Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

Different Security Issues of Internet of Things (IoT)

Manish Shriram Patil
E&TC,
Sinhgad College of Engineering,Pune
Savitribai Phule Pune University Pune, India

Dr. Achala Deshmukh
E&TC,
Sinhgad College of Engineering,Pune
Savitribai Phule Pune University Pune, India

***Abstract*—In our daily life Internet of Things(IoT) are present everywhere. Internet of Things is the set of all physical objects that are attached to internet. IoT has various applications in hospitals,our homes, prevent fires and many more effective functions. But this applications can come under huge risks of security issues and privacy loss. To make this IoT device more secure, lot of research work has been carried out to counterpart those problems and find for better way to reduce those risks .In this paper we examine in detail about different security challenges,requirements in Internet of Things and research challenges.**

I. INTRODUCTION

The Internet of Things (IoT) describes about a future where every day bodily objects can be brought together to Internet and also will be able to know themselves to other devices.IoT is closely established with RFID, sensor technologies, wireless technologies. It permits objects to be sensed and also to control remotely across present network infrastructure. Internet is a medium which connects people all over the world for performing different applications like emailing, gaming, conferencing, online trading and so on. IoT also includes, Connection of Cameras to internet that allows you to post pictures online using internet with a single click, changing the lane while driving safely, switching off the lights automatically in a room when no one is around. Internet of things is able to transfer data over the network for longer distance without human interaction.

II. THE CONCEPT OF IOT AND ITS BASIC CHARACTERSTICS

IoT based objects has ability to gather data for physical world. IoT is smart intelligent system, which has communicating as well as computing ability. Some Characteristics of Internet of Things are :

A. Comprehensive awareness:

It is because of sensors and RFID. The advantage of this sensor is to collect the information of the object.

B. Reliable transmission:

Reliable transmission provides real time and high accuracy.

C. Intelligent processing:

Intelligent processing does the analyses and couples the intrinsic information as per the user speculation.

III. IOT ARCHITECTURE

There is a extreme necessity for a flexible layered architecture as IoT is capable of operating as a unit with various heterogeneous objects through the Internet. The figure 1 shows the 3-layer IoT architecture.

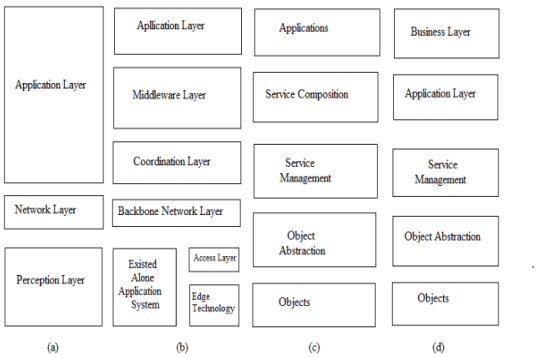

Fig. 1. IoT Architecture (a) Three Layer (b) Middle-ware based Layer (c) SOA based Layer (d) Five-layer

The main standard is a 3-layer architecture can be divided into three layers which are classified as Application, Network, and Perception Layers respectively. In recent times, another block is added called literature abstraction to IoT architecture.

A. OSI Layer

The first layer is the perception layer or objects, which includes different sensors that are used in IoT that collect and processes the data. The object layer includes actuators and sensors. The actuators and sensors carries out different operation like identifying motion,weight,location,temperature, humidity, acceleration, vibration etc. The proper digitalisation and transformation of information to object abstraction layer is performed using OSI layer. The data through secure channels are transferred by perception layer.The perception layer initiates big data created by IoT. [3] Object layer explains physical meaning to every object.This layer consists of data sensors in the various form of RFID tags, IR sensors or other wireless sensor networks (WSN) which senses temperature, location, speed, humidity, and so on. This layer fetches the important information of objects from sensing device which are joined to those objects and transmit the data into digital signals. Once the digital signal is obtained it is passed to network layer [4].The collection of sensor, actuators which forms WSN s done in Perception Layer [6].

B. Object Abstraction Layer

This layer transmits information to the Service Management layer which is produced by perception layer via secure channels. The data can be transmitted through WiFi,3G,RFID,GSM,Bluetooth,ZigBee,etc. Object Abstraction Layer carries the processes of Cloud Computing and Data Management [3].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

C. Service Management Layer

Middleware layer or Service Management layer matches services with the user request data based upon the name and addresses. This layer passes the received data, then makes the decisions and finally delivers the required services. The Middleware layer allows the IoT based application programmers to concern with the heterogeneous objects by not considering specific hardware platform [3]. We can say that the Information which is received from sensor based devices is processed by the Middleware Layer.

D. Application Layer

The Application flake makes available the services which are asked by the user. Like it provides air humidity and the temperature measurement. This layer is useful for the larger scale development of the Internet of thing network. The different applications of IoT can be smart transportation, smart homes and son on [4]. Application Layer is top most layer that includes business logic and formulas [6].

E. Business Layer

This layer runs the complete IoT systems behaviour and services. Also builds a business model,flowcharts,graphs etc which are based upon the information experienced by this Layer. This Layer also monitor,implements,designs, analyzes and also develops the elements related to IoT. Business layer also gives the assistance to the decision making processes which is based upon Big Data analysis. [3].

IV. SECURITY ISSUES IN IoT

1) Security issues in perception layer

Perception layer is last layer of the IoT construction setup. It provides the needed information to user using the IoT. There are many security issues in Perception layer like security of information collection and security of physical sensing device . Sometimes due to energy limitation and diversity of sensing node IoT is not able to provide proper security system which affects the security of WSN and RFID. The RFID also has various security issues like leakage of information, information tracking, replay attacks, tampering, man-in-the-middle attacks, cloning attacks. Different security issues faced in perception layer are the capture gateway node, unfair attacks, congestion attack, cloning attacks , and forward attack [8].

2) Security issues in physical layer

This layer carries outs various operations such as selection and generation of carrier frequency, Demodulation ,modulation, encryption and decryption, reception and also transmits the information [5]. Physical layer, mainly attacked through Jamming and Node Tampering.

3) Security issues in application layer:

The close integration between the computer technology, communication technology, and industry professional which is able to find applications in multiple aspects are application of IoT. Tampering and eavesdropping are some of the security issues [8]. Responsibility of the traffic management also lies with the application layer. Also providing software services for different applications that performs the transmission of information into a generic form or helps in collecting information by sending any queries [5]. To create large traffics in route towards the base station, Path-based DoS attack is initiated in this layer by stimulating the sensor nodes.

4) Security issues in network layer

Network Layer faces some kind of risk such as illegal access,dataeavesdropping,confidentiality,integrity,destruction, DoS attacks, man-in-the-middle attack, virus attack, etc.IoT senses more number of devices hence multiple variety of formats of information is gathered and the information has a different-sources, solid and diverse characteristics. Different network security issues like transferring of information requires higher number of nodes which leads to network congestion, resulting in DoS assault are also caused in network layer [8]. Various DoS assault in the network layer are:

a) Hello flood attack:

This type of attack generates more traffic in channels by adding the channel with large count of useless messages. One malicious node transmits useless message then that message is replied by attacker to generate the high traffic.

b) Homing:

A search is carried out in traffic for key managers and cluster heads which have the ability to switch off whole network.

c) Selective Forwarding:

In Selective Forwarding, nodes which are compromised transmits some selected nodes rather transmitting all other nodes. The proper node selection depends on the requirement of attacker to obtained the malicious objectives and so such nodes don't forward the packets of information.

d) Sybil:

In this type of attack, the attacker attacks one single node and then presents it with multiple identities to different nodes.

e) Wormhole:

This attack causes new location of bits of information from its original position. By passing bits of information over the low latency, the relocation of the packets of data can be carried out.

V. CONCLUSION

In this paper we have discussed about the present state of internet of things, also we have examined the different security threads in IoT. We discussed the various layered in IoT architecture and applications of IoT.We have also discussed about the solutions to improve the robustness in various service level and systems for global navigation satellite system. In future, detection of Denial of Service (DoS) attack in IoT will be put forward and effectiveness will be calculated.

ACKNOWLEDGMENT

Author express his sincere thanks to our research guide Dr.Achala Deshmukh,Department of Electronics & Telecommunication Engineering, for their valuable guidance and continuous support. Also Author takes this opportunity to thank Dr. M.B.Mali, Head of Department of Electronics & Telecommunication Engineering and our PG Co-coordinator Dr. Achala Deshmukh for their helpful suggestions.

REFERENCES

[1] Jun Wei Chuah ―The Internet of Things: An Overview and New Perspectives in Systems Design‖ 2014 International Symposium on Integrated Circuits 978-1-4799-4833-8/14.

[2] Sarita Agrawal, Manik Lal Das ―Internet of Things – A Paradigm Shift of Future Internet Applications‖ Institute of technology, nirma university, ahmedabad – 382 481, 08-10 december, 2011.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

[3] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash ―Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications‖ ieee communication surveys & tutorials, vol. 17, no. 4, fourth quarter 2015.

[4] 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) Volume 113 - No. 1, March 2015.

[5] Tuhin Borgohain, Uday Kumar and Sugata Sanyal ―Survey of Security and Privacy Issues of Internet of Things‖

[6] Krushang Sonar, Hardik Upadhyay ―A Survey: DDOS Attack on Internet of Things‖ International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X Volume 10, Issue 11 (November 2014), PP.58-63.

[7] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito and Mark Vinkovits ―Denial-of-Service detection in 6LoWPAN based Internet of Things‖ 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).

[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] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva ―Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues‖ ieee communication surveys & tutorials, vol. 17, no. 3, third quarter 2015.

[10] Qi Jing • Athanasios V. Vasilakos • Jiafu Wan • Jingwei Lu • Dechao Qiu ―Security of the Internet of Things: perspectives and challenges‖ Wireless Netw DOI 10.1007/s11276-014-0761-7.

[11] http//www.slideshare.net.―A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks‖ [Deng+].

[12] Eason, B. Noble, and I.N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (references)