE Access, vol. 9, pp. 50957–50975, 2021, doi: 10.1109/ACCESS.2021.3067331