Internet of Things: Architecture, Security Issues and Countermeasures

Mayuri A. Bhabad
P.G. Scholar
Dept. of Computer Science and Technology
Usha Mittal Institute of Technology,
SNDT Women's University
Mumbai, India

Sudhir T. Bagade
Assistant Professor
Dept. of Computer Science and Technology
Usha Mittal Institute of Technology,
SNDT Women's University
Mumbai, India

ABSTRACT

Internet of things (IOT) is widely distributed network of things in which all the information is sent to the internet with the help of sensing devices and Radio Frequency Identification (RFID) tagging system. As IOT does not need any human to machine interaction, it seems to be one of the largest waves of revolution as per the research going on, hence security is needed. But the rapid development of IOT has evolved with the challenges in terms of security of things. This paper is mainly focusing on the concept of IOT, architecture and security issues with suggested countermeasure and suggested further areas of research needed.

General Terms

Security in IOT, Architecture, Challenges, Countermeasures, Security parameters

Keywords

Internet of Things, Wireless Technology, Security issues, Intelligent System

1. INTRODUCTION

The term Internet of Things (IOT), also known as Internet of Objects refers to the networked interconnection of everyday objects, which is generally viewed as a self-configuring wireless network of sensors whose purpose would be to interconnect all *things* [1].

Today the world is totally dependent on the information provided on internet, which is captured by taking images or through text. This clearly specifies the major involvement of a human being for collection of the information. But the problem with human involvement is that, people have limited time and less accuracy, which leads to inappropriate and inconsistent data. Hence, such a system is needed which can automatically capture the data and transfer it to the internet without any human to machine interaction.

Internet of things is a scenario in which all the things are connected to the internet through the information sensing devices for the purpose of intelligent identification and management [2]. These things are provided with the unique identifiers which can be read using RFID tags with the help of sensors (information sensing devices). The thing in the internet of thing can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built in sensors to alert the driver when the pressure is low or any other manmade object that has a unique IP address with the ability to be connected to the network for the transfer of the data [3]. There is a major participation of wireless technology, Micro-electromechanical Systems (MEMS) and the internet in the making of IOT [2]. One of the basic things needed to sense the object in the environment is RFID. Sensing can be possible by assigning each object a unique identifier and then connected to the internet, for smart processing by the transfer of information. IPv6 is playing a very important role in the development of IOT, by using its huge address space one can easily assign an IP address to every *thing* on this planet and could transfer the data over network.

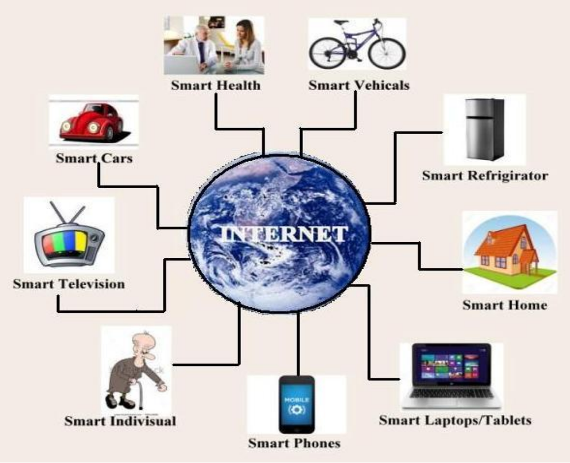

Fig 1: Internet of Things Scenario

IOT is one of the upcoming concepts of technological innovation in the field of networks which will help not only in the industrial development but also in the day to day life of a human being, hence now days IOT is being the research emphasis topic for the researchers and for the enterprises. The typical scenario of IOT is shown in figure 1, depicting the interconnection among things like smart television, phones/laptops, smart refrigerator and smart individual etc. via internet. One can say that by the smart use of IOT, it would be possible to know when the things need to repair, recall or replace without any human interference; which greatly reduce the waste and loss of the objects.

The main objective of this paper is to provide the understanding of security issues of IOT which needs to be studied along with their countermeasures. This paper presents a brief idea of IOT which includes the architecture of IOT, security issues at each layer and countermeasures. These issues would be studying theoretically using parameters like authenticity, integrity, availability, confidentiality etc.

The remainder of this paper is organized as follows. In section II the architecture of IOT have presented. Section III gives main emphasis on security parameters and issues faced by IOT with its countermeasures. Finally, concluded the paper along with the direction for further work in section IV.

2. ARCHITECTURE OF IOT

Internet of things is composed of two words i.e. "Internet" which give a look of interconnected networks and "Things" which clearly shows some objects. But when these two words put together gives a means of "a world-wide network of interconnected objects, uniquely addressable, based on standard communication protocols" [4]. Internet of things does not have a unique definition but as per the different definitions by several research groups around the world, a common concept can be drawn as, when objects can sense and communicate, the intelligent decision making and management is possible without human to machine interaction. Below it present the architecture and security of IOT.

Real time working of IOT is possible through the integration of various technologies together. Xiong Li, Zhou Xuan in [8] described the general architecture of trusted security system based on IOT. Security system such as trusted perception module, trusted terminal module and trusted network module. In this paper, a layered architecture of IOT is presented that gives an idea about basic architecture of IOT. Generally, IOT is divided into three layers: Perception layer, Network layer, and Application layer [5] [6]. All of these three layers have large scale of information with different enabling technologies and features as shown in figure 2.

- Perception layer: The main working of IOT i.e. collection of information is done at the perception layer with the help of different devices like smart card, RFID tag, reader and sensor networks, etc. It has a feature of comprehensive sensing through the RFID system to get object's information anytime and anywhere. Each RFID electronic tag has a unique ID called Electronic Product Code (EPC) which is the only searchable ID allocated for each physical target. Extra information about the product is given by a string of figures imposed on it such as manufacturer and product category with its manufacturing date and expiry date etc. [2].

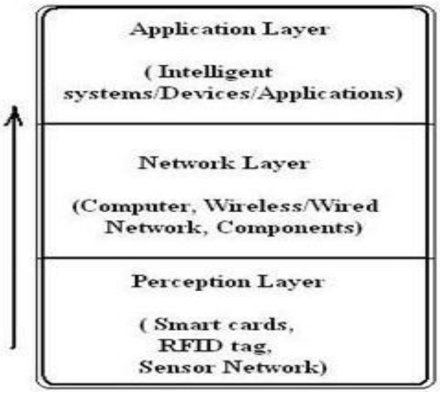
Application Layer
(Intelligent systems/Devices/Applications)
Network Layer
(Computer, Wireless/Wired Network, Components)
Perception Layer
(Smart cards, RFID tag, Sensor Network)

Fig 2: Architecture of IOT

- Network layer: The data gathered by sensors used to be sent to the internet via network layer with the help of computers, wireless/ wired network and other components. Hence network layer is mainly responsible for the transmission of information with the feature of reliable delivery hence this layer also includes the functionality of transport layer.
- Application layer: Analyzing the received information and making the control decisions to achieve its feature of intelligent processing by connection, identification and control between objects and devices. Intelligence means makes use of intelligent computing technology such as cloud computing and process the information for intelligent control like what to do and when to do things hence this layer is also called as process layer.

In the next section a brief idea of security issues at each layer has given.

3. SECURITY OF IOT

Various security issues of IOT has been studied from [2] [5] [9] papers which talk about Security of Things such as Perceiving Security for Information Collection, Transmission Security for Reliable Data Transfer, Processing and Application Security for secure information handling. Below these issues have covered in detail.

3.1 Security Issues

The growing use of IOT system needs a powerful protection against all possible attacks or vulnerability. Hence security is needed at each layer of the IOT system; each layer either consists of devices, applications or networks. Some classified security issues at each layer are as given below:

3.1.1 Security at Perception Layer

Perception layer mainly includes: Smart card, Reader, RFID tag, Sensor network. Each of these devices has following vulnerability which leads to be a security issue of IOT such as sensor attacks, sensor abnormalities, radio interference [14].

3.1.1.1 Terminal security issues [5]

For perception of things it needs a large number of terminals, terminals are used for real-time data collection to be presented to the user. This process needs an authentication and data integrity. Due to the wireless nature of communication, IOT can face threat from the hackers, virus attacks etc. The main problems existed in perception terminals include leakage of confidential information, tampering, terminal virus, copying and other issues.

3.1.1.2 Sensor network security issues [5]

The sensor nodes are responsible for data transmission, data acquisition, integration and collaboration. As they operate on their own battery with less security protection, they can face complex security issues as follows:

- Invoking Malicious Codes: Malicious programs such as worm which does not require any parasitic file, can easily affect the wireless and sensor network, hence it will be very difficult to detect the malicious code and act accordingly.
- Defect of the tag: Due to the limited cost of tag, it is not possible to provide enough security which leads to illegal use of legal reader due to which an attacker can easily get the information on tag and can illegally access RFID system without any authorization by counterfeiting. Any rewritable tag can be copied, decoded or fabricated by the attacker.

3.1.2 Security at Network layer

Network layer mainly including Computers, Wireless or wired network, faces security issues such as network content security, hacker intrusion, illegal authorization [15].

3.1.2.1 Data transmission security issue

The goal of network layer is to transmit information, the information need to be transmitted securely. The security of the network layer is of two main types: The first is from the security risks of the IOT itself; the second is from the related technologies and protocol defects during design and implementation [5]. In wireless networks, nodes can move freely, they can join or leave the network at any time without any prior authentication. This makes wireless networks to be more malicious or vulnerable for the security concern. IOT network should have that capacity to handle such malicious destruction, but as per the researchers existing mechanism is not enough to handle this security issue.

3.1.3 Security at Application layer

Application layer mainly includes the intelligent devices for effective decision making. Each of these has some vulnerability which leads to be an issue of the security of IOT.

3.1.3.1 Application safety issues

Application layer mainly contains a variety of applications for example, industrial monitoring, smart grid, monitoring services, or any other intelligent system. The main security problem can be its own design flaws that can attract any attacker to attack. Malicious code or software vulnerabilities can be introduced in such defected systems. Another issue can be the integration of various areas of techniques and business needs which can cause a bottleneck for the massive data processing and on operation control [12] this can lead to the security issues of reliability and safety for IOT.

Some of the issues could be privacy protection technology, database access control, protection technology of secure electronic products, information leakage tracking technology and intellectual property of software [16].

3.2 Security Parameters

Based on the IOT security issues, the need of security is required for IOT system. Therefore looking at the traditional parameters of security demand it needs to build a safe internet system of things, which are as follows,

- Authenticity: Received information by a reader should be noticeable whether is sent from authenticated electronic tag or not.
- Confidentiality: Sensitive Information shall not be leak to any unauthorized reader by using an RFID electronic tag.
- Integrality: While transmitting the information to IOT, data integrity can ensure the originality of information. It should ensure that the information transmitting is not fabricated i.e not rewritten, copied or replaced by the attacker.
- Privacy: Privacy such as identity or commercial interest of an individual user should be protected by the secure IOT system.
- Availability: An authorized user can able to use various services provided by IOT and can prevent DOS attack for the availability of the services. DOS attack is major cause for threat to the availability.

3.3 Security Countermeasures

The Xu Xiaohui [5] talked about the countermeasures for the security issues of IOT. Some of them as certification, access control, data encryption and cloud computing are discussed in this subsection.

3.3.1 Certification

Certification is a secure way of confirming the true identity of both the parties which communicate with each other. Hence by using Public Key Infrastructure (PKI), it is possible to achieve the strong authentication by two way public key certification for preventing authenticity and confidentiality of the IOT system. Notarization is another solution for security purpose. Notarization is a trusted third party i.e. a certificate authority that facilitates interactions between the users to assure the properties of data exchange [13].

3.3.2 Access Control

Access control is another mechanism which gives secure environment of IOT by limiting the access control for machines, objects or people which are illegal to access the resources. Certification and access control technology are correlated with each other. For correct access control, IOT should ensure the correct identification by certification technique. Access control can be implemented on the area such as: Encrypt password, confidential directories or files, configuration and update rights etc. Designing a secure key Agreement scheme to restrict the key information to be attacked on can be helpful for it.

3.3.3 Data Encryption

Encryption technique is used to prevent the information from tampering and to maintain confidentiality as well as integrity of the information. When data is intercepted by an attacker, encryption prevents that data from being deciphered. There are two ways of Encryption: 1) Hop by Hop Encryption Provides cipher text conversion on each node to make it more secure for network layer. 2) End to End Encryption in which encryption-decryption performed at sender-receiver end only. According to the business needs, one can choose different encryption methods. Using more secure key exchange and key management schemes one can prevent attacks on IOT such as eavesdropping, fabrication, record and replay etc [10].

3.3.4 Cloud Computing

Cloud is a name for huge data storage capacity, high performance with affordable low cost. In the essential working of IOT i.e. large number of sensor nodes that collect and analyze huge amount of data, storing and processing of data where cloud computing can be used very effectively. Another use of cloud computing is providing third party security. IOT security can be enhanced using cloud's security at minimum cost, as cloud provides the feature of 'pay for how much you use'. While using cloud computing it needs to make sure that the 'Scale' of IOT is large for example in areas such as, earthquake monitor, smart grid, industrial applications etc. [11].

A summarized view of the working and security of IOT in Table 1 is given, and discussed about individual layer, components involved in the layer, working of each layer with its security issues and countermeasures.

4. CONCLUSION

In this paper, a summarized view of IOT including its architecture has been presented. IOT is an upcoming technology of innovation but still at its early stage of research and development. IOT cannot be used widely if it is not safe.

Therefore, the paper has discussed security issues of IOT and some countermeasure for required security parameters.

Even though in recent years, an active research on IOT is going on, but still some issues can be further focused on: 1) Use and evaluation of Wi-Fi, Ethernet, Bluetooth for networking of IOT or ZigBee protocol; 2) Application oriented study is needed for different industrial application in which IOT can be used in order to initiate a new technological revolution; 3) New security challenges and application of lightweight cryptographic protocol need to be studied further.

Table 1: Summary of IOT layers and its specifications

IOT Layer	Components	Working Of Layer	Security Issues	Security Parameters	Countermeasures
Perception layer	Smart Card, RFID tag, Sensors	Collection of information	Terminal Security issue Sensor network security issue	Authentication Confidentiality	Certification and access control Authentication Mechanism
Network layer	Wireless or wired network, computer, components	Transmission Of information	Information transmission security	Integrity Availability Confidentiality	Hop by Hop Data encryption
Application layer	Intelligent devices	Analysis Of information. Control decision making	Information processing safety of IOT	Privacy	End to end encryption

5. REFERENCES

[1] Conner, Margery (May 27 2010). Sensors empower the "Internet of Things" pp. 32–38. ISSN 0012-7515

[2] Shao Xiwen "Study on Security Issue of Internet of Things based on RFID" 2012 Fourth International Conference on Computational and Information Sciences

[3] http://whatis.techtarget.com/definition/Internet-of-Things

[4] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nano systems, in: co-operation with the working group RFID of the ETP EPOSS. Internet of Things in 2020, roadmap for the future, version 1.1, 27 May 2008.

[5] Xu Xiaohui ‘’ Study on Security Problems and Key Technologies of The Internet of Things", 2013 International Conference on Computational and Information Sciences

[6] Yan L, Zhang Y, Yang L T. The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems. Auerbach Publications, 2008.

[7] Atzori Luigi, Iera Antonio, Morabito, "The Internet of Things: A survey " Computer Networks, v54, n15, October 2010, pp.2787-2805.

[8] Xiong Li, Zhou Xuan, Liu Wen "Research on the Architecture of Trusted Security System Based on the Internet of Things" 2011 Fourth International Conference on Intelligent Computation Technology and Automation

[9] Benjamin Khoo "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy" 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing

[10] Rolf H. Weber "Internet of Things – New security and privacy challenges" computer law & security review 26(2010) 23 – 30

[11] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010. ISBN: 978-1-4419-1673-0.

[12] N. Gershenfeld, R. Krikorian, D. Cohen, The internet of things, Scientific American 291 (4) (2004) 76–81

[13] Abdemalek Amine, Otmane Ait Mohamed, Boualem Benatellah "Network Security Technologies: Design and Applications"

[14] SHEN changxiang, ZHANG Huanguo and FENG Dengguo, "Literature Review of Information Security" Science in China (Series E: Information Sciences), vol.37, no.2, 2007, pp.129-150

[15] WU chuankun, "A Preliminary Investigation on the Security Architecture of the Internet of Things," Bulletin of Chinese Academy of Sciences, vol 25, no. 4, 2010, pp 411-419.

[16] Anne James and Joshua Cooper, "Database Architecture for the Internet of Things," IETE Technical Review, vol.26, 2009, pp.311-312.