International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 10 | Oct -2017 www.irjet.net p-ISSN: 2395-0072

A Brief Review on Internet of Things

Animesh Sarmah[1], Kaustabh Kailyan Baruah[2], Amlan Jyoti Baruah[3]

[1,2]Dept of CSE, Assam Kaziranga University
[3]Assistant Professor, Dept of CSE, Assam Kaziranga University

---

Abstract - *The paper presents a brief description of this wide familiar technology. We have entered a new age of technology that became well known in recent time, the name of the technology is IoT that refers to "Internet of Things". IoT is too known as the Internet of Intelligent Thing, Internet of Everything etc. The IoT basically consists of web-enabled devices that can read or collect, send and respond to the data they acquired from the environment by the use of highly functioning sensors, hardware that can communicate, network connection and processors. The main aim of IoT is to transform the real world objects into an intelligent virtual object in order to make human's lives much safer and easier. Since we have seen the communication form is either human-human or human-device, but machine-machine communication is not seen before the invention of IoT. This form (M2M) of communication is possible because of IoT. The first phase of the IoT can be seen in the revolution of Internet, smartphones etc. The Internet or the net in simple term can be described as "the worldwide system of an interconnected network that uses the IP Suit- TCP/IP (Transmission Control Protocol/Internet Protocol)". Our objective of writing this paper is to give a generalized idea about the well-known technology Internet of Things.*

Key Words: Technology, IoT, IP, Suit, TCP/IP, data, M2M, Sensors, network, processors, web-enabled, devices.

1. INTRODUCTION

We have reached that stage of life where almost every individual is connected to the Internet. The advancement of Internet technology took a new shape where everything around the planet can be connecting among each other and that technology is named as IoT (Internet of Things). It is a huge concept which is evolving day by day and the opportunities in IoT is infinity. The number of internet service's users and the internet services in the devices are increasing day by day either they are connected via wires or wireless. Anyone can gain any information just at their fingertips. Before the invention of IoT, there were only two types of communication either human-human or human-devices, but the invention of IoT made it possible to establish communication among machines-machines (M2M). The concept of IoT dates back to 1982 where a coke machine was modified and able to connect to the internet. The machine generated a report of the drinks whether the drinks were cold or not. The primary idea behind the Internet of Technology is to exchange information between real-world objects around us, with the help of leading technologies like RFID (Radio Frequency IDentification) and WSN (Wireless Sensor Network) which are sensed by the highly functioning sensor devices and are further processed by a processor for making decisions and the actions are performed automatically without any individual's interference [1].

In simple terms, we can say that IoT is the new revolution of the Internet. It provides a stage where objects can communicate, organize and manage by themselves [2].

2. HISTORY

The name "Internet of Things" was first officially named in the year 1990. Though the idea of IoT was used at Carnegie Mellon University in early 1982 where a modified coke machine became the first machine to establish an internet connection. The machine reported whether the latest loaded drinks were cold or not. The idea of IoT was popularized in the year of 1999.

3. ELEMENTS OF INTERNET OF THINGS

Elements of the Internet of Things are as follows:

a) **Hardware:** These are the sensors, communication hardware etc.
b) **Middleware:** Data analytical tools and storage.
c) **Presentation:** Delivery of the information to the end users [3].

3.1 A brief description of the key elements of IoT:

a) **Sensing**: It is the method of capturing information by some highly functioning hardware. These are the types of hardware devices known as "sensors" capture or gather information from the environment and respond to it.

b) **Communication:** This element plays a very significant task in IoT. This element helps to communicate with the cloud services. The information that is sensed at the machine level is further transmitting to the cloud-based service for sequential processing.

c) **Cloud-based capture and consolidation:** The information that is gathered is transmitted to the cloud-based service so that the information gathered at the device level can be grouped with other cloud-based data, to provide useful information to the end user. After that, the data are being consolidated or combined from various internet sources or from other similar IoT devices and start processing.

d) **Delivery of information:** This is the last element of IoT where the data after being processed are delivered to the end-users. The data delivery may be a person or it may be to another device in M2M (Machine-Machine) workflow [4].

3.2 A few enabling technologies used in IoT:

a) **Radio Frequency Identification (RFID)**: This technology plays a very significant task in IoT as it uses an electromagnetic field to recognize and track the tags or the labels that are attached to the objects. The tags or the labels contained some electronic information stored in. It comprises with a 2-way radio receivers-transmitters to recognize and track those tags or labels attached to an object. The application of this technology is found in transportation, retail and supply chain management etc [5].

b) **Wireless Sensor Networks (WSN)**: WSN is the networks that are wireless in nature which consists of some inter-connected or not inter-connected autonomous device which is known as sensors that are used to sense or monitor physical and ecological conditions such as temperature, pressure etc [6].
The WSN comes or builds up with nodes where these nodes are connected to a single sensor or sometimes it is connected to more than a sensor. A few parts of such sensor network nodes are:
- A radio transceiver with an antenna placed inside the radio transceiver or sometimes antenna placed outside the radio transceiver.
- A micro-controller.
- A circuit (electronic) is used for merging with the sensors together with an energy supplier that may be a battery.

Few applications of WSN are:

- Monitoring Area.
- Healthcare monitoring.
- Industrial monitoring.
- Landslide detecting etc [7].

c) **Addressing schemes:** As we all know that when devices get connected to the internet, the devices are addressed with some unique digits which are called as IP addresses. It is a very important technique on the Internet of Technology too as this technique helps to identify a device uniquely. This technique is not just to identify devices but it also helps to control remote devices through the internet.

d) **Data storage and analytics:** Due to the huge numbers of data generated by the IoT, this concept plays an inevitable task in the IoT. This forms the middleware layer of IoT that focuses on the storage and analysis of those data. The data that are generated by the IoT is stored in a secure and systematic way using various algorithms such as Novel fusion algorithm is used to make sense of the data that are collected. There are numerous other techniques like a genetic algorithm, neural networks, temporal machine learning methods that are based on evolutionary algorithms etc.
Since the year 2012, the cloud-based storage along with the cloud-based analytics and the visualization platform became popular.

e) **Visualization:** This plays a very serious task for IoT application. These technologies allow the user to interact with the surroundings. This encompasses the event of visualization and detection of the information (modeled and raw data) and to represent the information to the end-user according to their needs [8].

4. IOT ARCHITECTURE

The IoT architecture comes in six layers. The layers of IoT are as follows:

a) **Coding Layer**: This layer is considered as the foundation layer of the IoT as this layer assigns a unique ID to the objects to specify their identities.

b) **Perception Layer**: The layer contains the data sensors that too in the different form of IR sensors, RFID etc that are used to sense the temperature, speed, humidity, and location etc of the objects. One of the important functions of this layer is that it linked and converts the information gathered by the sensors into digital signals which are further transferred to the Network layer.

c) **Network Layer**: The functions of this layer are to receive and transmit the digital data to the middleware layer that are received from the perception layer for processing. Those data are transmitted onto the middleware layer over some transmission medium such as Wi-Fi, 3G, and GSM etc along with protocols like IPv4, DDS etc.

d) Middleware Layer: The data that are received from the network layer is processed in this layer. This layer uses the technologies like cloud computing, ubiquitous computer etc.

e) Application Layer: Based on the processed data, the IoT's result is finally released to the end-user at this layer.

f) Business Layer: This layer acts as the manager for the application and services of the IoT [9].

5. SECURITY THREATS OF IOT

A brief discussion of the "Security Threats of IoT" is provided below:

5.1 Perceptual layer security threats

In this layer, the perceptual nodes that usually build a dynamic circulation network that gives limited nodes resources change in network topology and distributed organized structure. The lists below are the threats that come in this layer.

Table 1: Different threats in the perceptual layer

Threat's Name	Threat's Description
Physical capture	Usually, nodes are deployed statically in some area that could be easily captured by the hackers and thus information is physically compromised.
Brute force attack	Due to the limitation of the resource storage as well as the computation of the sensor nodes brute force attack is an easier tool.
Clone node	If the hardware structures of the perceptual nodes are simple, the hackers can easily clone it that can reduce the integrity of the network.
Routing attack	The middle nodes are used as the attack relay means in order to compromise the information as the routing takes place between sources and sink nodes.
Denial of Service (DoS) attack	DoS methodology is used to stop the services on the network as the nodes usually have a limited capacity of processing.

5.2 Network layer security threats

The routing protocol that is used in this layer of IoT is similar to the protocol used in the network layer of the standard internet, but this layer (network layer) of the IoT basically focuses to make a lossy and low-power network. This layer is also known as a next-generation network.

The lists below are the major threats that take place in this layer:

- The counterfeit attack, Man-In-Middle attack, Hello Flood attack etc.
- Some malicious behavior might be seen in certain nodes that spoil the QoS (Quality of Service) of a network and sometimes the packets are routed improperly.

5.3 Middleware layer security threats

Middleware layer is too known as a support layer in IoT. The core purpose of this layer is to provide a platform that is reliable for the application layer. In simple language, we can define this layer as the layer that performs the task of a link between the application and network layer.

The lists are below are the threats of this layer:

Table 2: Different threats in middleware layer in IoT

Threat's Name	Threat's Description
Unauthorized access	Accessing a network by altering its configuration unauthorizedly.
Session attack	Hackers illegally entered the network and hijack or sometimes destroy the session.
Denial of Service	This attack is done to

(DoS) attack	terminate the services of the network for a definite period of time.

5.4 Application layer security threats

The application layer is also known as the upper layer of the IoT as this layer is responsible to provide all the services as per user's requirement. The lists are below are the threats of this layer:

Table 3: Different threats in application layer

Threat's Name	Threat's Description
Malicious code	Malicious codes are deployed in order to spoil the IoT's normal work.
Social Engineering	This attack is done by seeking or stealing information via chats or by knowing each other.
Denial of Service (DoS) attack	This attack is alike to the attack of the other layer. Its aim is to stop or spoil the services of the network [10].

6. ADVANTAGES AND DISADVANTAGES OF IOT

The advantages and disadvantages of IoT are as follows:

Advantages	Disadvantages
• The biggest advantage of IoT is its communication, as it can communicate between the devices which are also known as M2M communication. IoT can start a connection without human interference.	• As IoT is growing rapidly, numbers of vendors are coming forward with their goods, due to this privacy is much concerned.
• IoT can gather information with the use of sensors and make its right decision [11].	• In some cases, the IoT's implementation makes an unskilled employee lose their job, as IoT is an advanced technology which is not familiar to everyone.
• IoT reduces the monitoring time.	• The internal architecture of IoT is different from each other, which means sometime IoT comes with a very complex system.
• IoT process and deliver information accurate and faster in the smallest amount of time and minimum utilization of energy.	• Due to architectural difference sometime in case of network failure, it needs time to restore the service to the customers [12].
• IoT systems are used in home security which can control by the smartphones.	

7. CONCLUSION

The use of IoT is spreading widely across the globe. In the study, we have learned that in the near future IoT is going to connect to different source and it will help human to get rid of workloads, in the simple term we can say that IoT is going to make an individual's life simpler than now. Along with the advantages of IoT, especially in the industrial field, there is a disadvantage that IoT may need huge space, time, money etc to implement.

8. ACKNOWLEDGEMENT

We express our sincere gratitude and thanks to Mr. Amlan Jyoti Baruah (Asst. Professor, Computer Science and Engineering) department of The Assam Kaziranga University for his valuable support and guidance during the preparation of this review paper.

9. REFERENCES

[1] http://research.ijcaonline.org/volume113/number1/pxc3901571.pdf

[2] http://www.engpaper.net/free-research-papers-iot-internet-of-thing.htm

[3] http://ijesta.com/upcomingissue/04.04.2015.pdf

[4] http://intelligentproduct.solutions/blog/internet-of-things-4-key-elements/

[5] https://en.wikipedia.org/wiki/Radio-frequency_identification

[6] http://www.ni.com/white-paper/7142/en/

[7] https://en.wikipedia.org/wiki/Wireless_sensor_network

[8] http://www.buyya.com/papers/Internet-of-Things-Vision-Future2013.pdf

[9] http://research.ijcaonline.org/volume113/number1/pxc3901571.pdf

[10] http://researchscript.com/wp-content/ uploads/2015/04/IJRCS020405.pdf

[11] https://e27.co/advantages-disadvantages-internet-things-20160615/

[12] http://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-IoT-Internet-Of-Things.html

BIOGRAPHIES

Animesh Sarmah has completed his B. Tech degree in Computer Science and Engineering from The Assam Kaziranga University, Jorhat, Assam in the year 2017.

Kaustabh Kailyan Baruah has completed the B. Tech degree in Computer Science and Engineering from The Assam Kaziranga University, Jorhat, Assam in the year 2017.