International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-06, Issue-09, DEC 2020

# A Literature Survey on Internet of Things

**P.V.Vijaya Durga, Asst.Prof, VIT, Bhimavaram, India, vijji210@gmail.com**

**T.Sujith Kumar, Asst.Prof, VIT, Bhimavaram, India, tsujithkumar.108@gmail.com**

**ABSTRACT: This paper provides the brief introduction about Internet of Things(IOT). The interesting fact of IOT is integration of various technologies and tools like smart sensors, communication technologies, Internet Protocols. Day to Day the world changes with full of devices, sensors and other objects which will communicate and make human life far better and easier than ever. This paper provides an overview of current research work on IoT in terms of architecture, technologies and applications. The main purpose of this survey is to show all the latest technologies, their corresponding trends and details in the field of IoT in a systematic manner.**

**Keywords:** ***Internet Of Things(IOT),RFID,M2M,V2V,NFC.***

## I. INTRODUCTION

Internet of Things can be defined as the combination of two terms: one is Internet, which is defined as networks of networks which can connect a lot of users with some standard internet protocols. The second term is Thing, this term is basically mean to these devices or real world objects which turn into intelligent objects. IOT can be defined as "Internet of Things "(IOT)[1] is a network of physical objects or people called things which can sense, accumulate and transfer data over the internet without any human intervention".

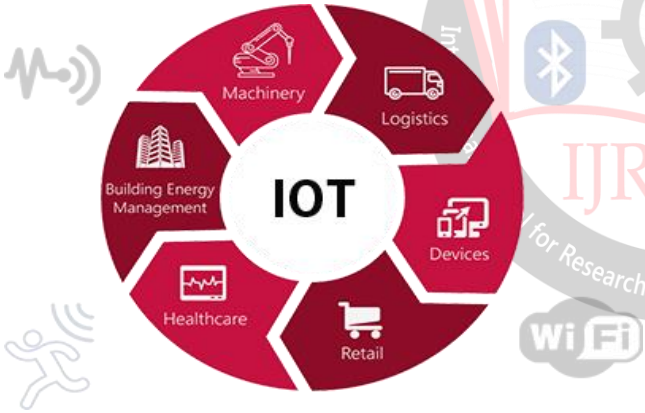


**Figure 1: Internet Of Things(IOT)**

## II. HISTORY OF IOT

The IoT domain become a world of technology and communication to a new era where objects can communicate, compute and transform the information as per the requirements. The term Internet of Things was Proposed by Kevin Auston,

The Executive Director of Auto-ID Labs in MIT in 1999.The table 1 shows the entire history about IOT [9].

| Year | Industrial Participation & Involvement |
|---|---|
| 1970 | The idea of connected devices was proposed |
| 1990 | Romkey created a toaster which could be turned on/off over the Internet |
| 1995 | Siemens introduced the first cellular module built for M2M technologies. |
| 1999 | The term "Internet of Things" was used by Kevin Ashton during his work at P&G became widely accepted |
| 2004 | The term was mentioned inthe famous publications like the Guardian, Boston Globe.. |
| 2005 | UN's International Telecommunications Union (ITU) published its first report on this topic. |
| 2008 | The Internet of Things was born |
| 2011 | Gartner, the market research company, include "The Internet of Things" technology in their research work. |

**Table – 1. History of Internet of Things**

## III. ARCHITECTURE

There is no fixed architecture for IoT,[5]Different architectures have been proposed by different researchers.

### 3.1 Three- and Five-Layer Architectures

The basic architecture is a three-layer architecture as shown in Figure 1. It was introduced in the early stages of research in this area. The three layers are namely, the perception, network, and application layers.

 DOI : 10.35291/2454-9150.2020.0717 

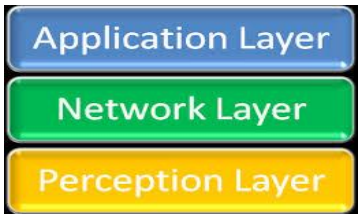


**Figure 2: 2 - 3 Layer Architecture**

**1. Perception Layer -** This layer also called as physical layer, collects data/information and recognizes the physical world. In this layer all the actuators work according to the information collected by the sensors of different object in order to perform specific operations by the corresponding objects.

**2. Network Layer** - Network layer is the middle layer, it establishes an interface link between application layer and perceptual layer. It is responsible for the initial dataprocessing, data broadcasting and connecting devices.

**3. Application Layer- This** layer is responsible for delivering application specific services to the user. It defines different types of applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health.

This 2-3 layer architecture of Internet of Things is not a sufficient for the today's technology. So a new architecture was designed for IoT devices. The new architecture having 5 layers and is known as 5 Layer architecture New architecture has perception, transport, processing, application and business layers.

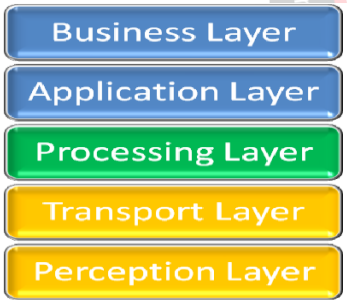


Fig. 3 - 5 Layer Architecture

**Figure 3: 3-5 layer architecture**

**1.Perception layer –**this layer works in a similar manner as previously described in the 3 layer architecture. The purpose of this layer is to take information from the sensors and implement it.

**2. Transport layer -**takes the data from the perception layer and pass this data to processing layer and vice versa. This will done with the help of various networks like LAN, wireless technology, 3G, 4G,LTE, RFID etc.

**3. Processing layer-**Itis the third layer and also perform the major task because it will process all the information gathered by the perception layer. There is a large amount of data and it will be stored with the help of some techniques like cloud computing or any DBMS. Then it will analyze how to fetch data whenever required in order to complete the intended task.

**4. Application layer – It** is the next layer which implements the working of IoT. For this an application is required with the corresponding device in order to complete the intended task.

**5. Business layer –It** is the last layer of this architecture ,manages the working of entire system along with many other features, one of them is privacy.

Both the architectures are defining the working different types of IoT system of but they all are following the same sort of working in order to achieve its goal.

## IV. TECHNOLOGIES

There are various technologies used to define IOT, but the four main technologies[2] are as follows

**1. Radio Frequency Identification (RFID)**

**2. Near Field Communication (NFC)**

**3. Machine to Machine Communication (M toM)**

**4. Vehicle to Vehicle Communication (V toV)**

**Radio Frequency Identification (RFID):**

RFID[6] is a system in which there is a reader to read many tags and It uses the technology of radio waves to send the information of an object in the form of serial number which is attached to the tag. RFID uses the electromagnetic fields to transfer the data on the tags so that it can automatically identify and track the objects, corresponding to a particular tag. the initial phase of research RFID defines in three configurations:

- **Active RFID**
- **Passive RFID**
- **Active Reader Active Tag**

**Active RFID** - (Passive Reader Active Tag), the reader receives the signal or data from the device which runs on battery and this battery is operated by a device called active tag. This data exchange will take place in limited range of area in the active tags and the passive readers which is from 1-2000 feet depending upon the architecture.

**Passive RFID** - The second one is Passive RFID (Active Reader Passive Tag), most commonly used, such tag does not require any battery or onboard power supplies, so it requires energy to send the data and thus collecting the energy from the RFID reader.

**Active Reader Active Tag -** The last one is the combination of the reader and tags are active so it is an Active Reader Active Tag.Although both the reader and the tags are active, but tag will starts sending information only when it is awoken by the reader or when it comes in the closeness of the reader. So the major components of this technology are

 DOI : 10.35291/2454-9150.2020.0717 

tag, reader, power supply, antenna, access controller, software and server.

**Applications:**

The main functions of RFID system generally include three aspects: monitoring, tracking, and supervising. Monitoring means to be aware of the state of a system, by repeated observing the specific conditions, especially to detect them and give warning of change. Tracking means to observing of persons or objects on the move and supplying a timely ordered sequence of respective location data to a model. Supervising is the monitoring of the behaviors, activities, or other changing information, about the people.

**Issues** - There are several issues with RFID. It works on specific range of frequencies; if these frequencies differ at different places then it will create a problem in reading a tag at different locations. It is difficult to read more than one tag simultaneously.

### 4.2 Near Field Communication (NFC)

Near Field Communication[3] is somehow little bit similar to RFID, it combines a RFID reader in a mobile phone, which makes it better, reliable and efficient for the users. Near Field Communication is a short-range wireless technology with the frequency of 13.56 MHz, typically work for very small distance up to 4 cm. Allows intuitive initialization of wireless networks and NFC is complementary to Bluetooth and 802.11 with their long distance capabilities at a distance up to 10 cm.

**There are two modes in NFC technology:**

- **Active**
- **Passive**

**Active Mode** - In active mode both the devices are active and communicate with each other by sending the signals.

**Passive Mode** - In passive mode one of the device sends the signal rather other just receiving it

NFC doesn't need pairing, it cannot work from a long distance and in this way this technology is secure and use for mobile payments.

**Applications** - NFC works in a very short range so the devices must be kept nearby. It has several applications, the most important one is Payment App. Today, we have several applications (apps) by which one can pay without using a card, in this scenario the device works as a virtual card and the transaction will take place.

### 4.3 Machine to Machine Communication (M2M)

Machine-to-Machine (M2M)[4] refers to the communications between computers, embedded processors, smart sensors, actuators and mobile devices (DYE, 2008). The usage of M2M communication is increasing in the scenario at a fast pace. For instance, researchers predicted that, by 2014, there will be 1.5 billion wirelessly connected devices excluding mobile phones.

**Application** : In the industrial work, a machine can sense the work efficiency of the machine and work accordingly for maximum output. Smart homes where objects can communicate with each other like when there is no one in the home and unfortunately the owner forgot to lock the home then smart home will sense that there is no motion in the home and it will lock the home and send the unlock key to the owner. The same application is smart water supply, if there is a leakage then the machine sensor will sense this and send the information to the server. It will help to stop the wastage of water.

**Issues** - The key issues in M2M are - In M2M technology, devices or groups can use different naming process. Devices can use different names for their working or same name can be assigned different devices, objects or groups. They can use some temporary id, names and URIs for their communication.

### 4.4 Vehicle to Vehicle Communication (V2V)

In thisV2V[7] technology the objects are vehicles, which can communicate with another vehicle or the sensors around them. The main aspect of concern here is, there is no proper method to define the protocols because the object is moving and communicating with another moving object or with the sensors on the roadside. So we are not able to define any routing protocol. This communication can work for a long distance and make an efficient communication among objects. This technology was designed primarily with the aims of traffic control, safety and accident avoidance.

**Application** - Smart cars are the application of M2M, a car which is driverless or a car which have sensors and sense the speed of the nearby car who is getting slow uncertainly. So the car can be slow down to avoid accident.

**Issues** – The key issue in V2V are - The main concern of V2V is the loss of connectivity when any other object comes in between the communicating devices.

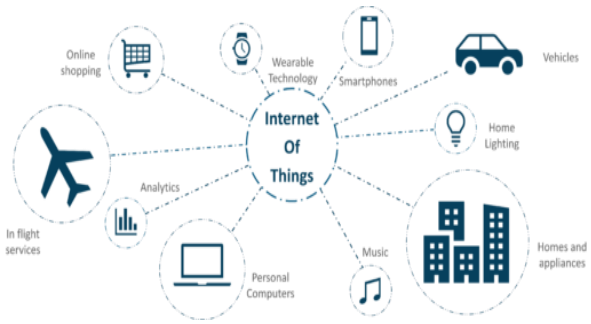


**Figure 4.Applications of IOT**

 DOI : 10.35291/2454-9150.2020.0717 

## V. SUGGESTIONS AND CHALLENGES:

The IoT can give a new dimension to the Internet and can contribute to extensive financial gains but it also faces some challenges[11,12].Some of them are listed below.

**1) Unique Identity Management**: The IoT aims at connecting millions and billions of physical objects which should be uniquely identifiable over the Internet. Thus, proper identity management scheme is needed which will dynamically assign and manage unique names for a wide range of physical devices.

**2) Standardization and Interoperability**: Many vendors introduce their devices having different technologies not known to everyone. There should be a standardized mechanism to ensure interoperability of all the physical and sensor devices.

**3) Privacy of the Information:** The IoT makes the use of various object identification technologies like RFID, 2Dbarcodes etc. As each object will be carrying these tags, it is extremely important to ensure privacy of the information thus, preventing unauthorized access.

**4) Safety of physical devices:** The objects irrespective of their geographic location need to be prevented from physical damage, unauthorized access in order to ensure its safety.

**5) Confidentiality of information:** The sensor devices transmit the information to the information processing system over the transmission media. The sensors should follow the encryption mechanisms to ensure data integrity at the information processing system.

**6) Network security**: The sensor devices send data either over wired or wireless transmission media. The transmission unit should tackle with this huge data without any loss of information and should incorporate strict measures so that no external intervention occurs.

## VI. CONCLUSION

Internet of Things (IOT)[8]depends on Internet, sensors technology which makes the communication possible among devices by implementing different protocols. After doing literature survey some major issues are observed, like the interrupted connectivity among devices effecting the communication. Also there is compatibility issue in devices. Security of devices during communication process and security of communication channel or link is also a major issue. Lots of work is to be done for the betterment and progress of this field; still there is more work to do, more standardization of technology, protocols and hardware are required to make completely reliable and secure domain of Internet of Thing.

## REFERENCES

[1] 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, pp.2347-2376.

[2].SomayyaMadakam, R. Ramaswamy, SiddharthTripathi, "Internet of Things (IoT): A Literature Review," Journal of Computer and Communications, 2015, 3, 164-173.

[3]. Gerald, Josef,Christian and Josef Scharinger, "NFC Devices: Security and Privacy", ARES 08 proceedings of the 2008 Third International Conference on Availability, Reliability and Security, IEEE Computing Society, Washington, DC, USA, 2008 .

[4]. A Survey paper on Cloud Computing and its effective utilization with Virtualization Anup H. GadeShri Ram Institute of Technology, Jabalpur. International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013 357 ISSN 2229-5518.

[5]. A Literature Survey on Internet of Things (IoT) Krishan Kumar Goyal, Int. J. Advanced Networking and Applications Volume: 09 Issue: 06 Pages: 3663-3668 (2018) ISSN: 0975-0290.

[6].Ms.NehaKamdar, Vinita Sharma, SudhanshuNayak, "A Survey paper on RFID Technology, its Applications and Classification of Security/Privacy Attacks and Solutions," IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol.6, No4, July-August 2016.

[7].PallaviSethi and Smruti R. Sarangi, " Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering Volume 2017, Article ID 9324035, 25 pages

[8]. https://www.codeproject.com/Learn/IoT/

[9] . www.abouttheinternetofthings.com/iot-features/11-best-iot-information-sites/

[10].https://www.tutorialspoint.com/internet_of_things/internet_of_things_overview.htm

[11] G. Gang, L. Zeyong, and J. Jun. (2011) "Internet of Things Security Analysis," International Conference on Internet Technology and Applications (iTAP).

[12] Z. Hu. (2011) "The research of several key question of Internet of Things," International Conference on Intelligence Science and Information Engineering (ISIE).

 DOI : 10.35291/2454-9150.2020.0717 