JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Internet of Things: Applications, Architecture, and Security Issues

**[1]Nazia Parveen, [2]Aleem Ali, [3]Yogita Chauhan**

[1]Research Scholar, [2]Associate Professor,[3]Research Scholar
[1]Department of Computer Science & Engineering,
[1]Department of Computer Science & Engineering, Glocal University, Saharanpur, India

***Abstract :*** The term "Internet of Things" (IoT) seems to have become synonymous with information technology.The phrase "immensely" affects us. In recent years, it has gained increased recognition. The Internet of Things (IoT) is a new technology that is transforming practically every industry today. A network of billions of objects that can communicate with one another is what is meant by the term "internet of things." The goal of the Internet of Things is to bring all the gadgets together under one roof. These devices are always under constant observation and supervision.They are able to converse, share information, and carry out the required tasks. In light of this, the work analyses research papers, business persuasive reports, scholarly review articles, and web resources to address the IoT notion. The paper also provides a comprehensive description of the Internet of Things, including its definition, history, obligations, aliases, architecture, and several technologies that are frequently employed in it. The study also touches on security issues and its application domains.

***Keywords* – IoT, M2M, EPC, Bluetooth , Actuators ,WSN, V2V, RFID, Zigbee, NFC.**

## 1. INTRODUCTION

Technology permeates practically every facet of our lives nowadays. We all rely on it in some way. In the field of information technology, the phrase "Internet of Things" (IoT) represents a paradigm shift. [9]. IoT creates a connected and effective communication environment. It makes it possible for the gadgets or things to communicate with other gadgets and people wherever they are and whenever they want. [11]. Than the individuals around us, there are more connected items. Computers, laptops, smartphones, tablets, and other embedded devices are some of these items or things. The gadgets have sensors and actuators that perceive the environment and gather data. IoT is simply an ecosystem where real-world items are connected via established protocols to exchange information. [1]. All of these objects exhibit cognitive behaviour, cleverly analyse the information, and draw insightful conclusions. IoT is recognized as a key area for cutting-edge technology. Smart Homes, Smart Cities, Healthcare, Industries, Environmental Protection, Commercial, and many more are among the various IoT application sectors.

The internet of things can be defined as a world that is digitally connected and has objects that are integrated with internet connectivity, sensors, actuators, and other hardware that enables communication through the web.

IoT is made up of the following four elements:

- **Devices/Sensors:**These gadgets gather information from their environment and transform it into useful information**.**
- **Connectivity:** Sensor data is being transmitted to a cloud infrastructure. Data transportation requires a medium. The sensors are connected to the cloud through a number of different mediums, including Bluetooth, WiFi, cellular networks, satellite networks, etc [6].

**- Data Processing*:*** When data is transferred to the cloud, the programme processes the data.
**- User Interface:** The end user will thereafter have access to the information. An interface is available for users to check in on their Internet of Things system [3].

## 2. GENESIS

The Internet of Things, which represents a revolution in the industrial sector, personifies the future of computation and communication. The first time a soda machine was connected to the internet was in the early 1980s [5].

A team of programmers installed and ran this machine at Carnegie Mellon University. Later, after checking the machine's status, the programmers decide whether or not a cool beverage will be ready for them. Kevin Ashton at MIT first used the phrase in 1999 [14]. The IoT concept first gained popularity in 2003. During the initial phase, a large number of devices or objects were linked to the internet[2]. These devices or objects are linked to serve various applications using a variety of technologies.

## 3. IoT CHRONOLOGY

The invention of the Internet in the late 1960s gave rise to the idea of the Internet of Things. The tests revealed that the first connected gadget was a Coca-Cola machine at Carnegie Mellon University. IoT was invented in 1999 at MIT by Kevin Ashton, who is credited with being its pioneer.

1982: Students at Carnegie Mellon University, which was connected to the ARPANET, created the coke machine.
1990: Using the TCP/IP protocol, John Romkey linked a toaster to the computer.
1994: Steve Mann invented a wearable camera that is connected to the Internet.
1999: The phrase "Internet of Things" is first used by Kevin Ashton.
2000: The first refrigerator with Internet connectivity is unveiled by LG.

2004: IoT is first mentioned in a book title.

2008: In Zurich, Switzerland, there was the inaugural International Conference on Internet of Things.
2011: IoT is now included in Gartner's hype cycle.
2014: There are more connected gadgets than there are people.
2016: First malware detected for IoT
2018: The government begins to consider IoT security issues.
2020: Around 50 billion linked devices are anticipated, and the IoT market is projected to be worth $8.9 trillion.

## 4. IoT ARCHITECTURE

Since the idea is so broad, no uniform architecture has been suggested for it. Researchers, experts, and scholars presented various IoT architecture [3].
The Architecture, which comprises of the layers for perception, network, and application, was first introduced [11]. Three-layer architecture is the name given to this design and shown in Fig 1.

### *4.1 Three-Layer Architecture*

**- Perception Layer:** The physical layer is another name for the perception layer. Sensors in this layer are used to sense the environment and acquire data. The sensors gather data from various objects during this phase, and the actuators later use that data to perform precise operations [1].

**- Network Layer:** This layer establishes an interface link between the application layer and perception layer by acting as an intermediary layer between the two. The network layer manages connections to servers and other devices.

- **Application Layer:** The implementation of IoT takes place at the application layer. The functionality of the sensors and actuators is managed by the application layer. It might also be viewed as software that utilizes sensors.

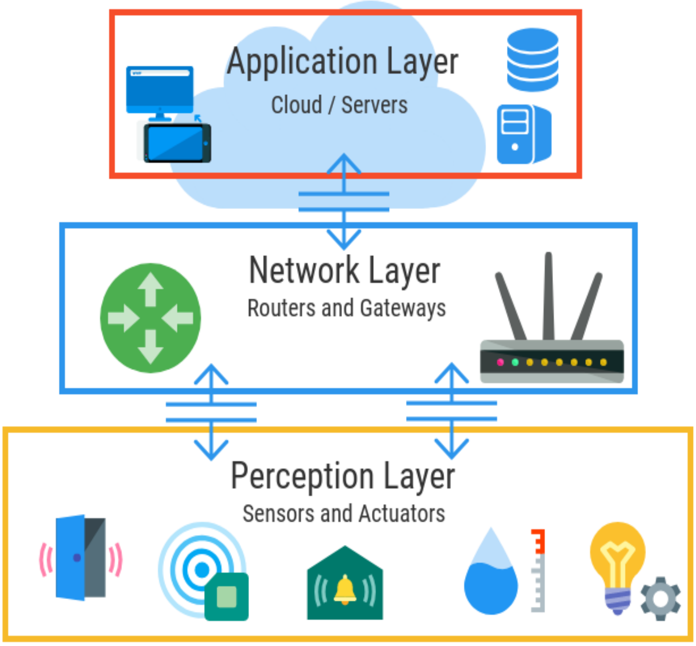

**Fig 1. Three-Layer Architecture of IoT**

The three-layer IoT architecture was not well suited for existing technologies, so a new architecture was created. The perception, transport, processing, application, and business layers make up this new architecture [6]. Five-Layer Architecture is the term given to it.

### 4.2 Five-Layer Architecture

When project work is done with various cutting edge technologies and broad application area, 5 layer architecture is considered as best. 5 Layer model can be considered as an extension to the basic architecture of IoT because it has two additional layers to the basic model as shown in Fig 2.

- **Perception Layer:** Similar functions to those in the three-layer architecture are performed by this layer. At this layer, the data collected from sensors is put into practice.
- **Transport Layer:** Data from the perception layer is transmitted to the processing layer with the aid of the transport layer.The transport layer uses a variety of technologies, including LAN, wireless technology, 3G, 4G, LTE, and RFID.
- **Processing Layer:** The middleware layer is another name for this layer. At the Processing layer, the entire information will be processed. This layer makes use of a variety of technologies, including big data processing modules, cloud computing, databases, etc. An enormous amount of information will be stored by using such methods. After successfully storing the data, it will examine how to retrieve the data in order to provide the desired result.
- **Application Layer:** It is in charge of making IoT function. It outlines the IoT applications that are used.
- **Business Layer:** The Business layer controls how the entire IoT system operates.

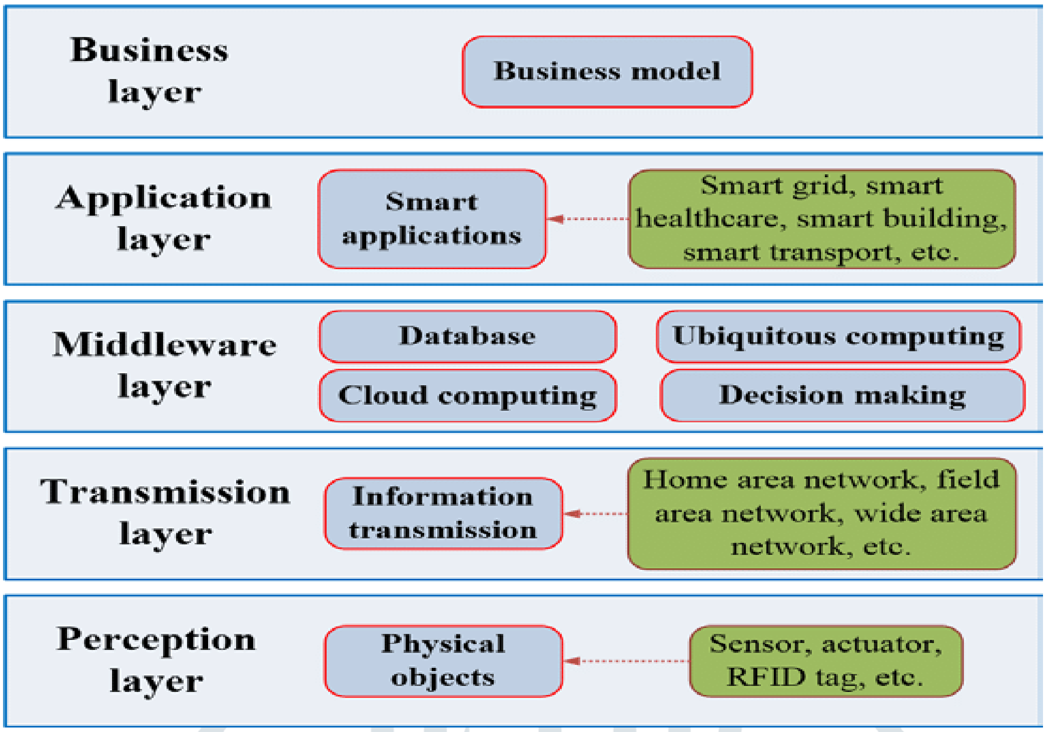

**Fig 2: Five-Layer rchitecture of IoT**

## 5. TECHNOLOGIES USED IN IoT

The Internet of Things employs a variety of technologies, some of which are listed below.[1]

5.1 Radio frequency Identification (RFID)

5.2 Near Field Communication (NFC)

5.3 Machine to Machine Communication (MtoM)

5.4 Vehicle to Vehicle Communication (VtoV)

5.5 Electronic Product Code (EPC)

5.6 Wireless Fidelity (Wi-Fi)

5.7 Bluetooth

5.8 ZigBee

5.9 Actuators

5.10 WSN (Wireless Sensor Network).

## 6. IoT APPLICATIONS

The Internet of Things gave the objects cognition and connectedness. Applications for IoT are paving the path for adding lasting value to our lives. IoT is being used in many different fields [4].

### 6.1 Connected Healthcare System

The Internet of Things is very important for health care. The technology-driven connected healthcare system could improve the effectiveness and standard of care. IoT in healthcare permits information sharing, machine-to-machine connection, and intercommunication to ensure adequate delivery of healthcare services [5].

The IoT gadgets can keep an eye on a patient's medical file. Sensors can be used to track data about a person's body temperature, heart rate, blood pressure, etc. In the event of an emergency, the patient's doctor will receive notification of all the data that these sensors have collected [18]. The connected setup lowers costs by making better use of resources, reducing pointless visits, and improving planning and allocation[6].

### 6.2 Smart Home Automation

This IoT application allows customers access to gadgets and applications that may be grouped to give them complete control over their homes. Recently, there has been discussion on how the world is interconnected with just a touch of the fingertip or a straightforward voice command to Alexa, Google Assistant, Siri, or Cortana [7]. Home automation enables you to unlock your door from anywhere in the world, turn your lights on and off with a single touch, and detect motion in your home.

### 6.3 Smart Cities

Another strong IoT application is smart cities. Technology is advancing quickly to streamline cities. The goal of a smart city is to improve people's quality of life by reducing traffic congestion, spotting energy supply shortages, preserving open parking spaces, analysing air quality, etc [8].

### 6.4 Smart Farming

Today's farming is more technologically oriented. The Internet of Things has a covert objective to increase agricultural productivity at a lesser cost. It provides an opportunity for professionals to pave the road for smart farming solutions [9]. Using smart agriculture tools, farmers can gain control over the process of raising livestock and cultivating crops.

### 6.5 Smart Grid

The traditional energy grid's issues are addressed by the idea of a "smart grid." It is a communication network that gathers and analyses data and remotely monitors everything from lighting to traffic signs to parking spots to road warnings and everything in between [10]. The traditional power system's issues with unidirectional information flow, energy waste, dependability, and security are all resolved by a smart grid.

### 6.6 Industrial Automation

By automating various industries, IoT devices are bringing about amazing improvements. Industrial automation, which employs numerous control devices to manage various processes and machines in an industry, is being more favoured and adopted by industries. As a result, less human interaction is required [12]. The size of the industrial market is anticipated to reach 73.5 billion US dollars by 2023, which underlines the expansion of IoT in Industrial Automation, according to the current analysis.

### 6.7 Connected Cars

In response to the rapid improvements in technology, vehicle manufacturers now provide new services. Autonomous driving is made possible by networked car environments, which also redefines what it means to be mobile. With the ability to make judgments quickly and consistently, connected cars have a network of sensors, antennas, embedded software, and communication technologies at their disposal. By 2026, the market for globally connected cars is anticipated to reach $280.36 billion, according to the market research consulting organization. In cars that are connected, comfort, performance, safety, and security are prioritized alongside connectivity.

### 6.8 Smart Retail

IoT enhances the retail industry by incorporating cutting-edge digital instruments into this procedure. It provides retail businesses with precise consumer behaviour data. Retailers are choosing to use IoT solutions to modernize shop operations, decrease theft, increase pick up, and approve precise inventory control.

## 7. SECURITY ISSUES OF IoT

The technological and security problems are two broad categories for security worries. The heterogeneous and pervasive nature of IoT devices is a cause for technological concern, yet the processes that need to be put in place to achieve a protected network provide security conundrums[9]. Technology difficulties are those related to distributed nature, extending capabilities, and wireless technologies. Issues with security demand the ability to defend security through authentication, confidentiality, end-to-end protection, integrity, etc. The security regulations given below must be taken into account in order to achieve a secure communication.

### 7.1 Confidentiality

Only authorized users should have access to data in order to maintain confidentiality. In a nutshell, an IoT user can be an internal object, a human, or a gadget [2]. As a result, it is difficult to guarantee that sensors won't share the obtained data with nearby objects. Making people familiar with data management tools is a crucial difficulty in ensuring data protection.

### 7.2 Integrity

Since connected devices are now exchanging data, it is crucial to confirm that the data is coming from the correct source and has not been altered during connection. Integrity in IoT communication can be achieved by maintaining end-to-end security. Although data flow is handled by firewalls and protocols, this does not guarantee endpoint security.

### 7.3 Availability

IoT planned to link a sizable number of smart gadgets. Users should always have access to data whenever they need it, and devices and services should also be readily available.

### 7.4 Authentication

Every object in the linked environment needs to be able to identify and authenticate other objects. This approach can be difficult due to the nature of IoT, as objects, people, processing units, support, and access providers are perplexed. As a result, a method must authenticate these items while the two parties are interacting[5].

### 7.5 Lightweight Solutions

A distinctive security measure A lightweight method is introduced to get over the devices' drawbacks, namely their lack of computing and power efficiency. This is a limitation that needs to be taken into account while creating protocols for data and devices.

### 7.6 Heterogeneity

IoT includes a variety of items or things with unique capabilities, complexities, Features, Versions, and technological features. The shift in environment that occurs anytime a device communicates with different devices is another issue that is investigated. An ideal cryptography system and compatible security protocols are needed to achieve security.

## 8 CONCLUSION

The Internet of Things is currently a well-known term. The Internet is necessary for device and item communication. Everyone is somewhat susceptible to technology. It becomes necessary in today's world. Both people and things are typically interconnected. The security of these gadgets while communicating is one of the main problems. Device compatibility is another problem. The Internet of Things has been the subject of a lot of study, but there is still more to be done. It is necessary to use efficient technology and accepted protocols to make this area a little bit more dependable and secure.

## References

[1] Patel, A.K. and Patel, B.M., 2016. Internet of things (IoT): A literature review. IJSRD—International Journal for Scientific Research &Development, 4(5), pp.1001–1003.

[2] Saleem, Y., Crespi, N. and Rehmani, H.M., Internet of things-aided smart grid: Technologies, architectures, applications, prototypes, and future research directions.

[3] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., 2013. Internet of things (IoT): A vision. Architectural Elements, and Future Directions, 29(7), pp.1645–1660.

[4] Banka, S., Madan, I. and Saranya S., 2018. Smart healthcare monitoring using IoT. International Journal of Applied Engineering Research, 13(15), pp.11984–1

[5] Lee, I. and Lee K., The internet of things (IoT): Applications, investments, and challenges for enterprises.

[6] Daniel Minoli; Kazem Sohraby: IoT Considerations, Requirements, and Architectures for Smart Buildings—Energy Optimization and Next-Generation Building Management Systems

[7] Nihong Wang, Wenjing Wu, 2012 The ArchitectureAnalysis of Internet of Things, Computer and ComputingTechnologies in Agriculture V IFIP Advances inInformation and Communication Technology, 193-198

[8] Sudip Misra, P. Venkata Krishna, Harshit Agarwal,Anshima Gupta, Mohammed S.Obaidat, 2012 AnAdaptive Learning Approach for Fault-Tolerant Routingin Internet of Things. IEEE Wireless Communicationsand Networking Conference: PHY and Fundamentals,815 – 819.

[9] L. Atzori, A. lera, G. Morabito, The Internet of Things: Survey. Computer networks, 2787–2805.

[10] Polgavande, A.S. and Kulkarni, A.D., 2017. Internet of things (IoT): A literature review. International Journal of Research in Advent Technology (IJRAT) Special Issue, E-ISSN: 2321-9637.

[11] Asghar, M.H., RFID and EPC as key technology on Internet of Things (IoT), pp.121–123, ISSN: 0976-8491 (Online), ISSN: 2229- 4333 (Print).

[12] Sedrati, A. and Mezrioui A., 2018. A survey of security challenges in internet of things. Advances in Science, Technology and Engineering Systems Journal, 3(1), pp.274–280.