IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.7, Special Issue.2, Jan 2019 E-ISSN: 2347-2693

A Literature Survey on Internet of Things security issues

V. Suganthi[1*], P.K. ManojKumar[2]

[1,2]Dept. of Information Technology& Computer Technology, Nehru Arts and Science College, Coimbatore, India

[*]*Corresponding Author: suganthi.grd@gmail.com Tel.: 9994154509*

Available online at: www.ijcseonline.org

***Abstract*—** In day-to-day life, IoT plays a major role . The functionality of IoT is deployed in hospitals, banking sector and also in homes. The work of IoT starts from preventing fires at homes and also supports for the changes in environment. Apart from those benefits, security and privacy is also considering factor. In terms of IoT, the devices connected may not be of the same type which includes type of devices, network used , protocols followed etc. When such variations occur, the security issues cannot be considered in general. Based on the type of device, the security concern has to be independent. An Analysis of various existing protocols and mechanisms are discussed to secure communications in IoT applications. In this paper, Survey of various heterogeneous devices connected to IoT and the security issues related to IoT applications are discussed. Such a survey will be helpful in identification of security issues for different types of IoT applications.

***Keywords*—**Internet of Things, Security, Privacy

I. INTRODUCTION

The Internet of Things is the model of connecting a device to the Internet and also to other devices. It is a connected network where people and things are connected. The information is shared between the environment and the devices.

IoT plays a major role which is used to connect everyday objects in life which are operational with microcontrollers and transceivers for digital communication [1]. A variety of devices for example home appliances, surveillance cameras, sensors that are used for monitoring interacts with IOT to facilitate easy and smart working. When there are varieties of devices connected to IOT, there comes the problem of heterogeneous. Heterogeneous is defined in IOT with connection to different types of networks, types of data that is gathered from different devices and the technology that is used for each device. Such a heterogeneous field of application makes the detection of solutions which is proficient of satisfying the necessities of all types of application becomes a challenging task.

IoT is a combination of many things that is involved in the world. It cannot act independently. Humans , computers and smart objects are combined together to form the cyberspace. Existing network systems are cloud computing, social and industrial networks, along with Internet and smart phones. The heterogeneous networks has evolved the concepts of CoT (Cloud of Things) ,WoT(Web of Things) and SIoT(Social Internet of Things)[2].

II. RELATED WORK

Many of the research works have been carried out to reduce the hazards that are related with the functions of *Physical* IoT. As per the survey conducted, there are four segments. The first one deals with the limitations of IoT devices , the second one classifies the attacks. The third segment has an insight into architectures for authentication and the fourth about the issues involved in the security of various layers[3].
IoT applications provide a lot of profit to the human's. At the same time, the prices are much huge. Customers are ready to pay a huge but there is a lack of security. IoT manufacturers less concentrate on the security system provided to the customer. The number of systems connected to the internet is high in number and also may cause a unsecured environment [4].As far as consumers are concerned, security and privacy are the major issues for IoT devices. Such devices apart from collecting personal data, it also monitors user activities. So when they use such devices, they care about their data and its security. They have to check before disclosing of personal data either in public or private cloud [5].

About 90% of tested devices collected from the recent survey conducted by HP says that at least one bit of information is stolen from the personal information. This may easily attacked through cyber-attack. This will lead to lack of security , confidentiality and integrity of the data. The users may lack confidence in securing the data.
According to 2020 conceptual framework, the term Internet of Things (IoT) is expressed as
IoT= Services+ Data+ Networks + Sensors [6].
The IoT four key technological enablers are: -

- For tagging the things RFID technology used
- For sensing the things sensor technology used
- For thinking the things smart technology used
- For shrinking the things Nanotechnology used [7]

The Basic architecture of IoT consists of 3 layers. They are

1. Application Layer- It consists of various applications and services.

2.Network Layer- It includes network communication software and physical components such as topologies, protocols and network nodes which are used in communication.

3.Perception Layer- It consists of different kinds of sensory technologies.

The IoT is a combination of heterogeneous networks which includes chip technology. The fast growth of internet applications such as agriculture, smart community, control and tracking systems. By the research analysis in 2020 IoT objects will be a part of human social life[8].

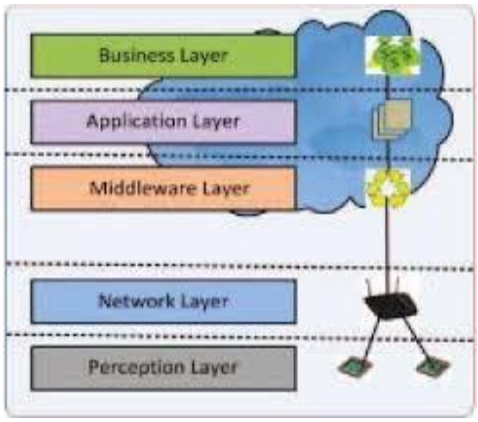

Figure 1.Layers of IoT architecture

The security is an essential part of the rapid development of IoT-based applications environment in the present era. The traditional IoT security architecture and standard of IoT is not enough for the user using different intelligent devices. The difference exists because of the heterogeneous devices. The objective of the paper is to come out with the solution to provide security features even though the devices are heterogeneous.

Many of the literature surveys have been conducted on IoT security. Classifications are done based on IoT attacks and solutions. A new classification of IoT devices attacks has been provided by Andrea et al.[9]. The IoT attacks which are presented in four distinct types as physical, network, software and encryption.

Each and every Layer has its own impact on security issues. Most of the time, the security may be forbidden because of the fact that it has some loop holes. Physical layer is attacked when the attacker is in a much closer distance. The network attack damages the networking part. Such attack happens in IoT.

The preventing measures can be implementing of hash and cryptographic algorithms at the physical layer, authentication mechanism at network layer. The application layer can provide the security in terms of authentication, encryption and verification of integrity where it allows only authenticated users to perform the transaction.

A pervasive authentication protocol and a key establishment scheme for the resource constrained wireless sensor networks (WSNs) in distributed IoT application, called Pauth Key was proposed and designed by Porambage et al. [10]. It consists of two phrases . one is registration phase and the other one is authentication phase. The end devices that are connected to IoT are registered in the registration phase and establishment of key and authentication is provided in the second phase.

Sharaf et al[18] proposed a approach which is new for the authentication process. The base used for the authentication was the unique finger print. The details such as location, physical state of object is stored using the unique finger print. When there is a group of IoT Objects , then there is a need of variety of fingerprinting techniques. For the application of this idea, a new approach called two-fold approach was proposed where the first phase adopted the Infinite Gaussian Mixture Mode(IGMM) as a generative model for base assumption of finger prints for each object. The second phase compares the clustering result with that of IGMM. The end result is expected to be cluster shape for the result.

Zhang et al[11] proposed an algorithm to secure against DDoS attacks . It consists of four nodes. They are working node, monitoring node legitimate user node, and the attacker node. The collection of information is performed by working nodes. They have enough memory computation, and for storage. The purpose of the working node is to differentiate the request between the cruel and genuine ones. A genuine user's request will be stored in the list and for the next time when the request arrives, the node can easily detect the user. This algorithm was useful for preventing DDoS attacks.

An authorization access control model called SmartOrBAC which is an extension of the basic model OrBAC (Organization Based Access Control) was proposed by Bouij et al. This work supports the network layer of IoT framework. IoT network framework was divided into four layers as constrained ,less constrained, organization layer and collaboration layer. Security domain features are enhanced along with the basic model of OrBAC. The central element of the less constrained layer is referred as Client Authorization Engine (CAE), on the client side, and Resource Authorization Engine (RAE), on the source side. It is more easy to use than capabilities based model and reduces the risk of errors.

III. CONCLUSION

In this survey Paper, architecture of IOT is discussed with different layers. The differences in the IoT architecture exist due to the heterogeneous devices connected to IoT. The security issues in IoT applications are discussed. The safety of devices which are commercially available in market today depends on the technologies, the protocols which are framed and the security mechanisms that are used for individual applications. But the mechanism differs from one device to the other. Based on the IoT attacks, some sort of techniques can be made general in nature for the IoT applications.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things" A survey, Comput. Netw, 2010 , vol. 54, no. 15, pp. 2787–2805.

[2] Ke Xu, Yi Qu, and Kun Yang. "A Tutorial on the Internet of Things:From a Heterogeneous Network Integration Perspective" IEEE network,March/April 2016.

[3] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li_, and Hongbin Zhao "A Survey on Security and Privacy Issues in Internet-of-Things"

[4] Margaret Rouse, "Iot security (internet of things security)," Internet of-Things-security, 2013.

[5] J. Granjal, E. Monteiro, and J. S. Silva, "A secure interconnection model for ipv6 enabled wireless sensor networks," in 2010 IFIP Wireless Days, Oct 2010, pp. 1–6

[6] L. Atzori, A. Iera, and G. Morabito, "Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm," Ad Hoc Networks, vol. 56, pp. 122-140, 2017.

[7] L. Srivastava and T. Kelly, "The internet of things," International Telecommunication Union, Tech. Rep, vol. 7, 2005.

[8] K. Zhao and L. Ge, "A survey on the internet of things security," in Computational Intelligence and Security (CIS), 2013 9th International Conference on, 2013, pp. 663-667.

[9] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in 2015 IEEE Symposium on Computers and Communication (ISCC), July 2015, pp. 180–187.

[10] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key Establishment scheme for wireless sensor networks in distributed iot applications," in International Journal of Distributed Sensor Networks, 2014.

[11] C. Zhang and R. Green, "Communication security in internet of thing: Preventive measure and avoid ddos attack over iot network," in Proceedings of the 18th Symposium on Communications & Networking, ser. CNS '15. San Diego, CA, USA: Society for Computer Simulation International, 2015, pp. 8–15.

Authors Profile

Dr. V.Suganthi is working as an Assistant Professor in Nehru Arts and Science College. She has 11 years of teaching experience. She has presented many papers in conference and published articles.

Mr.P.K.ManojKumar is working as Head of the Department, Department of IT & CT in Nehru Arts and Science College. He has 14 years of teaching experience. He has participated and organised many international conferences

