

# Internet of Things(IoT): A Brief Information and Challenges of Implementing.

V.Ashok Kumar, S.Aarif Ahamed

**ABSTRACT---** *Internet of Things is nothing but the devices that has been not connected to the internet world so far. Each and every devices ranging from home appliances to electronic items has been going to be under the cover of internet. Communication among the internet connected devices is the key matter of the area to be concerned. So far the application controlled devices so far software systems has been connected to the internet. The devices connected to the internet may not be related to each other but it is connected to the surrounding objects by means of Internet. By upon examining the current trends and advancement in field of IoT the paper presents possible future expansion by overcoming the challenges by applications.*

**Keywords:** *Internet of Things(IoT), Communication*

## I. INTRODUCTION

Internet of Things(IoT) is group of varied devices both in size and manner in which works or it is connection among mechanical devices, human being or animals that is provided with a unique identifier having the ability to transfer the data among them or to the rest of world. The IoT architecture doesn't require a human to human communication or a human to computer interaction. As more and more electronic devices or mechanical objects enters into our home the real objects are represented in a digital form. A network has been created for exchange of information among the connected objects with the assistance of software, sensor and electronic devices. Network of physical devices connected to the internet will create an environment that enables to improve and assist the quality of human beings living by means of security and better management of objects that will enhance the usage in day to day living. When a communication is going to be among with the static devices and the information available with them that builds a connection from people to people, people to the physical devices and physical objects to other physical objects. Each and every devices connected to the internet now has been changed, starting from the 90's era the communication between the user and rest of the world was made by a large desktop machine that resides in our table to the portable PC's or laptop's that makes the expansion of PC's available to the common people both in terms of cost and also the efficiency of the working of Laptop machine

that matches the performance needs of desktop. Later mobiles has been the one thing that gains popularity when the networking infrastructure expands by making the more number of mobiles connecting to the internet. And now with the advent of rapid expansion of Smartphone entering into the market and into the lives of common people 90 percent of traffic connecting to the internet is from the smartphones and tablets. As per reports from IDC report there will be more than 30 Billion devices connected to the internet connected and sensor enable devices by 2020. The rapid growth of smartphone and smart devices makes the convergence of internet data and processing making valuable.

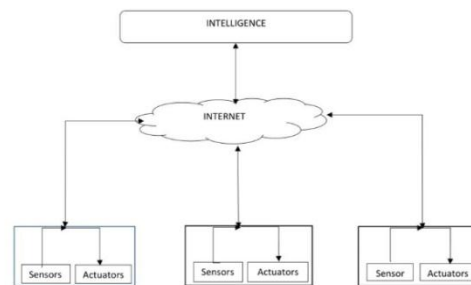


Fig-1: IoT Architecture

## II. CHARACTERISTICS OF IOT

### 1. Consumption:

As IOT is about the connection of devices that of more capable in producing the real time data that each and every devices connected with it. The data that is produced from each and every devices must be capable of producing a data that is operational so the produced data is consumable to the structure of network.

### 2. Connection:

Based on the connectivity to the IoT production of intelligence around the data can be build. As more and more devices connected to the IoT network, connections are made in a manner for efficient handling of data.

### 3. Conversion.

As machines produce raw data converting them into a manner by which human being can interpret the sensor data is critical task. Each binary values produces is expanded to know the information it contains and the context of data can be identified.

**Revised Manuscript Received on February 14, 2019.**

**V.Ashok Kumar** Assistant Professor, Department of Computer Science and Engineering, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science & Technology, Avadi, Chennai 62, Tamilnadu, India. (E-mail: ashokvijay872@gmail.com)

**S.Aarif Ahamed** Assistant Professor, Department of Computer Science and Engineering, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science & Technology, Avadi, Chennai 62, Tamilnadu, India. (E-mail: aarifahamed10@gmail.com)

4. Centralization:

As more and more physical devices coming into the existing IoT network, the need for centralized data is important to manipulate different, disconnected to perform data analytics.

5. Results & discussions

Once the centralization of data is done, the information about the data is done by a analytical process by applying the context to the data.

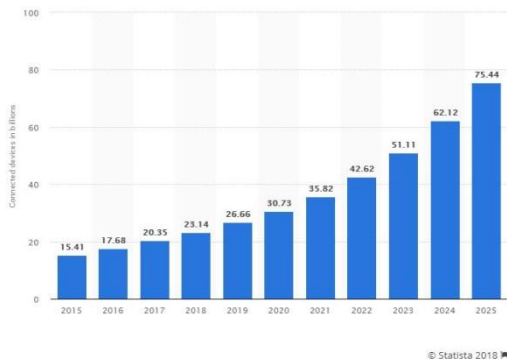


Fig-2:IoT Connected Devices

6. Configuration:

Each and every devices may send some anonymous data or a data that may improve the performance, speed or a bug that stops operating the manner in which it is designed. That data should be fed back into IoT network so the machines can work better and smarter in the way.

7.Co-Ordination:

Scheduling the devices that connected to the IoT network is important about the priority in the manner about the operation of devices so that it can't disrupt or reduce the performance of IoT network.

8. Smart sensing capabilities:

The devices that are connected with IoT will have the smart sensing capabilities to maximize the energy efficiency by turning on or off when the resource is needed. For example to turn the light on or off based on the ambience of temperature inside the living room.

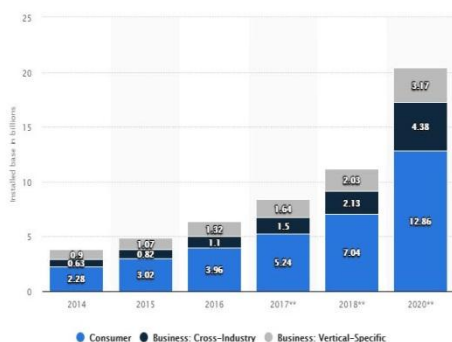


Fig-3: IoT Units Installed

9. Intelligence:

As IoT collects data in regular intervals the processed data can be made efficient with self learning capabilities.

For example a fitness tracker can collect the data about the speed of walk,time,energy bursted during walk,blood pressure and then compare with the previous data by segregating the results and organizing the collection of data in a spreadsheets as graphs by sending the user statistics to intended user or saving the results in cloud storage.

10. Save Energy:

In order to utilize the energy in an efficient manner the IoT have a built in sensors that can switch on the tap while the user enters near the basin and switch off while leaving outside the basin. This reduces lot of power and reduces in wastage of energy by maximizing the energy efficiency.

III. CHALLENGES IN IMPLEMENTING IOT

One of the foremost concern is the security challenges to overcome the implementation of Internet of Things(IoT) devices. IoT data can belong to a group or individual, or a government organization that caters the needs of common people requests or issues stored in a large volume of data. For example an IoT application may stores current and historical data about persons shopping behavior like the products mostly purchased, stores that mostly visited, amount of money spend in each and every item. Another example while considering about the applications focusing on location is that it may geo focus the areas that is mostly accessed, this may lead to serious concern especially in defence sector. There are areas concerning the efficiency of services provided by IoT like scalability, response time takes, price of the product and the ownership details. There is not a common standards for implementing an IoT.

As more and more devices come into the IoT infrastructure amount of data produced is also more. Security is the major concern when data is transmitted across the channels especially government organization like defence,manufacturing and health sector.

Consider an IoT application of large warehouse that contains the big sized door that can be opened and closed with the smartphone. In case if the system has attacked by burglar the person can easily enter into the warehouse by smartphone and steal the things without the knowledge of owner.

1.Secure constrained devices:

As IoT devices have limited number of storage and has minimum number of operational capability based on the battery constraints. Considering with the encryption details IoT devices cannot able to derivate a methodology for a complex type of encryption or decryption as of available now for transmission of data in real time.

2. Authorize and authentication of device:

As more and more number of devices connected to the IoT network, devices must establish their identity before entering into the gateway and this is the area where most number of devices are lagging in marking their presence in IoT world.



### 3. Updation of devices management:

For any application that is been integrated into the internet world it must be frequently updated to match the growing needs and feedbacks from the users. Considering for an example with smart home system connected with IoT network some of the devices may be age older that may not eligible to receive an update, in that case the devices may be opt out from the current system of home as the devices are not supported for updation from the manufacturer.

### 4. Secure communication:

As communication is the most important among the devices that is connected in the IoT network. A nature of trust is the concern when concerning about the originality of message that is has been sent and received.

### 5. Ensuring data privacy and integrity of data:

There may be more number of crunch data produced, and it is important to dispose the data that is no longer important by ensuring the privacy of data. Intended data generated from a particular device connected in the IoT network must be received for the intended receiver without the data being modified.

### 6. Secure mobile and web applications:

Mobile and web applications that are designed as part of IoT infrastructure must be safe and secure for all type of operations. The generated data must be properly segregated into the cloud storage that is capable enough to conceal the data from any type of attacks.

### 7. Ensuring high availability:

Considering a smart city that IoT infrastructure may depend on live details of traffic, bus management system, metro management system, Water supply details, electricity distribution. In that case at any point of time when a particular system or at a particular point if it fails then it may cost so much as the entire network may void of functioning.

### 8. Detecting vulnerabilities and incidents:

As for as the IoT infrastructure is concerned any thing that disrupts the normal operation of network must be taken into note and immediately consider for an action, because varied number of devices and applications that are connected with variety of protocols for communication makes difficult to find the exact location or a time at which the attack has been made on the network.

### 9. Predicting and preventing from security issues:

Security intelligence or security protocols not only for detection but also it is used to prevent from the potential security threats. Based on the analytics tools and monitoring the relevant events and visualizing the threats in real time to mitigate the attack.

## IV. CONCLUSION

The users participation and storage processing cannot be separated by the IoT application as the personal information and behavior of the users may differ from person to person and all the privacy disclosure may be weaken while more number of devices connected to the IoT network and this

may threaten the national security and it causes social unrest. Reducing the constraints and ensuring the high availability can be enhanced by developing some applications that is more and more secure efficient for data transmission without explicitly sharing the device information to the outer world. In future based on the security measures provided by IoT standards, we should take some complex measures to achieve the security goals to make IoT system a secure efficient to achieve the future needs.

## REFERENCES

1. Mahdi H. Miraz ; Maaruf Ali ; Peter S. Excell ; Rich Picking "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)" Internet Technologies and Applications (ITA), 2015, pp 219 – 224.
2. J. Sathishkumar ; Dhiren R. Patel "Enhanced location privacy algorithm for wireless sensor network in Internet of Things" ,2016 International Conference on Internet of Things and Applications (IOTA), pp 208 – 212.
3. Sushma Satpute ; Bharat Sing Deora "Improving performance of Internet of Things by using local IOT controller unit", 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), pp 1328 – 1330.
4. Sachidanand Singh, Nirmala Singh "Internet of Things (IoT) Security challenges, business opportunities & reference architecture for E-commerce", 2015 International Conference on Green Computing and Internet of Things (ICGCIoT).
5. Sébastien Ziegler, Sotiris Nikoletsea, Srdjan Krco, José Rolim, Joao Fernandes "Internet of Things and crowd sourcing - a paradigm change for the research on the Internet of Things" 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT).
6. Bengt Ahlgren, Markus Hidell, Edith C.-H. Ngai, "Internet of Things for Smart Cities: Interoperability and Open Data" IEEE Internet Computing, pp 52 – 56.
7. Yunchuan Sun, Ye Xia, Houbing Song, Rongfang Bie, "Internet of Things Services for Small Towns" 2014 International Conference on Identification, Information and Knowledge in the Internet of Things.
8. Xiaofeng Lu, Qi Li, Zhaowei Qu, Pan Hui, "Privacy Information Security Classification Study in Internet of Things", 2014 International Conference on Identification, Information and Knowledge in the Internet of Things.
9. Diane Keng, Simon G. M. Koo, "Spatial standards for Internet of Things", 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC).
10. Antonio J. Jara, "Wearable Internet: Powering Personal Devices with the Internet of Things Capabilities", 2014 International Conference on Identification, Information and Knowledge in the Internet of Things.