ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
*Published By:* **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
June 2017,
Vol. 10, No. (2):
Pgs. 454-459

# A Review on IoT Security Issues and Countermeasures

**J. YASHASWINI**

DoS in Computer Science, PG wing of SBRR Mahajana First Grade College,
K.R.S. Road, Metagalli, Mysuru, Karnataka, India-570016
Corresponding author Email: yashuj.krn@gmail.com

http://dx.doi.org/10.13005/ojcst/10.02.28

(Received: May 08, 2017; Accepted: May 17, 2017)

**ABSTRACT**

Internet of things (IoT) is a system of connected physical objects that are accessible through an internet. The things in IoT is an object that assigned with an IP address and have the ability to collect and transfer the data over a network without manual intervention. 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. The quick development of IOT has derived with the challenges in terms of security of things. This paper focus on the general security issues in IoT and measures used to overcome with those security issues.

**Keywords:** IoT, Security Issues, Security Measures.

## INTRODUCTION

Internet of things (IoT) that refers to uniquely identifiable objects, things, and their virtual representations in an internet-like structure, was first proposed in 1998[1]. IoT is a system in which all the things are connected to the internet through the information capturing devices for the purpose of intelligent identification and management[2]. These devices are provided with the unique identifiers such as an IP address or some different IDs, which can be read using RFID tags with the help of sensors (information sensing devices). The word things in IoT are an object that assigned with an IP address. It has the ability to collect and transfer the data over a network without manual intervention[3]. The IoT is a combination of wireless technology, micro electro mechanical system and an internet[2]. Basic thing needed to sense the objects in an IoT environment is by using sensors and/or RFID. Sensing can be easily achieved by assigning a unique identifier for each object and then connecting to an internet for smart information processing and transfer. The use of IPv6 can enhance the development of IoT applications, because of its huge address space any object in the world can have unique IP address using which the 'things' can communicate and transfer the information over network. Recent years the IoT is more popular because of its applications like, Intelligent Transport

System, Smart Electronic Meter Reading etc. the components IoT includes sensing, heterogeneous access, information processing, applications and services, and also needs additional components for security and privacy. The IoT will be faced with more severe security challenges. There are the following reasons: 1) the IoT extends the 'internet' through the traditional internet, mobile network and sensor network and so on, 2) every 'thing' will be connected to the 'internet' 3) these 'things' will communicate with each other. Therefore, the new security and privacy problems will arise. The main objective of this paper is to address the security issues of IoT and its countermeasures. This paper also gives a brief idea of IoT and its architecture, security issues at its each layer and countermeasures.

**IoT Architecture**

The IoT architecture mainly consists of four layers namely Perception layer, Network layer, Support layer and Application layer [4]. All of these layers have a large scale of information and support technologies as shown in figure 1.

**Perception Layer**

Perception layer is also called as recognition layer. The main working of IoT i.e., the information collection is done at this layer with the help of physical devices like RFID, Smart cards, Sensors, GPS devices etc. the information may be an object properties, environmental conditions etc. The key component of this layer is sensors for sensing and representing the physical world information in to the digital network world.

**Network Layer**

Next layer after perception layer is network layer, which is responsible for transmitting the information gathered at the perception layer to an internet. It includes the functionalities of

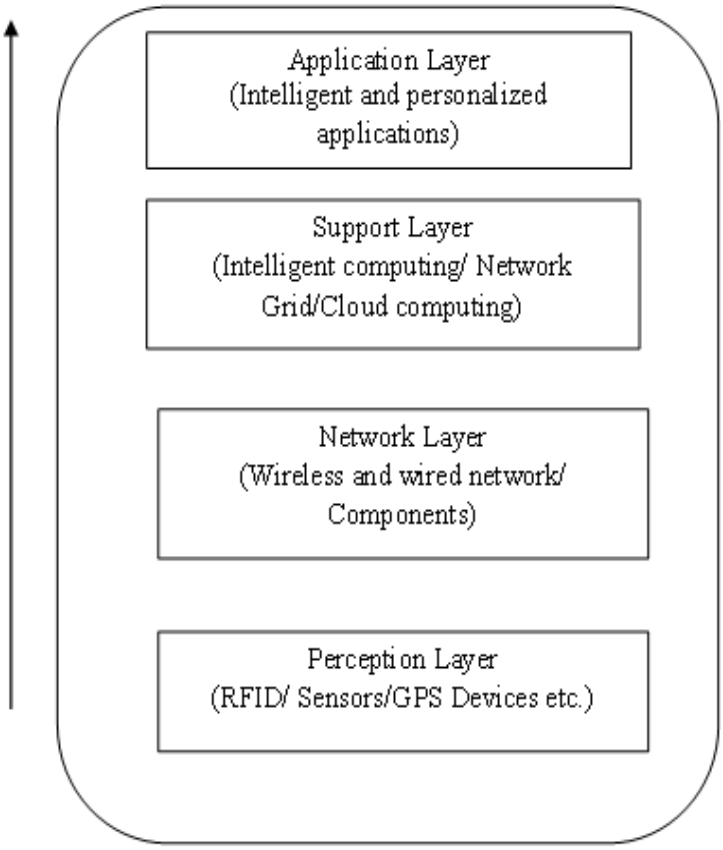


**Fig. 1: IoT Architecture**

the transport layer. The reliable transmission of information is depending on the basic networks such as internet, mobile communication network, and network infrastructure. Also communication protocols are required for information transmission between the devices.

**Support Layer**

Third layer is support layer, which provides a support upward for application layer and downward for network layer. This layer setup a support system for application layer, where all types of intelligent computing system are organized through a network grid and cloud computing.

**Application layer**

The application layer is the terminal layer of IoT, where it provides the services to users according to the need of user. Users can access the IoT applications through this layer using Personal computers, mobile devices etc.

**Security of IoT**

There are many papers that had addressed the Security issues of IoT[2,5,6]. This includes preserving the secrecy of information collection, securing the reliable data transmission, preserving the security of applications etc.

**Security Issues**

As the popularity of IoT application increased, it needs a protection against all possible types of attack and vulnerabilities. Therefore security is needed at each layer. The classification of security issues at each layer of IoT is given below.

**Perception layer**

Perception layer consists of physical devices like sensors, smart cards, RFID tags, etc. and these devices are used to capture the information. Computational powers of these devices are very less; therefore it is difficult to apply any security measures for protection system. Perception layer devices are more vulnerable to the attacks like sensor attacks, sensor abnormalities[7].

Terminal security issues[5] are defined at perception layer, where large number of terminals is used for real time data collections to be presented to the user. This process needs an authentication and integrity of data. Due to the wireless mode communication, IoT can also face threat from external network, hackers, virus etc. The main issue at perception terminals or devices includes loss of confidential information, terminal virus and other issues.

Sensor Network Security issues[5] - sensor nodes are responsible for data transmission, organization, integration and acquisition. As sensor nodes operate on their own battery with less security protection, they face complex security issues as includes invoking a malicious code such as worm that affects the wireless sensor network. It is also difficult to identify the malicious code. Fabrication is also a major issue at the perception layer. Fabrication is nothing but acting as legal reader to illegally use an RFID tags or sensor nodes.

**Network layer**

Network layer includes computers, wireless and wired network to transmit the information, which faces a security issues like illegal authorization, men in middle attack etc. Mean while the junk files and virus cannot be ignored because they cause network congestion. The main security issue at network layer is data transmission security issues[5]. The goal of network layer is to transmit the data securely. The security of network layer depends on security risk of IoT and the technologies, protocols required for data transmission. Nodes in the wireless network are free to move anywhere and also can leave the network at anytime. Because of this the network layer is vulnerable for malicious attacks.

**Support Layer**

This layer focuses on the large data processing and also makes an intelligent decision of network behavior. This processing should be limited to malicious information. But the security issue at this layer is the ability to identify the malicious information.

**Application Layer**

The Security needs of different applications will be different. The data sharing between the different techniques and business needs an integration of different application areas. This is a

bottleneck for processing of massive data and an operation control[8] and it also leads to security issues of safety and reliability for IoT.

IoT will also includes the security issues like privacy protection, data access control, protection of electronic products, leakage of information tracking and intellectual property of software[9].

**Security Parameters**

According to the above analysis, there is a need of security required for IoT System. Therefore looking at the traditional security parameters demands to build a secure and safe system of Internet of Things, are listed as follows.

- Privacy: Privacy of user identity or interest should be preserved by secure IoT System.
- Availability: IoT System should prevent the attacks like Denial of Service (DoS) and DDoS attacks by providing services to the authorized users.
- Integrity: Data integrity should be given by a secure IoT System. That is the system has to avoid the fabrication of information while transmission. Fabrication is nothing but rewriting, illegally coping or replacing original information by an attacker.
- Confidentiality: At any point in IoT system the sensitive information should be revealed to an unauthorized person.
- Authenticity: The received information or service by users should be checked for its source to confirm about it has transmitted from an authenticated device of an IoT system.

**Countermeasures for Security Issues of IoT**

There are some countermeasures available; using which the security issues of IoT can be reduced[5]. Those includes access control, data encryption, cloud computing and certification, communication security etc, discussed as below.

**Data Encryption Mechanism**

Encryption is the process of converting plaintext in to an unintelligible form known as cipher text. The network layer of IoT adopts hop-by-hop encryption mechanism to secure the nodes at network layer. This way the information is encrypted in transmission process, besides it needs to keep plaintext in each node through a encryption and decryption process.

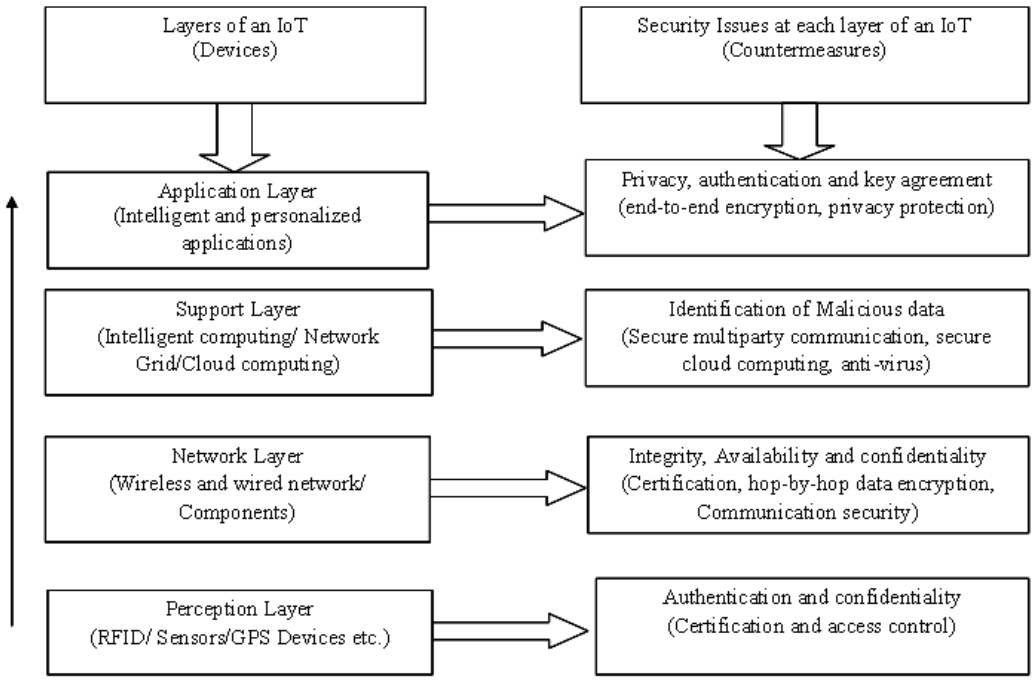


**Fig. 2: Summary of IoT Layers, Devices, Security Issues and Countermeasures**

While the application layer of IoT adopts end-to-end encryption mechanism to securely transmit the information between the sender and the receiver. According to the needs of business one can choose any encryption mechanism. Additional to this with secure key management and secure key exchange one can prevent attacks like eavesdropping, fabrication record, etc on IoT[10].

**Certification and Access control**

Using public key infrastructure (PKI) one can achieve authentication by public key certification for preserving the authenticity and confidentiality of an IoT system. It is also a secure way of finding the identity of the parties who involved in information transfer. The identification of parties can also be done through trusted third party known as notarization[11]. Access control will give a secure IoT environment by limiting the access for devices, things or a person's which are illegal to access the resources of an IoT system. For correct access control an IoT system should provide secure certification system.

**Cloud Computing**

Cloud is name given to store a huge data. The performance of cloud is high with low cost. The IoT can adopt cloud computing for data storing, processing the data, which has been collected from the many sensor nodes. It also provides the third party security to an IoT system[12].

**Security of Communication in IoT**

IoT consists of smaller devices with less power, this leads that communication security is week in IoT system. We need a very strong, secure communication protocol that provides a security to communication.

The Figure 2 summarizes the kind of device, security issues and countermeasures for those issues at each layer of an IoT.

## CONCLUSION

This paper is focused on summarized view of IoT system includes the architecture, security issues, countermeasures. IoT is an emerging technology with wide verity of applications. Using the IoT one can connect the many things through an internet. Therefore the privacy and also other security issues concerned. The paper has discussed the security issues of IoT and required countermeasures for those security features

## REFERENCES


1. R. H. Weber, "Internet of things – new security and privacy challenges," Computer Law & Security Review, vol. 26, pp. 23-30, 2010.
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. G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, "Security characteristic and technology in the internet of things," Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010.
5. Xu Xiaohui „ Study on Security Problems and Key Technologies of The Internet of Things", 2013 International Conference on Computational and Information Sciences
6. 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.
7. 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 .
8. N.Gershefeld, R. Krikorian, D.Cohen, "the internet of things", Scientific American 291(4)(2004) 76-81.
9. Anne James and Joshua Cooper, "Database

Architecture for the Internet of Things," IETE Technical review, vol.26, 2009, pp.311-312.

10. Rolf H. Weber "Internet of Things – New security and privacy challenges" computer law & security review 26(2010) 23 – 30 .
11. Abdemalek Amine, Otmane Ait Mohamed, Boualem Benatellah "Network Security Technologies: Design and Applications"
12. D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), "The Internet of Things", Springer, 2010. ISBN: 978-1-4419-1673-0.
13. Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, "Security in the Internet of Things: A Review," International Conference on Computer Science and Electronics Engineering 2012, IEEE Computer Society.
14. Mayuri A. Bhabad, Sudhir T. Bagade, "Internet of Things: Architecture, Security Issues and Countermeasures," International Journal of Computer Applications (0975 – 8887) Volume 125 – No.14, September 2015.