A STUDY ON INTERNET OF THINGS AND ITS SECURITY ISSUES

R.Valarmathi
Assistant Professor, Dr.Sivanthi Aditanar College of Engineering,Tiruchendur

Abstract

Internet Of things (IoT) is the network of physical objects that are connected t o the internet where each object can able to share data and information with other devices connected to the internet. IoT can be a person or an automobile with built in sensors. Physical objects that had been assigned an IP address can be able to share data and information without human intervention. Physical objects embedded with RFID (Radio Frequency Identification), sensor which would allow devices to communicate with each other. Security is a major challenge in IoT. Challenges include security, connectivity and power management. These challenges need to be addressed for implementation of IoT.

Keywords : IoT, RFID, Security, Network, WSN

I INTRODUCTION

IoT is the network of devices, buildings, vehicles and other things which are able to embed with electronics, sensors, software and network connectivity which allows these to connect, interact and can able to exchange data[3]. IoT is a wide range where billions of devices are having communication among each device through network. These devices can be able to monitored and controlled remotely. It is based upon WSN(wireless sensor networks) that comprising spatially distributed autonomous devices using sensors to monitor physical as well as environmental conditions. IoT plays a vital role and provide various internet applications. IoT is an intelligent technique that reduces manual effort as well as easy to access physical devices. This technique having feature that any device can be able to control without human interaction. IoT is a combination of software, hardware, data and services. Applications of IoT include smart home, smart city, smart farming, connected health, etc. Home automation system which uses Bluetooth or Wi-Fi for exchanging of data between various devices of home. It becomes growing and evolving technology so there is a need to notice various kinds of challenges and issues[10].

II IoT AND ITS CHARACTERISTICS

IoT is a collection of physical objects or things which has the ability to capture information. It is an intelligent system that have computing and communicating ability[8]. The basic characteristics of IoT are showed below[6,10,].

1. Interconnectivity

   With the help of IoT anything can be able to interconnect with global information and communication infrastructure.

2. Heterogeneity’

   Devices in IoT are heterogeneous as it will based upon different hardware platforms and networks. They can be able to interact or communicate with each other devices through different networks.

3. Dynamic changes

   State of devices would change dynamically, for example connected or disconnected, sleeping and waking up as well as context of devices includes speed and location.

4. Enormous scale

   More number of devices needs to be managed and that will be able to communicate with each other would be atleast an order of magnitude greater than the devices connected to the present internet. Generated data must be managed that will be more critical. This incorporates semantics of data as well as efficient handling of data.

5. Safety

We receive many benefits from IoT, hence we must ensure about safety. Safety includes our own personal data and safety of our physical well being. Create a security paradigm.

6. Connectivity

It enables network compatibility and accessibility. Accessibility means getting on a network whereas compatibility provides the ability to consume/use and produce data.

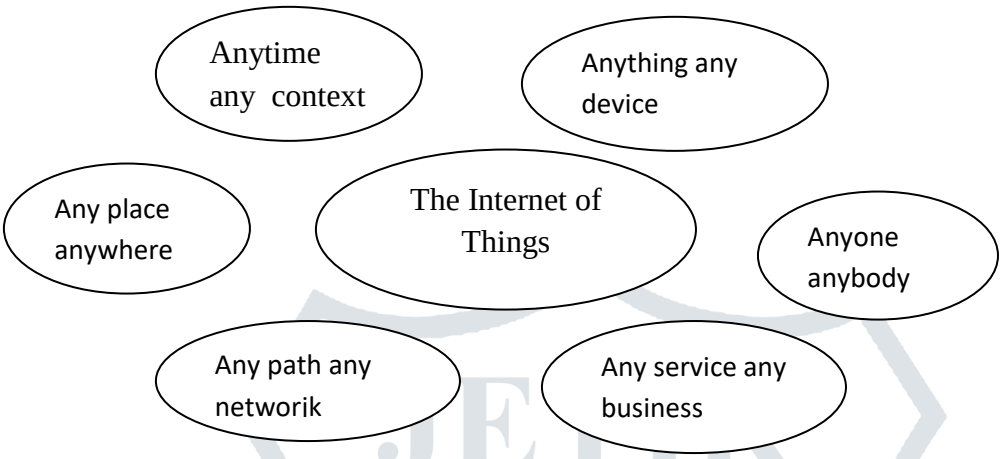

Figure 1 Internet Of Things

III ENABLING TECHNOLOGIES FOR IoT

It enables advanced services by interconnecting virtual and physical things based upon existing and evolving information and communication technologies. With the help of IoT communication is extended to all things/objects via internet. IoT is much more than M2M communication, sensor networks, WSN, GSM, 2G/3G/4G, GPRS,RFID, Wi-Fi, GPS, microprocessor, microcontroller, etc. These are considered as the enabling technologies that make IoT applications as much as possible.

Enabling technologies[7] includes and can be grouped into three categories as follows. 1. Technologies enable “things” to gain contextual information 2. Technologies enable “things” to process contextual information 3. Technologies to improve privacy and security. IoT is a mixture of different software and hardware technology and not a single technology. Hardware provides solutions based on integration of information technology while software is used to store, retrieve and process data and communication technology includes electronic systems being used for communication between groups or individuals. The key enabling technologies for IoT is shown in figure2.

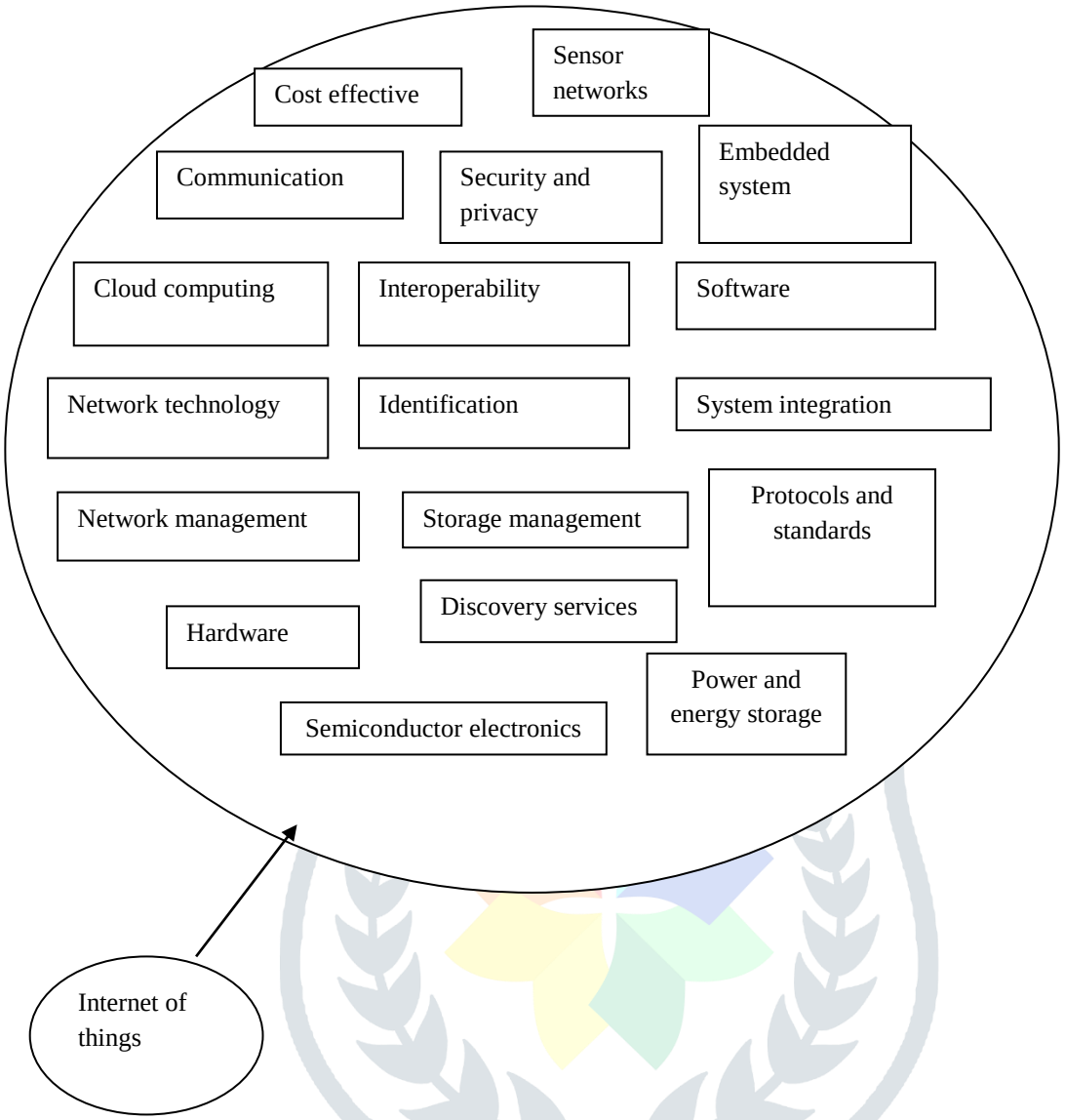

Figure 2 Internet of things: Enabling technology

IV IOT ARCHITECTURE

IoT architecture includes different layers of technologies that support IoT. Figure 3 represents the architecture of IoT. It illustrates how various technologies relates with each other and to communicate with modularity, scalability and configuration of IoT deployment in different scenarios. Functions of each layer is described below [10,12].

Smart device/Sensor layer

The lowest level layer is the smart objects which are integrated with sensors. Sensors would enable interconnection of physical and digital worlds which allows information to be gathered and processed. Different types of sensors are available for different purposes. Sensors have the ability to make measurements such as air quality, temperature, humidity, speed, pressure, movement, flow, electricity, etc. In some situations, sensors have also had memory which enables them to record certain number of measurements.

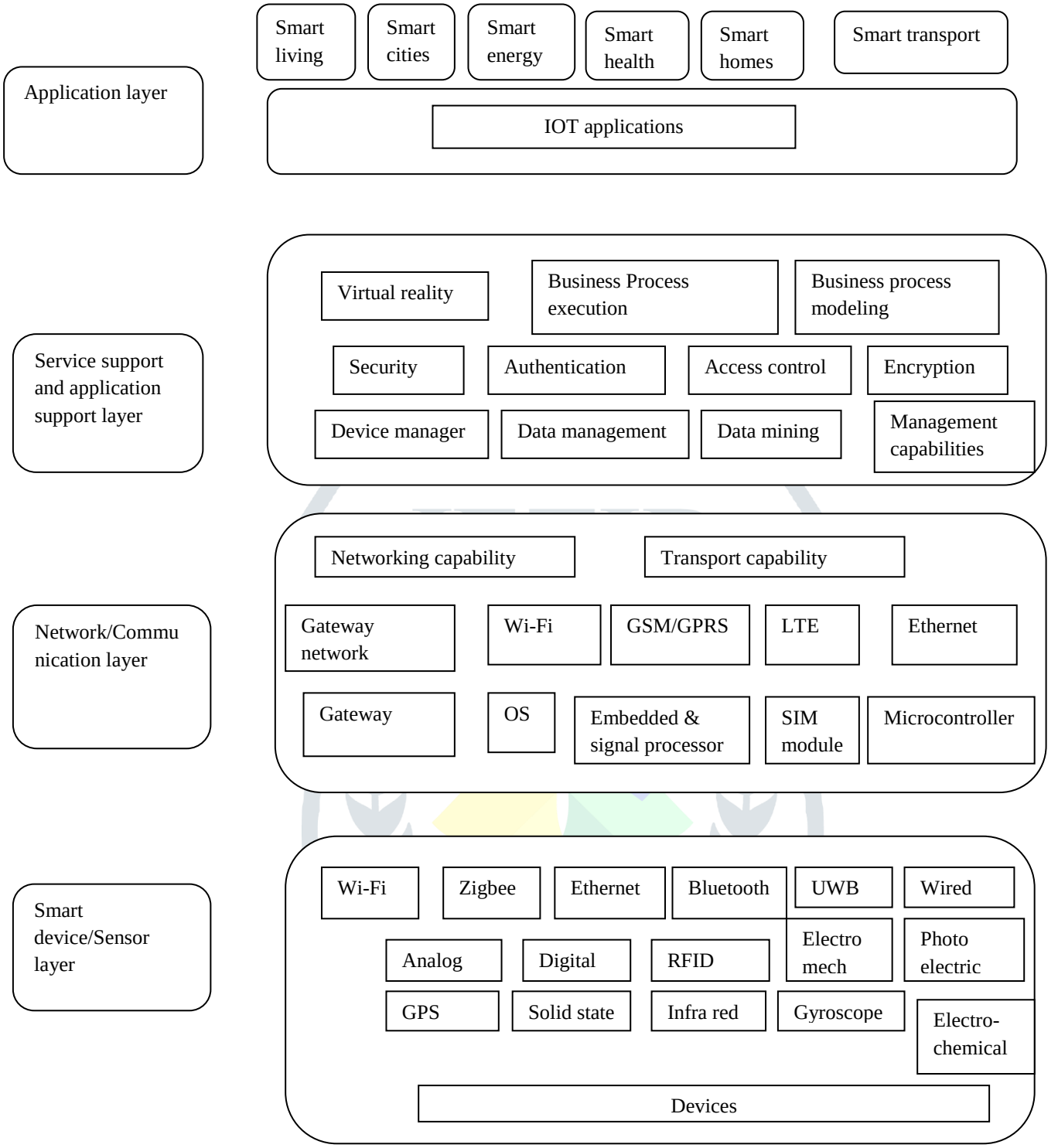

Figure 3 Architecture of IoT

A sensor can be able to measure the physical property and convert it into signal which can be understood by an instrument. Sensors are grouped together according to their different purpose such as body sensors, environment sensors, vehicle telematic sensors, home appliance sensors, etc.

Most of the sensors require connectivity to sensor gateways. This comprise of LAN such as Wi-Fi and ethernet or personal area network (PAN) such as Bluetooth, zigbee and ultrawideband (UWB). Sensors that does not require connectivity to sensor aggregators their connectivity to backend servers can be provided using wide area network (WAN) such as GPRS, GSM and LTE. Sensors that consume low power and low data rate connectivity that form networks named as wireless sensor networks (WSN). WSNs becoming popular while it retains adequate battery life and covering large areas.

Gateways and networks

Large volume of data would be produced by these small sensors and this requires a high performance, robust wired or wireless network infrastructure as a transport medium. With high demand needed to serve a wide range of IoT applications and services such as context aware applications, transactional services, etc. Multiple networks with different technologies and access protocols are needed to work with each other in a different configuration. These networks may be in public, private or hybrid models and are built to support communication requirement for bandwidth, latency, security. Various gateway networks (Wi-Fi, GSM, GPRS) and gateways (microprocessor, microcontroller) are shown in figure 3.

Management service layer

Management service layer important feature is the business and process rule engines. Data management is having the ability to manage data information flow. Management service layer having the data management, information can be able to accessed, integrated and controlled. Data filtering techniques includes data integration, data anonymisation, data synchronization are used to hide the details of information whereas providing only necessary/essential information that would be usable for relevant applications.

Application layer

IoT applications includes smart environments in fields such as agriculture, transportation, retails, city, factory, emergency, healthcare, culture and tourism, environment and energy, user interaction, lifestyle. IoT application includes smart homes, smart transportation, smart planet and so on [11]. It is a topmost layer which is having business logic, UI to end user formulas.

IV INTEROPERABILITY IN IoT

IoT main objective is to integrate physical world with virtual world via internet which provides a medium to communicate and exchange/ interchange information. Interoperability is the ability to exchange data and information. This provides various challenges on how to receive the information, exchange data and use information to understand of it and able to process it. Various types of interoperability includes technical interoperability, semantic interoperability, syntactical interoperability, organization interoperability [9]. Simple representation of dimensions of interoperability is shown in figure 4.

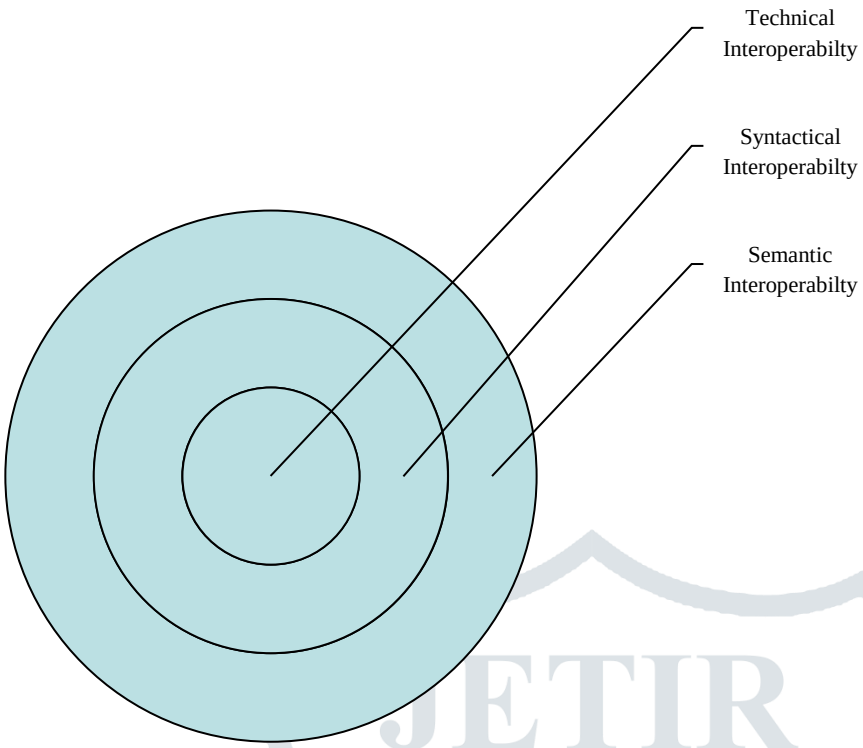

Figure 4 Dimensions of Interoperability

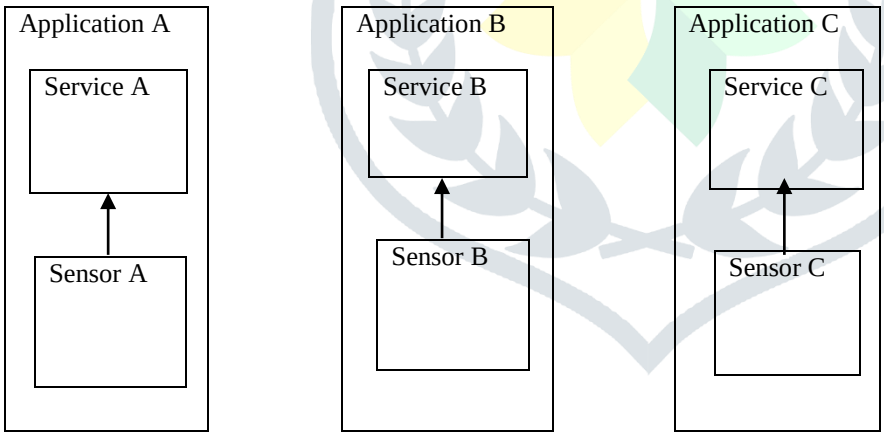

Figure 5 Non-Interoperable IoT

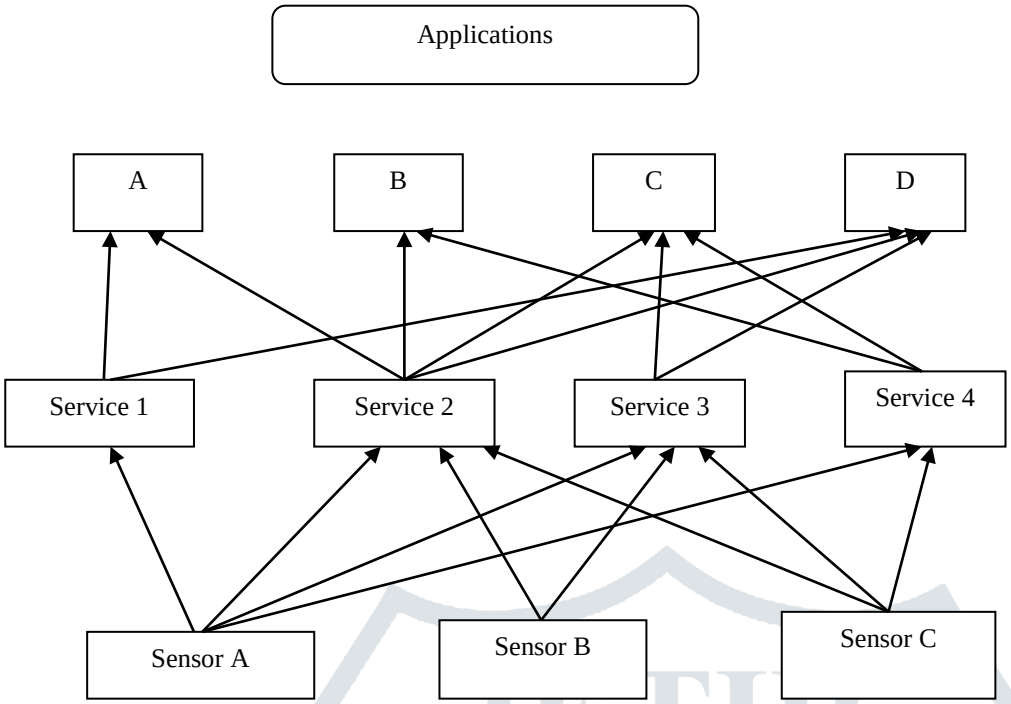

Figure 6 Interoperable IoT

V SECURITY ISSUES IN IOT

1. Security issues in Perception layer

It is the lowest level. It is the source of access to information throughout IoT. Security issues in this layer includes physical security of sensing devices and information collection security. IoT cannot provide security because of due to its diversity, simple and weak protective capability of sensing node, energy limited which would affect security of RFID, WSN and M2M terminal. RFID includes security problems such as information tracking, replay attacks, cloning attacks, man-in-the-middle attacks [8].

1.1 Security issues in WSN

WSN is a network of nodes that would sense and control the environment. It includes actuator nodes, sensor nodes. It is a collection of nodes so there may be a possibility of issues in security.

- Attacks on secrecy and authentication
- Attacks on network availability
- Silent attacks on service integrity

1.2 Security issues in RFID technology

RFID technology is mainly used as RFID tags for automatic exchanging of information without human intervention. RFID tags would occur to various attacks from outside due to incorrect status of security of RFID technology [5].

The most common types of attacks and security issues of RFID tags are as mentioned below.

i) Unauthorized tag disabling

In DoS attacks, RFID tags become incapable permanently or temporarily. This kind of attacks makes RFID tag available to misbehave and malfunction under scan of tag reader.

ii) Unauthorized tag tracking

Tracing of tag by dishonest reader resulting in giving important information for example persons address. Thus for customer point of view buying a product that have an RFID tag guarantees them no confidentiality.

iii) Unauthorized tag cloning

Capturing identification information through manipulation of RFID tags by dishonest readers. Once identification information tag is compromised, replication of tag is possible which can be used to bypass fake security measures.

iv) Replay attacks

In this attack, the attacker uses a tags response to a dishonest readers challenge to impersonate the tag.

2. Security issues in physical layer

It performs different functionalities such as encryption and decryption, modulation and demodulation, selection and generation of carrier frequency [5]. Attacks includes the following.

i) Jamming- Network would suffer

ii) Node tampering- Extracting sensitive information

3. Security issues in network layer

It includes confidentiality, DoS attacks, illegal access, data eaves dropping, virus attack, man in the middle, etc. It would also causes network security issues like transfer of data needs number of nodes would lead to network congestion resulting in DoS attacks [8].

i) Homing

In this, searching is made in the traffic for cluster heads and key manages which have the capability to shut down the whole network.

ii) Hello flood attack

It causes high traffic in channels which makes many number of useless messages.

iii) Selective forwarding

In this attack, a compromised node sends few selective nodes instead all the nodes.

iv) Acknowledgment flooding

In this attack, a malicious node spoofs the acknowledgement that would provide false information to the destined neighbouring nodes.

4. Security issues in application layer

It includes eavesdropping and tampering. A path based DoS attack is initiated in this layer by simulating the sensor nodes to create a large amount of traffic in routes between the base station.

VI FUTURE CHALLENGES FOR IoT

Key challenges needs to be addressed before mass adoption of IoT would occur [1, 2, 12].

1. Privacy and security

We need to address security function and trust consequently and adequately. New challenges identified for trust, privacy and reliability includes i) providing trust and quality of information in shared information models to enable re-use of data among various applications ii) Provide secure exchanging of data between IoT devices iii) Providing protection mechanisms for vulnerable devices.

2. Cost versus usability

IoT uses technology to connect physical objects/devices to the internet. Components cost needed to support capabilities such as sensing, tracking and control mechanisms would become inexpensive in the forthcoming years.

3. Interoperability

Nowadays different industries use different standards to support their applications. Having numerous sources of data and heterogeneous devices, it is important to use standard interfaces between these diverse entities. Hence IoT systems need to handle or maintain high degree of interoperability.

4. Data management

   Data management is the main thing in IoT. Massive amount of data are generated and exchanging of data and information is taken place hence that data needs to be handled that becomes critical.

5. Device level energy issues

   How to interconnect things in an interoperable way so that taking into energy constraints knowing that communication is the most energy consuming task on devices.

VII APPLICATIONS

IoT application includes smart environment/ spaces in fields such as agriculture, health, transportation, environment and energy, etc. Some of the IoT applications are described below [2].

1. IOsL (Internet of smart living)

   It includes remote control weather, smart home appliances, switching on and off remotely appliance to save energy and avoid accidents. Smart home appliances includes refrigerators with LCD screen saying what is inside in refrigerator, ingredients that you need to buy and what are and all the food that are going to expire, etc and with all these information available on the smart phone app. Weather displays outdoor weather conditions comprising of humidity, pressure, temperature, rain levels, wind speed with ability to transmit data over long distances.

2. IOsE(Internet of smart environment)

   Air pollution, forest fire, detection, water quality, weather monitoring, river floods can be monitored. Protecting wildlife- Using GPS/GSM modules to identify location and track wild animals and communication would take place through sms.

3. IOsC(Internet of smart cities)

   Monitoring vibrations in bridges, building, historical monuments. Transportation- Smart roads and highways with warning messages to take diversions according to climatic conditions. Smart Parking- Availability of parking spaces in the city where the residents can able to find and reserve closest available spaces. Waste management, safety also includes in IOsC.

4. IOsH(Internet of smart health)

   Physical activity monitoring- Wireless sensors placed across mattress would sense motions like breathing and heart rate which provides data available via app on smartphone.

5. IOsA(Internet of smart agriculture)

   Animal tracking/Farming- Tracking location and identification of animals grazing in open pastures can be identified and also location can be tracked Field monitoring- Crop field can be efficiently monitored ie) Management of agriculture fields includes control of fertilizing, watering and electricity.

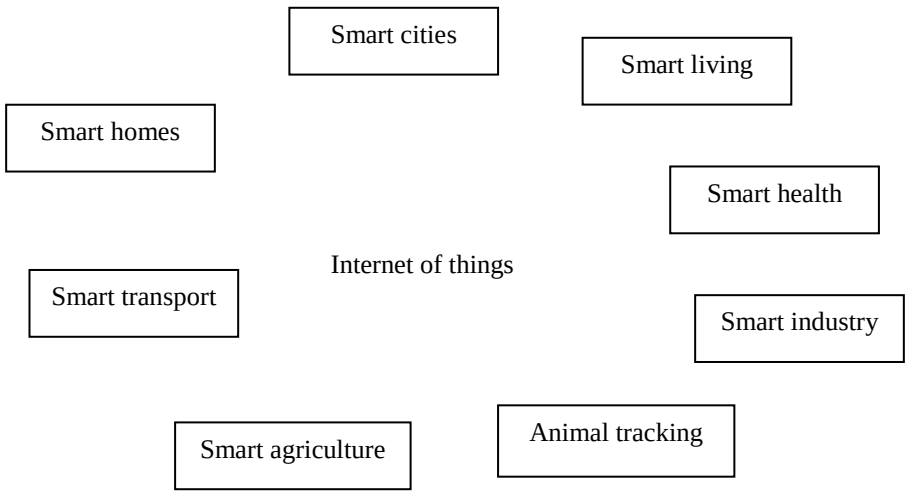

Figure 7 IoT Applications

VIII CONCLUSION

IoT is a new revolution of the internet and it is a research topic in the field of computer science and information technology, embedded because of having various applications and different mixtures of communication and embedded technology in its architecture. IoT would change our lifestyle, work, play, etc. It will going to change every aspect of our lives. Avoid accidents in cars through different kinds of sensors available ie) would sense and it would avoid accidents [4].

REFERENCES

[1] Dr. Ovidiu Vermesan SINTEF, Norway, Dr. Peter FriessEU, Belgium, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems", river publishers' series in communications, 2013.
[2] Dr. Ovidiu Vermesan SINTEF, Norway, Dr. Peter FriessEU, Belgium, "Internet of Things–From Research and Innovation to Market Deployment", river publishers' series in communications, 2014.

[3] https://en.wikipedia.org/wiki/Internet_of_things.

[4] Martin Serrano, Insight Centre for Data Analytics, Ireland ,Omar Elloumi, Alcatel Lucent, France, Paul Murdock, Landis+Gyr, Switzerland, "ALLIANCE FOR INTERNET OF THINGS INNOVATION, Semantic Interoperability" , Release 2.0, AIOTI WG03 – loT Standardisation,2015.
[5] Tuhin Borgohain, Uday Kumar and Sugata Sanyal ―Survey of Security and Privacy Issues of Internet of Things
[6] [http://www.reloade.com/blog/2013/12/6characteristics-within-internet-things-iot.php].
[7] Jayavardhana Gubbia, Rajkumar Buyya, Slaven Marusic , Marimuthu Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems 29 (2013) 1645–1660

[8] QuandengGOU, Lianshan YAN, Yihe LIU and Yao LI ―Construction and Strategies in IoT Security System‖ 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing.

[9] H. van der Veer, A.Wiles, "Achiveing Technical Interoperability —the ETSI Approach", ETSI White Paper No.3, 3rd edition, April 2008, http://www.etsi.org/images/files/ETSI WhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf
[10] Jim Chase, "The evolution of internet of things", White Paper

[11] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi and Talha Kamal ―A Review on Internet of Things (IoT)‖ International Journal of Computer Applications (0975 8887)

[12]https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/InternetOfThings.pdf