Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 41 (2016) 214-221 EISSN 2392-2192

# IOT Security Challenges and Issues – An Overview

**M. Sujithra**[1], **G. Padmavathi**[2]

Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India

[1,2]E-mail address: sujisrinithi@gmail.com , ganapathi.padmavathi@gmail.com

## ABSTRACT

A direct interpretation of the term Internet of Things refersto the use of standard Internet protocols for the human-to-thing or thing-to-thing communication in embedded networks. Certainly, the IoT security is more than a technicalproblem as it needs series of regulations and faultless securitysystem for common purposes. So, the study of IoT security problem is an emergent issue to be introduced in a research paper. There are many problems in security of Internet of Things (IOT) crying out for solutions, such as RFID tag security, wireless security, network transmission security, privacy protection and information processing security. This article is based on the existing researches of network security technology. And it provides a new approach for researchers in certain IOT application and design, through analyzing and summarizing the security of IOT from various angles. In this paper, the traditional techniques are studied and evaluated, which protect the IoT resources such as devices and data against hacking and stealing.

***Keywords*****:** Internet of Things, RFID, Security, Privacy protection, Network transmission

## 1. INTRODUCTION

The Internet of Things (IoT) denotes the interconnection of highly heterogeneousnet worked entities and networks following a number of communication patternssuch as: human-to-human (H2H), human-to-thing (H2T), thing-to-thing (T2T), or thing-to-things (T2Ts). Internet of things (IoT) refers to objects (things), which areuniquely identified and using the

( Received 01 February 2016; Accepted 10 February 2016; Date of Publication 11 February 2016 )

internet structure. IoT has four major features which are states as follows: sensing, information processing, heterogeneous access, services, and additional features like security and privacy. Recently, the IoT term may be called in other countries as machineto-machine communications or cyber-physical systems. The architecture of IoT contains a most important datacommunication tools, which is called Radio Frequency Identification (RFID) in addition to some complexcomputational items. Another definition of IoT is demonstrated and can be stated as follows; a universalnetwork infrastructure, communicate different types ofobjects through the utilization of sensing data andcommunication capabilities. Existing Internet and networktools are embedded in this infrastructure. It will offer specific object identification, sensor, actuator and connection capability as the basis for the development ofindependent federated services and applications.

Regarding the security issue, several challenges obstacle the progress of IoT applications due to the following reasons extension of IoT to collect recent technologiessuch as sensor network and mobile network, the internetwill comprise the passive and active things, and communicate these things is a must. Upon these natures of IoT, new security problems will arise. More attention to the research for IoT authenticity, confidentiality, and dataintegrity of data should be considered.

## 2. RELATED WORKS

Xiong Li, et al. proposed in a study of trusted security architecture for IoT. The weak points of this system can bestated as follows; 1) it concerned with a human being, which is not an important factor. The most important factors are IoT data and devices, 2) it demonstrated oldsecurity techniques and algorithms, which are not suitable for IoT, and didn't show an innovative idea, 3) thealgorithms and the techniques, which are demonstrated ineach system layer, are too large to be executed in the IoT systems. This is due to limited power machines such assensors and RFID that are considered as the skeleton of IoT systems, 4) in the trusted terminal module; the mainrequirement is secure operating system. This requirementis not accurate because most of current operating systemsare not completely secured, 5) this architecture contains 4types of agents, which are not identified in details. Inaddition, how these agents will communicate with eachother to accomplish this architecture target is not proposed.

Arijit U. et al. proposed in a trail to build security system for IoT. This trail demonstrated threats andproblems of low security IoT devices. The systemdiscusses some tools, which may be stolen. These tools canbe observed using monitor cars or cameras. This solutioncan be considered as traditional and did not in line with the nature of IoT because the devices, which are used in themonitoring such as camera, may be hacked or stolen.

Kiang Z. et al. proposed in security architecture for the IoT based on multimedia traffic. This trial idea is concerned with the multimedia traffic which is transmitted over IoT. So, it can be considered as a special purposesolution as it can be applicable only for multimedia. Inaddition, it is based on old and traditional techniques. Furthermore, it's under discussion and not implemented orevaluated so far.

Gang. et al. proposed in a general analysis for IoT security problem. It discusses somegeneral features such as identifying and controlling ofsensors remotely. Furthermore, it makes a defense againstthe Denial of Service (DOS) attacks to sensor nodes.

Hui S. et al. proposed in authentication and access control techniques for IoT systems. This trial focused on simpleand efficient elliptic curve cryptosystem secure key. Inaddition, role-based access control authorization method isadapted based on thing's applications and roles with respect to IoT nature. This authentication system has threedrawbacks; 1) it based on old security algorithms, 2) itdeals with only system users and not system data ordevices, 3) it is considered as a special purpose technique.

## 3. SECURITY ASPECTS

The term security subsumes a wide range of different concepts. In the first place, it refers to the basic provision of security services including confidentiality, authentication, integrity, authorization, non-repudiation, and availability. Thesesecurity services can be implemented by means of different cryptographic mechanisms, such as block ciphers, hash functions, or signature algorithms. For eachof these mechanisms, a solid key management infrastructure is fundamental tohandling the required cryptographic keys.

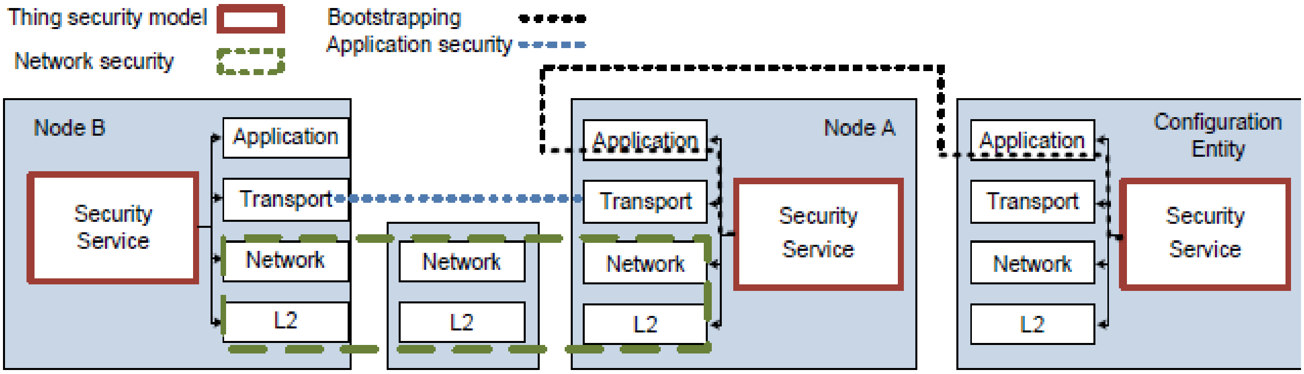

**Figure 1.** Overview of Security Mechanism

In the context of the IoT, however, security must not only focus on the required security services, but also on how these are realized in the overall systemand how the security functionalities are executed. To this end, we use the following terminology to analyze and classify security aspects in the IoT:

- The security architecture refers to the system elements involved in the management of the security relationships between things and the way these security interactions are handled (e.g., centralized or distributed) during thelifecycle of a thing
- The security model of a node describes how the security parameters, processes, and applications are managed in a thing. This includes aspects suchas process separation, secure storage of keying materials, etc.
- Security bootstrapping denotes the process by which a thing securely joins the IoT at a given location and point in time. Bootstrapping includes theauthentication and authorization of a device as well as the transfer of securityparameters allowing for trusted operation.

- Network security describes the mechanisms applied within a network to ensure trusted operation of the IoT. Specifically, it prevents attackers from endangering or modifying the expected operation of networked things. Networksecurity can include a number of mechanisms ranging from secure routingto data link layer and network layer security.
- Application security guarantees that only trusted instances of an application running in the IoT can communicate with each other, while illegitimateinstances cannot interfere.

## 4. IOT ARCHITECTURE

The proposed IoT security architecture can be extractedand clarified from above IoT architecture. So, this IoT architecture is adapted to be in concordance with thesecurity issue. The IoT security architecture consists of sixlayers; the security application layer, the application layer, the security network layer, the network layer, the securityperception layer, and the perception layer, seen in Fig. 2.

### 4. 1. Security of application layer

This layer is divided into two sub-layers. The first sub layers related to a local application security system. For example, intelligent transportation system may use encryption on the other hand smart home system may use steganography. The second sub-layer is related to national application security system. As stated above, the national application is concerned with management of local ones. Hence, the national application should be well secured. So, its security system should comprise more than one security technique to make sure that sent and received data are secure.

Accordingly, there are many security techniques, which may be applied in these types of applications such as selective disclosure, authentication, authorization, intrusion detection, firewall, and antivirus. In this issue, the most important recommendation is the used security techniques in the national application should not conflict with applied security techniques in the local applications.

### 4. 2. Security of network layer

Also, this security layer consists of two main sub-layers; wireless and wired. The wireless security sub-layer isconcerned with equipment, which communicate IoT applications using wireless channels such as wirelessinternet, mobile network, and cellular networks. Thesecurity techniques, which should be applied in this type ofnetworks, are key distribution, intrusion detectionalgorithms, identity based authentication, aggregated proofs, and anti-jamming. The wired security sub-layeris related to instrumentations, which communicate the IoT system objects using wired channels.

The securitytechniques, which should be used in this type of networks, are firewalls, router control, resource multiplication, routing flirting, and congestion control. This securitylayer is an extremely important since it responsible to transmit information among IoT systems’ components. Inaddition, it can be considered as a central unite to storecritical information. So, the sensitivity in selection ofsuitable security technique for each IoT element is target and challenge.

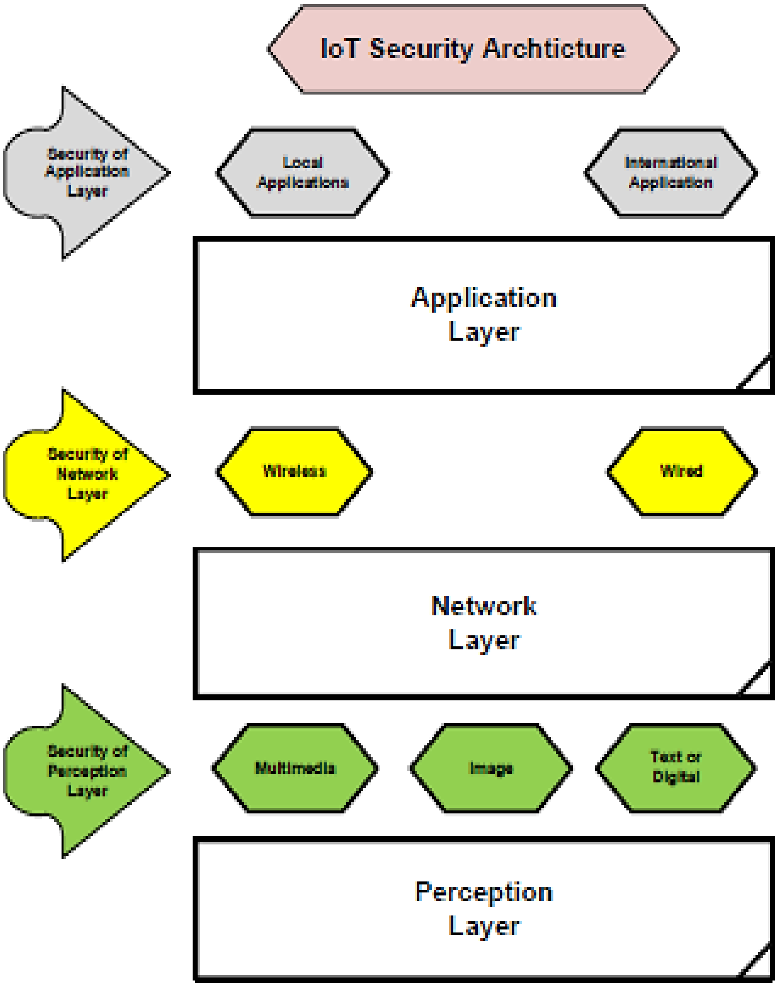

**Figure 2.** IOT Security Architecture

### 4. 3. Security of perception layer

The perception security layer consists of three sub-layers, which are classified depending on the gathered data. So, the first sub-layer, which is called multimedia, can use security techniques such as multimedia compression, encryption, time stamps, time synchronization, and multimedia session identifier. The second sub-layer, which is called image, can use image compression, and cyclic redundancy checks.

The third sub-layer, whichis called text information, can use encryption, compression, and anti-jamming. Since, the perceptionlayer contains tools, which are used to acquire data from atarget area, the traditional and straightforward securitysolution is to put a camera beside IoT perception layer tools. But, the more advanced solution is to make eachcamera sensor covers other objects beside its original function in the IoT system. Furthermore, there is a trackingsystem for stolen things should be developed.

## 5. CHALLENGES FOR SECURE IOT

The challenges in theoperational and technical features of the IoT are discussed as follows.

### a) Constraints and heterogeneous communication

Coupling resource constrained networks and the powerful Internet is a challengebecause the resulting heterogeneity of both networks complicates protocol designand system operation. In the following we brief discuss the resource constraints of IoT devices and the consequences for the use of Internet Protocols in the IoT domain.

### b) Bootstrapping of a Security Domain

Creating a security domain from a set of previously unassociated IoT devices is another important operation in the lifecycle of a thing and in the IoT network. Bootstrapping refers to the process by which a device is associated to another one, to a network, or to a system. The way it is performed depends upon the architecture: centralized or distributed.

In a distributed approach, a Diffe-Hellman type of handshake can allow twopeers to agree on a common secret. In general, IKEv2, HIP, TLS, DTLS, canper form key exchanges and the setup of security associations without online connections to a trust center. If not considered the resource limitations of things, certificates and certificate chains can be employed to securely communicate capabilities in such a decentralized scenario (e.g., for IKEv2, TLS, and DTLS). HIP and Diet HIP do not directly use certificates for identifying a host, howevercertificate handling capabilities exist for HIP and the same protocol logic couldbe used for Diet HIP. It is noteworthy, that Diet HIP does not require a thingto implement cryptographic hashes. Hence, some lightweight implementationsof Diet HIP might not be able to verify certificates unless a hash function isimplemented by the thing.

### c) Privacy Protection

Information privacy is directly reflects for confidentiality of IOT information. Location information of perception terminal is an important information resource of things, and also is one of the sensitive information need to be protected. In addition, there are also privacy issues in data processing, such as behavior analysis based on data mining.

## 6. CONCLUSION

With the overall development of IOT, a variety of different wireless communication technologies and network structure are aggregating, and the communication network environment has become increasingly complex, the basic network security issues carried by all kinds of business are more complex and difficult to solve. IOT safety is huge system engineering, network security system is established after the communication system architecture, and a variety of complex heterogeneous communication system may have impact on the overall security issues due to its characteristics.IOT makes the interoperability between virtual world and the physical world not only related to information security, interoperability, but also includes important social functions, intellectual property protection, privacy on important national basic industries and social key services. If these security issues are not addressed, there will be a big risk on the application of IOT. Therefore, IOT security issues is bound to rise to the national level, and it is great significant to promote IOT security.

## 7. FUTURE WORK

More security techniques should be tested in each layer ofthe proposed architecture to test compatibility. So, in thefuture, the techniques such as authorization, authentication, and time synchronization will be tested. Also, thesimulation environment should be larger (as possible) toprovide more accurate results.

## References

[1] Yinghui H., Guanyu L., Descriptive Models for Internet ofThings. *IEEE International Conference on Intelligent Controland Information Processing*, Pages: 483-486, Dalian, China, 2010

[2] Luigi Atzori, Antonio Iera, Giacomo Morabito, The Internet of Things: A survey. *Computer Networks*, Volume 54, Issue 15, 2010, Pages 2787-2805, https://doi.org/10.1016/j.comnet.2010.05.010

[3] Yuxi Liu, Guohui Zhou, Key Technologies andApplications of Internet of Things, *IEEE Fifth International Conference on Intelligent Computation Technology and Automation*, Hunan China, Pages: 197-200, 2012

[4] Huansheng N., Ziou Wang, Future Internet of ThingsArchitecture: Like Mankind Neural System or Social Organization Framework, *IEEE Communication Letters*, Vol. 15, No. 4, Pages: 461, 2011

[5] JunweiLv, 11, Xiaohu Yuan and Haiyan Li, A New ClockSynchronization Architecture of Network for Internet of Things, *International Conference on Information Science andTechnology*, Pages: 685-688, Jiangsu, China, March 26-28, 2011.

[6] Castro, M., Oxygen Cylinders ManagementArchitecture Based on Internet of Things, InternationalConference on computational science and its applications (ICCSA), Pages: 271-274, Murica, Spain, 2011.

[7] Miao W., Ting L., Fei L., ling S., Hui D., Research on thearchitecture of Internet of things. IEEE International Conferenceon Advanced Computer Theory and Engineering (ICACTE), Sichuan province, China, Pages: 484-487, 2010.

[8] Neil Bergmann, Peter J. Robinson, Server-Based Internetof Things Architecture, 9th Annual IEEE Consumer Communications and Networking Conference, Brisbane, Australia, Pages: 360-361, China, 2012

[9] Jing Liu and Yang Xiao, C. L. Philip Chen, Authentication and Access Control in the Internet of Things, *International Conference on Distributed Computing Systems Workshops*, Pages: 588 – 592, Tuscaloosa, AL, USA, 18-21 June, 2012

[10] Lan Li, Study on Security Architecture in the Internet of Things, *IEEE International Conference on Measurement, Information and Control* (MIC), Pages: 374-377, Harbin, China, 18-20 May, 2012

[11] Wei Jiang, LiminMeng, Design of Real Time Multimediaplatform and Protocol to the Internet of Thing, *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Pages: 1805-1810, Liverpool, United Kingdom, 25-27 June 2012

[12] Shao Xiwen, Study on Security Issue of Internet of Thingsbased on RFID, *IEEE International Conference on Computational and Information Sciences*, Pages: 566-569, Chongqing, China, 17-19 Aug. 2012

[13] Uckelmann, Dieter; Harrison, Mark; Michahelles, Florian, Architecting the Internet of Things, Springer, 2011. ISBN 978-3-642-19156-5

[14] Xiong Li, Zhou Xuan, Liu Wen, Research on the Architecture of Trusted Security System Based on the Internet of Things, *IEEE International Conference on Intelligent Computation Technology and Automation*, Pages: 1172-1175, Shenzhen, China, 28-29 March, 2011

[15] ArijitUkil, Jaydip Sen, SripadKoilakonda, EmbeddedSecurity for Internet of Things, *IEEE International Conferenceon Emerging Trends and Applications in Computer Science (NCETACS)*, Pages: 1-6, Kolkata, India, 4-5 March 2011

[16] Liang Zhou, Multimedia Traffic Security Architecture for the Internet of Things. *IEEE Network*, Volume 25, Issue 3, Pages: 35-40, 2011

[17] GAN Gang, LU Zeyong, Internet of Things SecurityAnalysis, *IEEE International Conference on Internet Technology and Applications (ITAP)*, Pages: 1-4, Chengdu, China, 2011

[18] HuiSuoa, Jiafu Wan, CaifengZoua, Jianqi Liu, Security in the Internet of Things: A Review, *International Conferenceon Computer Science and Electronics Engineering*, Pages: 648-651, Guangzhou, China, 2012

[19] Odrigo R., Cristina A., 2011. Key management systems forsensor networks in the context of the Internet of Things. Elsevier, *Computers and Electrical Engineering*, Volume 37, Issue 2, Pages 147–159

[20] Shen Bin, Liu Yuan, Wang Xiaoyi, Research on Data Mining Models for the Internet of Things. *International Conference on Image Analysis and Signal Processing* (IASP), Pages: 127-132, Zhejiang, China, 2010