ISSN 2348 – 9928
IJAICT Volume 4, Issue 9, September 2017 Doi:01.0401/ijaict.2014.08.13 Published on 05 (9) 2017

A NOVEL SURVEY ON INTERNET OF THINGS SECURITY AND ITS APPLICATION

Ms. R. Sujitha
Computer Science and Engineering,
SriGuru Institute of Technology,
Coimbatore, Tamilnadu, India

Mr. N. Vijaya Raghavan
Computer Science and Engineering,
SriGuru Institute of Technology,
Coimbatore, Tamilnadu, India

Ms. K. S. Suganya
Computer Science and Engineering,
SriGuru Institute of Technology,
Coimbatore, Tamilnadu, India

Prof. A. Devipriya
Computer Science and Engineering,
SriGuru Institute of Technology,
Coimbatore, Tamilnadu, India

Abstract— The Internet of Things (IoT),is a vision of connectivity for anything, at anytime and anywhere, which defines the interconnection of objects (or Things) for various purposes including identification of objects, communication, sensing, and data collection. Internet of Things (IoT) combines grid sensor technology, embedded computing, Internet services and wireless communication technology, distributed information handling technology. Hence, the revolution of the Internet of Things (IoT) has attracted highly attention of domestic, government, academia and industry, in which major issues are consider in IoT is security. Security of IoT systems are considered as the most important challenges facing than system developers. Certainly, the IoT security over a technical problem as it needs series of rules and flawless security system for common purposes. So, the study of IoT security is an overcoming the issue to be introduced in a study paper. Therefore, this study explores tier of security is maintained in each layer to the IoT and investigates related security application service technologies.

Keywords — IoT, Network Security, Sensors, Wireless Technologies.

I. INTRODUCTION

The Internet of Things (IoT) refers to interconnection of objects (things), which are identified uniquely and using the internet content structure. A vision of IoT is made connectivity for everything, at anytime and everyplace, which may have an intense effect on our day today lives are similar to connect with the internet in past 10–20 years. As per the rapid growth of development of grid sensor technology, embedded systems technology, wireless network communication technology, high-concert computing and other related fields are needs enormous amounts of data, [1][2] which all data have to be stored, processed and accessible in a continuous manner, efficient and easily interpretable manner. This model will consist of several services of application and security concerns are delivered Regarding the security issue, several challenges are stuck the IoT applications due to the following reasons; 1) To extension of IoT to collect recent technologies such as grid sensor network and mobile network, 2) the internet will contain both passive and active things of objects, and 3) communicate these things is an essential, and finally 4) apply security on each and every layer based on tier applications. Upon these floras of IoT, various security issues may arise. In which based on major consideration to the research for IoT are authenticity, confidentiality, and data integrity of data should be monitored. This paper proceeds as follows; in Section 2, a problem design is demonstrated. In Section 3, the IoT architecture and the proposed architecture IoT security are defined and discussed. In Section 4, IoT applications finally, the conclusion are introduced in Sections 5.

II. PROBLEM DESIGN

Scalability of IoT technologies considers security to be an attractive target for most academics [3], [4]. The security problems of IoT system technologies are grid sensor attacks, network content security, unauthorized login, and intrusions. In addition, IoT faces other security problems such as information tracking over the internet, secure electronic systems, and data integrity of things. The main challenge of the current study paper is to introduced new way of providing security in IoT technological services and find a general solution for these IoT security problems provided in applications

III. IoT ARCHITECTURE

The IoT consists of three main tiers; the application tier, the network tier, and the context-aware tier. Hence, this application tier should be divided into three different layers namely application layer, middle layer, and computer technology. Each layer consists of two sub layers. In application layer, the first sub-layers called local such as logistics analytics and

monitoring, which mean that it comprises local applications. These types of applications maintain various local domains in the IoT technological systems such as smart homes, smart metering, e-health, and e-learning. The second sub-layer is called national applications, which is applied in general function application that also manages the IoT local applications. See Fig. 1. The services of this sub-layer are administration, conversion, and national application management. They are various technologies are introduced in second sub-layer, such as cloud computing, grid computing, artificial intelligent as well as web application technologies. In Middle layer, [5][6] the first sub-layer consists of to manage various managements like information management, service management, user management and technical management. In final layer of intelligent computer technology provides two sub layers, first sub-layer contains SOA and second sub-layer is cloud computing. Regarding the network tier which contains network layers, it comprises the tools, which are used in communication of IoT hardware to software applications, such as sensors, mobiles, wireless technologies etc. Tools must be varied based on methodologies. The first sub-layer is wireless methodology, which contains tools such as wireless sensor networks (WSN) and mobile communication networks and wireless technologies like ZigBee, Wi-Fi etc.

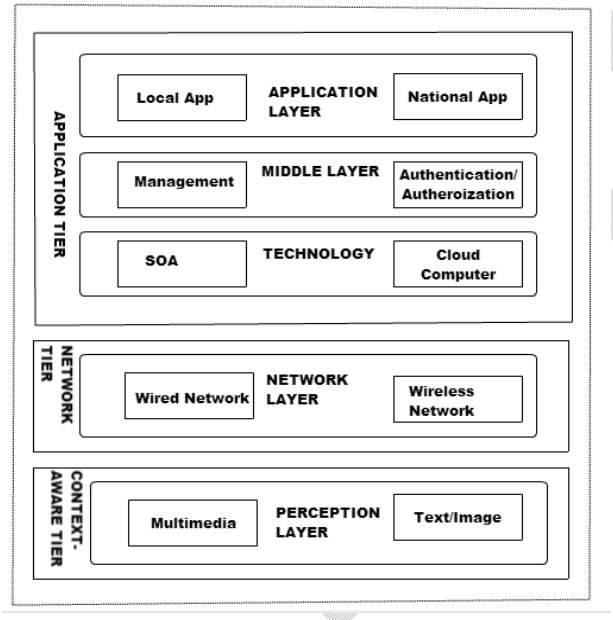

Fig 1: Proposed IoT Architecture

The second sub-layer is wired methodology, which contains tools such as routers and gateways. Reliable data transmissions, quality of services, and connectivity issues are related to this network layer are managed by management stations see Fig.1. For the perception layer under context-aware tier, it includes devices, which are used to collect data from a specified environment. The devices used in perception layers are sensors, RFID, Bluetooth and Wi-Fi. This layer can be classified into various layers depending on a type of data to be collected. Some tools may collect multimedia objects and others may collect images and texts as in Fig. 1.

IV. SECURITY OF IoT ARCHITECTURE

Security consider the major challenges in IoT, consequently the proposed IoT security architecture can be developed and discussed from above IoT architecture. So, this security IoT architecture is mainly concentrated in security field. in which improving security is [7] applied security at each tiers separately. The IoT security architecture consists of three tiers; the application tier security, the network tier security, and context-aware tier security, and providing various securities to tier, based on the capacity and services is called as coarse-grained security cell as in Fig. 2. In the following subsections are discussed, only three important layers in each tiers are clarified.

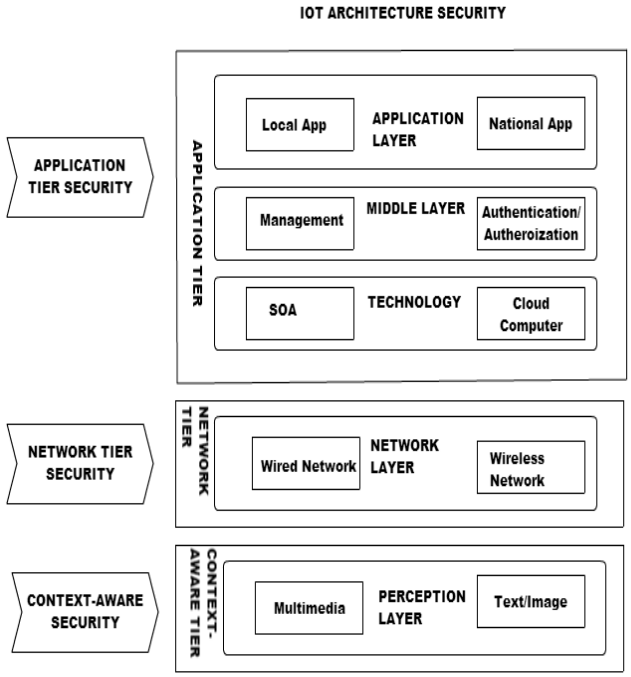

Fig 2 : Security of Proposed IoT Architecture

4.1 Security of Application Layer

This layer is contains two sub-layers. Provide security to local applications consider various techniques. For example, ITS may use encryption techniques and smart home system, smart metering may use stenganography techniques. The second sub-layer is related to national application security system. Hence provide high security to the national application in a secured manner. As stated above, the national application should be well secured. So, its security system should contain various security techniques is based on to make sure that sent and received data are secure. Accordingly, there are many security

techniques applied in this systems such as selective disclosure, authentication, authorization, access control list, intrusion detection, firewall, and antivirus.

4.2 Security of network layer

The security of network layer consists of two main sub-layers; wireless and wired. The wireless security sub-layer is concerned with methodologies, which communicate IoT applications using wireless medium such as wireless internet protocol, mobile network communications, and cellular networks communications. The security techniques are applied in wireless type networks are key distribution, pre-shared key, intrusion detection algorithms, identity based authentication, and role based identity. The wired security sub-layer is concerned with devices, which communicate the IoT system objects of things using wired channels medium. The security techniques are applied in wired type networks are firewalls and router device. This security layer is an extremely important because gives more in-charge to transmit information among IoT systems components.

V. SECURITY OF PERCEPTION LAYER

The perception security layer consists of two sub-layers, which are varied based on thedata collection. So, the first sub-layer, which is called multimedia, can use security techniques such as multimedia compression, stenography, water marking, encryption, time session and intellectual property. The second sub-layer is image, to use security in images as image compression, and CRC. Since, the perception layer contains tools, which are used to collect data from a targeted area and send that information to network layer using wireless technologies in a secured manner.

VI. APPLICATIONS OF IoT

There are numerous number of applications are used in the Internet of Things (IoT), which monitoring the sensing objects automatically based on applications. The number of applications is never-ending. Various application securities are discussed below based on importance of security.

6.1 Identity-Related Services

Identity-related services are one of the most simple and important application of the Internet of Things (IoT). The most important technology used in identity-related services is RFID. Which is the data read by an RFID reader and it is processed data to be transmitted by a tiny portable device, called a tag to RFID server. It is mainly used for device identification and barcode/QR scanning. RFID is does not require line of sight transmission, it may arise various risks like unauthorized access and modification of tags. The RFID tag stores an ID code is unique to that device, an unprotected tags may be vulnerable to eavesdropping, denial of service attacks, traffic analysis or spoofing. The RFID reader reads that unique ID code, and looks up the device in the RFID server. The hardware of RFID reader provide efficient techniques as cryptographic functions, random number generators, symmetric encryption, and message authentication codes will improve RFID security.

6.2 Information Aggregation Services

Information aggregation services is combined with the identity related services, along with other components of technologies such as WSNs, mobile communications, and access gateways to collect information of data and forward it to the application layer for processing the analytics. In WSN is powerful tool for collecting and communicating data between devices, the multiple WSN are linked using access gateway for security.

6.3 Collaborative-Aware Services

The information aggregation services and collaborative aware services is vary based on how the collected data to make decisions and perform actions. The collaborative aware service security services are vary based terminal device processing power. Terminals device is consist of sensor, which is ported into embedded devices within the network. In collaborative aware services provide security to terminal devices. Hence, collabora-tive-aware service is incorporates both terminal to terminal (T2T) and terminal to person (T2P) communication, which is ac-accomplished using standard IPv6 protocol.

VII. CONCLUSION

In this paper, the architecture of IoT is introduced. Based on this architecture, a new security model for IoT is proposed. The proposed architecture idea is based on providing accurate security mechanism for each IoT layer as tier. The proposed architecture apply the security in application tier which is divided the application layer into two security sub-layers, which are called local and national applications. The network tier of security is applied in each network layer in the IoT architecture is divided into two sub-layers, which are called wireless and wired. The perception layer is divided into two sub-layers, which are called multimedia, image, and text. To estimate the proposed security architecture is identified efficiency, scalability and cost; the energy consumption, the consumption of time, and the security accuracy and also applications are discussed based on security.

References

[1] Omar, Development of an Innovative Internet of Things SecuritySystem, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013

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

[3] Yuxi Liu, Guohui Zhou, Key Technologies and Applications 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 Things Architecture: Like Mankind Neural System or Social Organization Framework, IEEE Communication Letters, Vol. 15,

[5] Huansheng Ning, et al. "Cyberentity Security in the Internet of Things", IEEE computer, Volume:46 , Issue: 4,Pages: 46-53, 2013.

[6] Weizhe Zhang1, Baosheng Qu., Security Architecture of the Internet of Things Oriented to Perceptual Layer, International Journal on Computer, Consumer and Control (IJ3C), Vol. 2, No.2(2013)

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