A Comprehensive Literature Review on Internet of Things

Mr.Ramesh R[1], Assistant Professor, Mr.Shobika K.R[2], Mr.Balasundari S[3]
[1, 2, 3] Dept of BCA
[1, 2, 3] Sri Krishna Arts and Science College, Coimbatore

Abstract- The internet of things is the concept of connecting devices to the internet and the other connected devices. It is network of connected things and people which contains and share data related to the usage and environment. It is an extending internet connectivity beyond electronic devices such as desktops ,tablets , smart phones ,laptops and even to any range devices which does not have any internet connectivity (everyday objects). It is a technology which enables the devices communication and interaction which can remotely monitered and controlled.It gives us large benefits that weren't possible before.Iot is short form of internet of things. It refers to nonstop growing network of objects that feature an ip address for internet connectivity and the communication that occurs between these objects and the internet enable devices and systems.

Iot devices are any of the many things in the internet of bthings are non standard computing devices that connect wirelessly to a network and have the ability to transmit data.

I. INTRODUCTION

Internet of things is a network of interrelated computing devices , digital and mechanical machines , objects or people that have the feature of unique identifier and transfers data over a network. Sensors and actuators embedded in physical objects are linked through wired and wireless network. It is a pretty simple concept where it takes all the things in the world and connecting it to the internet. It is the most popular term to describe this phenomenon.

Internet of things is currently hot technology across the world wide Governments, acadamey and industry are involved in various aspects of research ,implementation and business with iot. It removes different applications domain verticals from civilian to defence sectors and these domains include agriculture, space , manufacturing , healthcare ,construction and mining .

II. HISTORY

The term internet of things was initially coined in 1999 by Kevin Ashton during his work at procter and gamble , Ashton wanted to attract his senior management attention to a new exicting technology called RFID ,the term was not so popular until 2011 and it reached the mass market in early 2014.
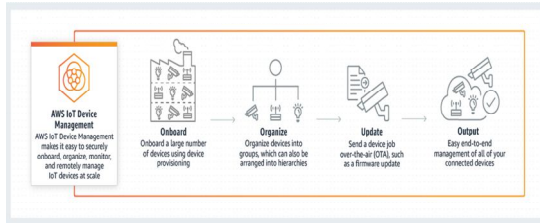
1. DEVICE MANAGEMENT:

There are many challenges faced which deploy the success of the iot system. These challenges could be solved by managing the iot devices by standard protocols or services.

Device managing is nothing but helping corporates to integrate , organise , monitor and remotely manage devices which offers features that maintains health connectivity , security of the devices through out their life time . these features include :
*registration
*authentication
*configuration
*provision
*monitoring
*trouble shooting

Iot device management easily secure , on board ,organise monitor and remotely manage iot devices at a scale . It lets you organise and manage devices .This allows to track operate and manage your devices to the bussiness and security requirments acordingly .

It easily allows you to maintain the health of your device fleet. You can update the device software which have been deployed in the filed .

Device management allows to track monitor manage and secure the devices that are connected . The devices that are connected with iot can be accessed remotely that allows to manage , provisioned in the real time . It reduces the operational and maintenance cost .

It provides continuous information that allows the operation department and it department to work continuously on project . IOT device management allows managing , monitoring and updating devices easily . With the nonstop device management facility there is a possibility of business success .

2. DEVICE CONNECTIVITY AND NETWORKING :

The iot applications are mostly used in networking ,communication and connectivity protocols with internet enabled devices .Communication protocols include CoAP,DTLS and MOTT. Wireless protocols include IPV6,LPWAN ,Zigbee. While sharing the sensor data they collect ,iot devices connect to an iot gateway or other end device where data is locally analysed or sent to cloud for analysis

An example of short range wireless connectivity solutions are as RFID ,NFC,bluetooth ,wifi and zigbee
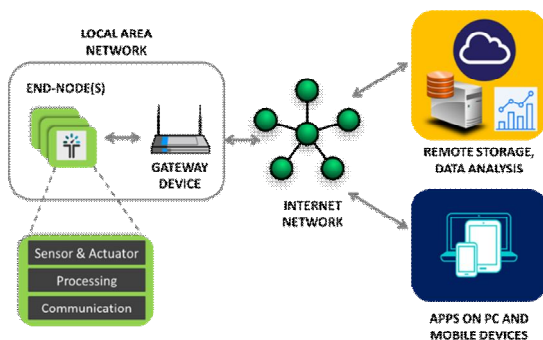
3. IOT DEVICE SECURITY :

IOT is a technology which provides safeguarding facility to the connected devices and networks in the iot.

Iot provides additional features such as internet connectivity to the system of inter related computing devices ,

mechanical and digital machines . Allowing third party access to the connected devices there are certain vulnarabilities if the devices are not properly protected .

There are certain challenges in the security of iot environment which ensures end to end security .In the design phase of a device security is not given atmost importance .

A Major drawback of iot security is default password which leads to security breaches .even when the new passwords are entered they are not strong enough to prevent third Party access .

There are certain iot security tools which was released by GSM association , the IOT security foundation , the Industrial ,Inertnet Consortium .

IOT networking security is a challenging facility than the traditional network security because it has a wide number of communication protocols ,standards and device sub capabilities . These capabalities include end point security features such as providing antivirus and antimalware features which prevents the third party access .
Common iot security measures are :
*incorporating security at the design face.
*public key infrastructure (PKI)and digital certificate .
*API security .
*Identity management.
*Hardware security .
* Network access control .
*Security gateway .
*Patch management and continuos software updates.
*Integrating teams .
*Consumer education

*Incorporating security at the design phase:

Iot should develop security at the design phase of any consumer or enterprise,or industrial based development .

*Public key infrastructure and digital certificates:

This plays a crucial role in the security development of iotdevices ,providing the control and trust to the encrypted keys which secures data exchanges over network
*API security:

Application program indicator is the most essential factor which provides intergration of data that is sent from iot devices to back end systems

*Identity management:

Providing device with the unique identifier is a very difficult to understand its behaviour ,how it is ,what it is,and how it interacts with the other devices

*Hardware security:

It makes the devices tamper-proof or tamper – evident.Thiswill be used when the device are used in the bad environment where the devices are not monitored physically.

*Network security:

Protecting the iot network includes port security ,disabling port forwarding and closing ports when not needed .it uses antimalware and firewalls prevents system blocking

*Network access control:

NAC helps identifying the devices that are to the network. It provides a facility which tracks and monitors the devices

*Security gateways:

It acts the intermediary between iot devices and the network,it have the best processing power memory and capabilities
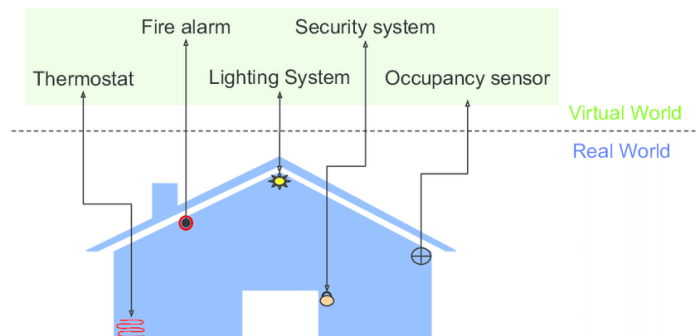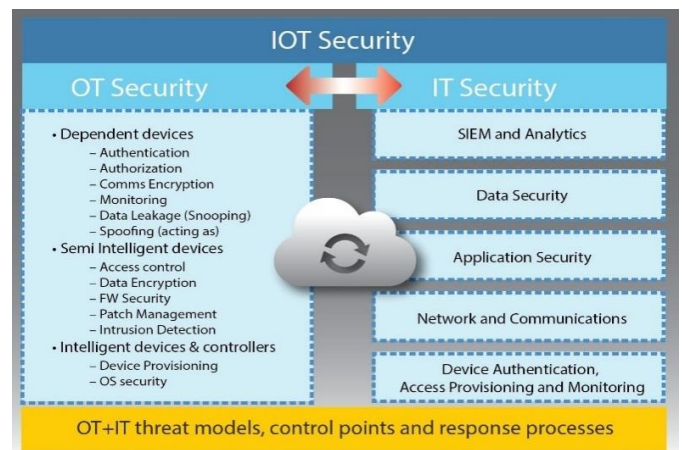
*Patch management :

It provides continuous system updates to devices than senting it through internet connection

*Integrating teams:

Along with the security,training integrating teams and siloed teams are also useful

*Consumer education:

Consumer should be aware of the drawbacks and the dangers of iot systems and provide steps to stay secure.


BENEFITS OF IOT

Iot provides communication between devices and machine to machine communication. There is no human intervention the machine are controlled and connected automatically. It provides vast information which helps to take better decision .And the most important advantage of iot is monitoring .It monitors the devices that are connected to internet of things.Iot is best one in saving the time.And the second most imporatant advantage is saving money .It provides tge best facility at cheaper rate. As the iot allows the automation of devices that are connected leads to better monitoring of devices without any human intervention. The

machine to machine interaction provides better efficiency. It gives appropriate results in a less time. The applications of this technology are more comfortable,and convenient .
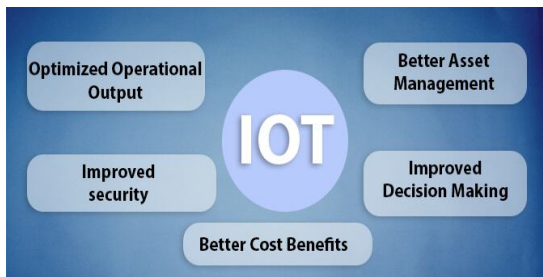

Functions and Benefits of IOT
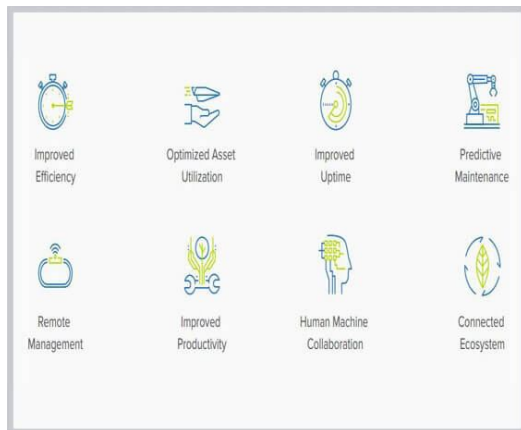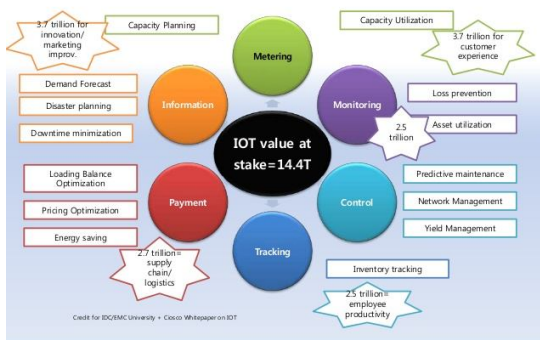
DISADVANTAGES:

The internet of things is not compatible for international tagging and monitoring equipment.And these are complex systems which have more opportunities of failures.And the iot data are being transferred privacy of data is lacking in iot. As there is no privacy of data the security is also major problem here ,as the hacker can easily access to the devices
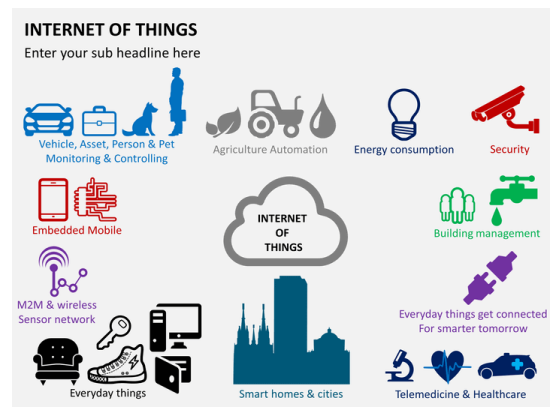
Disadvantages of IOT

- The IOT are the breach of privacy
- Over-reliance on technology
- Loss of jobs
- Decreasing the traditional ethics
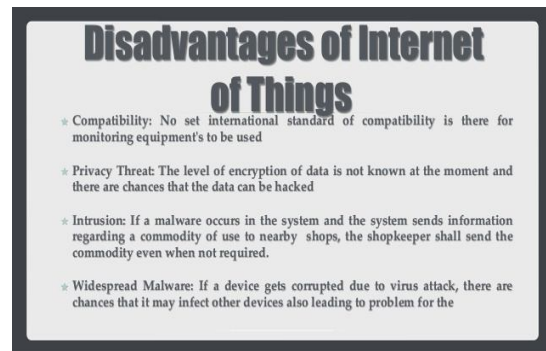
III. CONCLUSION

The internet gave us the opportunity to connect in ways we could never have dreamed possible. The internet of things will take us beyond connection to become part of a living ,moving,global nervous system . the number of technology are being used in iot in behalf of the deployed technology . these technology supports in various activities. In the upcoming modern world the internet of things will develop in drastic manner and will provide many facilities.

REFERENCES

[1] https://www.iotforall.com/what-is-iot-simple-explanation/amp/

[2] https://www.webopedia.com/amp/TERM/I/internet_of_things.html

[3] https://internetofthingsagenda.techtarget.com/definition/IoT-device

[4] https://internetofthingsagenda.techtarget.com/definition/Io
    T-security-Internet-of-Things-security

[5] https://aws.amazon.com/iot-device-management/

[6] https://www.linkedin.com/pulse/advantages-
    disadvantages-internet-things-iot-tommy-quek