Internet of Things (IOT) Basics - An Introduction to the New Digital World

[1]Mohammed Rahmat Ali
[1] Researcher Scholar,
Kulliyah Information Communication Technology- Computer Science,
International Islamic University Malaysia (IIUM),
Gombak Malaysia.

Author Address:
Mr Mohammed Rahmat Ali
Researcher Scholar,
Kulliyah Information Communication Technology
Computer Science,
International Islamic University Malaysia (IIUM).
Gombak, MALAYSIA.
9-8-256, Bada Bazar, Golconda Fort, Hyderabad-500008, Telangana State. Mobile: 91-9985220384
Email: rahmat_ali2u@yahoo.com

Abstract: Internet of Things abbreviated as IoT, is gaining the market due to its advantages of being intelligent and easy to use and cost effectiveness but also lack in term of security. IoT is accepted as the intelligent device which can receive, monitor and generate the outcome of the given input. And also is responsible to analyse and take decision based on the generated input, industries are accepting the role of IoT to reduce their efforts and to increase the productivity and profitability in different sector of society. But the Major concern with the IoT devices is the security. As the IoT devices are connected to the network, data security and integrity is always been questioned.

*****

I. INTRODUCTION

Internet of things is an intelligent device which can receive, store and process the data according to the requirements. Internet of things is a connection of devices in a network, a typical IoT device has sensors actuators and microchips embedded into it, which sends and receives information to and from the network. Also can be said as Internet of Things (IoT) is a physical device on to which some software and been embedded and the device is connected to the network and posses some an IP address. Internet of Things has made the life easy and intelligent, with the help of IoT we can assume a smart house, smart car, smart traffic signal, smart industry and smart cities too.

Internet of Things (IoT) are also used in the medicine to monitor the health of the patient and to advice good medicine to the patient according to the condition being away from the patient. It is also used in auto tracking system where on vehicle can be traced used IoT device. IoT has also become a part of smart homes, where anything and everything can be controlled by tip of your finger. Industries are also accepting the role of IoT which intern reduces their efforts and increase the productivity and profitability and can produce goods according to the requirement of the customers which saves time and material of the industry.

According to a survey analysed be IoT Asia, the acceptance of IoT technology in Asia ranges from 157.8%, as Singapore to 1.2%, as Thailand, where as India, stands last second in the list with the adoption of the IoT with readiness of 8.1% and Malaysia with 34.8%, respectively. The increase in the production and usage of smart devices and decrease in the data charges is the peek sign that soon or later we are going to be digital or we will be digitalized as an individual, i.e. the place in which we live or the city in which we live will soon be digital city.

KEY FEATURES OF INTERNET OF THINGS (IOT)

There are many of the key features of Internet of Things (IoT), some of them mentioned here are as follows,

SENSORS

Sensors are now used in different applications, such as mobile phone, smart devices, automotive systems, industry controls, health care, oil exploration and climate monitoring etc.,. Sensors are now used almost everywhere, and now sensor technology has begins to simulate the latest human tracking machine. The Internet of Things (IoT) technology which allows you to sense, is a combination of sensors, which utilize microcontrollers(intelligent device) to integrate individual data collected from different sensors to obtain a more accurate and reliable display of data than can be obtained using any separate sensor. A sensor leads to a

situation where the range of intelligent devices is much greater than the human form.

CONNECTING TO REAL WORLD FOR REAL TIME PROCESSING

Every individual smart device connected to internet through a proper IP address is an IoT device in either of the means. This device receives information, manipulate operations based on the input, send the messages based on the input received. Consider an example of a security camera, which is used to monitor the things and keep an eye on things without the presence and interface of the human. The cameras are designed in such a methods that it detects the faces of the people and help analysing the things easily and effectively.

ENERGY EFFICIENCY

Every IoT device uses less amount of energy or uses others sources of energy. Consider an example of Automatic sensor Air Conditioner, it gathers the information and process the information accordingly, when the temperature is set to a point the air conditioner will be switched off automatically if the surrounding temperature is equal to the temperature set. This helps us in saving energy and time.

INTERCONNECTIVITY:

With regard to the initiative, everything can be linked to the global information and communication infrastructure.

THINGS-RELATED SERVICES:

If you are able to provide services related to things such as privacy protection and semantic consistency between physical objects and virtual objects. To provide services related to things within the limits of something, both techniques in the physical world and the information world will change.

HETEROGENEITY:

Devices in heterogeneous operations techniques based on platforms and different networks of devices. They can interact with other devices or service platforms across different networks. Dynamic changes: The status of the device dynamically changes, for example, suspension and / or wake up and / or stop, and device context, including location and speed. Additionally, the number of devices can change dynamically.

ENORMOUS SCALE:

The number of devices that need to be managed and connected with each other will be at least one order of a larger size than the current connected device. More importantly, data management is generated and interpreted for application purposes. This is related to data connotations, as well as efficient data handling.

SAFETY:

When we take advantage of IoT, we cannot forget safety. As the creator and receiver of IoT, we must plan for safety. This includes the security of our personal data and the security of our physical well-being. Maintain endpoints and networks and transfer data across all media to create a security model that will scale.

CONNECTIVITY:

The connection provides network access and compatibility. Access comes to the network, while compatibility provides the same capabilities for data recovery and generation.
Architecture of Topology

ARCHITECTURE OF INTERNET OF THINGS

Internet of Things architecture identifies the basic necessity of each component in the application and further each component is again been broken into smaller components so that one component can communicate with another component and form a stack of components. Architecture of IoT is been proposed in different form among those the two important architecture are 1. Layers of Architecture and 2. Fog or Cloud based architecture.

LAYERS OF ARCHITETECTURE

Layers of architecture have different layers suggested from 3 layers to 6 layers. We will discuss the 4 layers architecture. The four layers architecture is classifies as

SENSOR CONNECTIVITY AND NETWORK LAYER

In this layer the sensor will sense the data and will receive the information for the different source of information through sensors. The information will gathered by the different modes of sensors used. Consider an example of health monitoring system, the patient data will be sensed the sensors used in medical equipment and the result analysis will be soon on the screen a total health report will be maintained by the device been used. IoT sensors are also use in monitoring hypertension and diabetes.

GATEWAY AND NETWORK LAYER

The information being collected by the sensor need to passed to the device which receives the information through a network gateway or the network device, Wi-Fi or Wide Area Network (WAN) is been used at this level.

MANAGEMENT SERVICE LAYER

The data been sent on the network is managed by the management service layer, the data is been sent to the device and a proper action or the sequence of observation is been

made to analyse the data from the device and accuracy of the data is also been monitored.

APPLICATION LAYER

The data being received and monitored is applied in the real life in the sector of health and retail. Industries are accepting the role of IoT to reduce their efforts and to increase the productivity and profitability and can produce well according to the requirement of the customers which saves time and material of the industry.

In case of accident and emergency the IoT device can act as life saving device as the information can be sent to the nearest hospital with the condition of the patient and treatment required the doctors and medicine can be ready at the hospital before the patients arrives to the hospital.

FOG OR CLOUD BASED ARCHITECTURE

The fog or the cloud based architecture is based on the following layers.

Physical Layer
Monitoring layer
Pre-processor layer
Storage layer
Security layer
Transport layer

INTERNET OF THINGS CLASSIFICATION

CUSTOMER TO BUSINESS OR PEOPLE TO THINGS

IoT's devices that are either wearable or are through application purpose. The devices such as the health monitoring machines, camera with face deduction, or the cars with sensors are the example of people of things.

MACHINE TO MACHINE OR THINGS TO THINGS

The things with the interconnections of the object which communicate with one another and make an anayslsis and give a report are the things to things devices. For example analysis of a medical device to monitor health issue and reports related to it, on a particular patient.

IOT HARDWARE REQUIREMENTS

TYPES OF SENSORS

All IoT applications need one or more sensors to gather data from the environment. Sensors are an important element of smart objects. One of the most important aspects of the Internet article is contextual awareness, which is not possible without sensor technology. Sensors are often small, low cost and low power. They are limited by factors such as battery capacity and ease of use.

Some of the Sensors are

1. Mobile sensor
2. Medical sensor
3. Neural Sensor
4. Environmental and chemical sensor
5. Radio frequency Identification.

COMMUNICATION INTERFERENCE

Basically, Internet of Things stuff is an extension of worldwide internet connections from our computer to the devices and sensors that surround us. For the most part, wireless communication, especially in wide area networks that is, a set of mobile devices and other carry through and implant devices comes along with people.

Most of the devices have adopted the Radio Frequency Interference Devices (RFID) technology such as Bluetooth, ZigBee and Wi-Fi connection. Also known as remote field transmission, radio frequencies are large when connected to a distance, but become a problem when applied to remote isolated ecosystems, such as private radio area networks.

AMOUNT OF DATA TO BE CAPTURED AND TRANSMITTED

The devices connected to the internet generates a lot of data, that data should be preserved analyses and then reported or sent to the other devices and bases on the data received and analyzed the further instruction can be taken.

FREQUENCY OF THE DATA TRANSPORTATION

The amount of data that is been generated by the IoT devices cannot be updated to the internet but the data which is important and has more weight age will be uploaded to the internet. Consider an example of an aeroplane flying at high altitude cannot to the server and data cannot be transferred. It's been stored at the local memory devices.

STORAGE IN IOT

The data generated by the devices connected to internet is enormous according a prediction by the end of year 2020 every car will generate two peta byte of data every year, and an aeroplane will generate forty terabyte of data daily. And data that is been generated cannot be transferred instantly on the network, its uses simple memory devices and store the data. Later the data is been uploaded to either the cloud of data ware houses.

TOPOLOGIES OF IOT

POINT TO POINT

The point-to-point network establishes a direct connection between the nodes of the network. Communication between these nodes or devices can only occur. Examples of these types of networks are Bluetooth connections between mobile phones and headphones. The advantages of point-to-point communication are simplicity and low cost. The main constraints arise from the one-to-one relationship between the two devices. This network should not exceed two of these nodes. Therefore, the network range is limited to one

hop and is defined by a single device transmission network. One side is usually the Internet port or another traditional network that allows users to use the device.

STAR TOPOLOGY

The network star is the core (also known as the node), which is connected to all other nodes (for example, node sensors) networks. This middle axis acts as a shared connection point for all other nodes in the network. All terminal nodes can communicate with anyone else by sending only the core and getting them from it. Examples of these topology centres are the Wi-Fi network in your home. The cube is usually a link to the outside world.

There are many important advantages of star topology. First, network performance is consistent, predictable, and fast (low latency and high output). In the network of stars, unlike the described nested network below, data packets usually only move jumping to reach the destination (if travelling between the centre and sensors), or up to two hops (if travelling between the two sensors) Predictable, low,

Second, there is the reliability of the entire network because of the ease of any crime and the device can be isolated. Each device uses a unique link to the hub. This makes the separation of individual devices, makes it easier to detect errors and remove network components that do not work.

The disadvantages of this type of network are similar to point-to-point networks. This range is limited to a single device transfer network. In addition, there is no ability to drive rack resistance if there is interference or network interruption. Finally, in the star network there is a point of failure, the entrance. In the network, if the connection loses, the network is disconnected from the world, but still can exchange and store the data internally. This is important for some applications, such as reading counters or cooling chain management.

MESH TOPOLOGY

A mesh network consists of three types of nodes:

1. Hold the gate as in a series of stars, as long as the data can reach the outside world
2. Sensor knots are easy
3. Node / router, a sensor node with redundant / routing capabilities

The sensor / router nodes not only capture and publish their data, but also act as relays to hold another. This means that they must work with neighbouring nodes to spread data across the network.

A network node is moved so that each node within the transmission range is at least one other sensor / router node. Pack data through various sensors / hold the router to achieve the gateway node.

Network topology is used for many applications that require extensive coverage and long-term coverage. Applications include building automation, power management, industry automation and asset management, to name a few. Because network networks are not limited to single-device transmission networks, network networks can be very wide, covering large areas such as buildings or universities. The network can span to thousands of nodes, providing high density coverage with multiple sensors and wide drive devices. Flexible network designs allow coverage in the environment to meet high RF challenges such as high frequency radio frequency interference or RF resistance. Network interruptions are reduced intermittently through automatic retrieval and retransmission capabilities that provide high levels of network security.

The main drawback is that network networks, by their nature, are more complex than network topology from point to point or star. Visual inspection is usually performed, followed by network installation and commissioning. In addition, there is greater network latency in the network as multiple networks of sensors jump to the portal.

These three network topologies form the basis for a more in-depth assessment of the characteristics associated with each of the established and emerging network standards.

SECURITY CONCERN

As IoT is connected to a network the possibility of attack on the network is also predictable. The attacks can be so serious that, the company might run out of or go bankrupt. Recent times the attack on Ukraine power unit or the attack on cyber security of German steel mill or the attack on the people's security camera to spy on them are the examples.

The security concern can be addressed by the use of smart cards or by using intelligent devices or security chips. Security chip will be embedded with all the information of one that can be used. But the concern is making the chip and testing it and making that chip to only be accessible to the person and thing to be used. Proper measures are been taken into consideration to avoid the security concerns to the IoT, Still a lot of work is still ongoing.

II. CONCLUSION

Internet of Things (IoT) is slowly but eventually will take over the world and help the living standards of the world to live a quality life. Many research work and practical experiments are been carried out to make it simple and easy to use and affordable and with less energy consumption. Security is still a concern for the devices and equipments being used, and security will always be a concern. Measures and precautionary steps are been taken to reduces the threat of security. IoT will help the increase the life measures of a human in many ways either by support or by the qualities IoT provides from smart home technology to medical

monitoring devices. As a whole it's a technology to which human can rely on.

REFERENCES

[1] http://ieeexplore.ieee.org/document/6468307/
[2] http://my.mouser.com/applications/sensor-fusion-iot/
[3] https://en.wikipedia.org/wiki/Internet_of_things
[4] http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
[5] TOPOLOGIES DRIVING IOT NETWORKING STANDARDS
[6] Internet of Things: Architectures, Protocols, and Applications by Pallavi Sethi and Smruti R. Sarangis
[7] The internet of Everything Protocol and Possible Attacks
[8] Digital Evidences challenges and things by R.C.Hegarty1, D.J.Lamb2 and A.Attwood3
[9] Energy Efficient Network Architecture for loT Application by Sarwesh pi, N.Shekar V. Sheet
[10] Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges
[11] IOT forensics Issue, Strategy and challenges by Jingang Lui
[12] The three software stack requirement for IOT architecture by eclipse.org
[13] Comparative analysis of IoT Architecture by Ravi Teja.