Internet of Things (IoT) Security Issues

Ranjana Sharma
College of Computing Sciences and IT,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India

ABSTRACT: ***Wireless communication networks are highly prone to security threats. The major applications of wireless communication networks are in military, business, healthcare, retail, and transportations. These systems use wired, cellular, or adhoc networks. Wireless sensor networks, actuator networks, and vehicular networks have received a great attention in society and industry. In recent years, the Internet of Things (IoT) has received considerable research attention. The IoT is considered as future of the internet. In future, IoT will play a vital role and will change our living styles, standards, as well as business models. The usage of IoT in different applications is expected to rise rapidly in the coming years. The IoT allows billions of devices, peoples, and services to connect with others and exchange information. Due to the increased usage of IoT devices, the IoT networks are prone to various security attacks. The deployment of efficient security and privacy protocols in IoT networks is extremely needed to ensure confidentiality, authentication, access control, and integrity, among others. In this paper, an extensive comprehensive study on security and privacy issues in IoT networks is provided***.

KEYWORDS: ***Application Layer, Confidentiality, Network Layer, Perception Layer, Security Issues.***

INTRODUCTION

The security issues of the Internet of Things (IoT) are directly related to the wide application of its system. Beginning with introducing the architecture and features of IoT security, this paper expounds several security issues of IoT that exist in the three-layer system structure, and comes up with solutions to the issues above coupled with key technologies involved. Among these safety measures concerned, the ones about perception layer are particularly elaborated, including key management and algorithm, security routing protocol, data fusion technology, as well as authentication and access control, etc. The information from IoT devices is further processed in the centralized system and delivered to the intended destinations.

With the rapid growth of communication and internet technology, our daily routines are more concentrated on a fictional space of virtual world. The Internet of Things (IoT) is a multitude of connected objects, services, people and devices which can be related to connect, exchange and receive information popular in numerous applications and fields. IoT has a lot of transport, fisheries, deployment domains, healthcare, generation and delivery of electricity. IoT appliances following an approach to identity security to be established related and heterogeneous appliances set. Likewise, in an IoT area, an IP address may be set but each is specified[1]. Each territory has a single entity. IoT seeks to change our current way of life, make smart devices around us perform routine tasks and chores. Intelligent houses, intelligent communities, intelligent transport and the words used in related networks etc[2].

There are several IoT domain areas personal and company worlds The application enables IoT users to engage in personal and social realms for their environments and individual consumers keep mutual ties and construct them[3]. A different application of IoT is in the field of travel, of which many intelligent vehicles, the aim of intelligent roads and intelligent signals is to safeguard and easy services for travel. The businesses and the domain of industries contains financial applications, banking, promotions, etc., to promote multiple organizational interactivities[4]. The last area of operation is the service and utility control industry. Agriculture, breeding, conservation of resources, recycling activities, etc. Recent advances in IoT implementations have been quick years attributable to radio frequency technology wireless Sensor Networks and Recognition (RFID) (WSN). The RFID makes it possible to tag or mark each person's device to act as the fundamental mechanism for recognition. Each "thing" (persons, computers etc.) because of WSN. It becomes a wireless entity to identify and interact in the real, digital and cyber world. The remaining document is arranged in this way. Division II the IoT structure and design defines three levels. In part III, the various security concerns principles of protection and nature are outlined in IoT devices. The section also covers the relevant security problems for every IoT layer. Chapter IV speaks about recent studies by others to comply with IoT security concerns counter measures. The big picture is given in Section V The work performed in IoT has been analyzed. The future in Section VI directions to take in view of established IoT status security. In Section VI the document is finalized.

DISCUSSION

IoT Security Issues:

Confidentiality, honesty and traditional security uses IoT is also covered by availability (CIA). Yet the IoT has many parts limitations and restrictions and supplies, computer and control and also the Heterogeneous and all-embracing existence of IoT further fears[5]. There are two sections to this section: The IoT must and the general security features relevant safety concerns for each IoT layer.

A. The Security Features of IoT:

IoT's safety challenges can be categorized into two classes; problems of technology and defence. The technical problems exist because of the omnipresent and heterogeneous essence of IoT devices the problems of defence are based on values and features to be incorporated to ensure a healthy network[6].

- All IoT computers should have apps running enabled.
- If an IoT system is triggered, it should first be activated before collecting, authenticate through the network or receiving data. Or sending data.
- The computing of IoT devices is constrained and firewalling memory capabilities are required in the IoT filter network for device-oriented packets.
- Device upgrades and fixes should be installed in a manner not offering extra bandwidth Eaten. The protection standards to be followed are the following forces to reach a stable system for contact tools, humans, systems, things[7].

1) Confidentiality: It is highly critical that the data is protected and stable and the approved users are open. An individual may be a person in IoT, machines and utilities, as well as internal artefacts (devices network components and external objects (devices not included) network part). Part. It is necessary, for example, to ensure that sensors do not disclose neighboring data collected from the knots[8].

2) Integrity: The IoT is focused on data sharing among several different groups phones, which is why the provision of the data accuracy; it comes from the proper sender and to ensure that the data was not distorted during transmission process for purposes or unforeseen purposes interference. The honesty attribute may be imposed on maintenance of IoT connectivity end-to-end security. The use of firewalls and protocols is the control of data flow, but the protection at endpoints is not assured because of the low processing power characteristic of IoT knots[9].

3) Availability: IoT's vision is to attach as many intelligent devices as possible it may. All data should be given to IoT users displayed whenever needed. Whenever needed. Yet data is not the only thing IoT component; devices and services are required to also be available as necessary in a timely manner to meet the IoT's needs[10].

4) Authentication: Each IoT object must be clearly recognizable and able to distinguish and check other objects for authentication. This method can nevertheless be quite efficient the existence of the IoT threatens multiple entities; participants (devices, individuals, facilities. Units of processing) and another issue is that objects also for the first time, may have to communicate with others (objects unfamiliar with). For all these purposes, a reciprocal function each IoT relationship involves authenticating entities.

5) Key Management Systems: The modules and IoT sensors must be substituted in IoT. Data confidentiality encryption products. A lightweight key management is required for this purpose system that enables trust between all frameworks various stuff and by using computers, you can spread keys minimum capacity.

B. Security Challenges in Each Layer of IoT:

The security breaches and attacks on any IoT-layer. These may be active or passive from which an intrusion from the external source or internal network insider. A successful attack stops the operation immediately when the IoT network information is tracked without passive sorting the barrier to its use. IoT equipment and facilities across any layer they are vulnerable to Service Denial (DoS) attacks the inaccessible computer, resource or network users. A thorough review of the following parts each layer has security problems.

1) Perception Layer: In the IoT experience layer, there are three protection problems. Initially wireless signals are the intensity. The signals are primarily wireless transmission between IoT sensor node technologies that can impact their performance waves. Secondly, IoT devices may use the sensor node not

only the owner but even the attackers are intercepted because in external and outside IoT nodes normally run environments, which lead to IoT sensors and physical assaults modules that can distort the hardware of an attacker appliance elements.

2) Network Layer: The network layer of IoT is as previously mentioned DoS-prone attacks are vulnerable. In comparison to the DoS threats, adversaries can also attack secrecy and confidentiality traffic, eavesdropping and passive network layer surveillance. These assaults are very likely remote control systems and data incidence system swap. The network layer is an incredibly vulnerable man-in-the-center assault, followed by an earthquake.

3) Application Layer: Because the IoT has no world policy and interaction and production standards there are many applications, many applications and security problems. There are various authentication programmes mechanisms that make all of them very interconnected data protection and verification of identification are difficult to ensure. Everyone has huge numbers of mobile devices triggering data exchange high overhead for data analysis systems that can have a huge effect on service availability.

CONCLUSION

The main emphasis of this paper was to highlight major security issues of IoT particularly, focusing the security attacks and their countermeasures. Due to lack of security mechanism in IoT devices, many IoT devices become soft targets and even this is not in the victim's knowledge of being infected. In this paper, the security requirements are discussed such as confidentiality, integrity, and authentication, etc. In this survey, twelve different types of attacks are categorized as low-level attacks, medium-level attacks, high-level attacks, and extremely high-level attacks along with their nature/behavior as well as suggested solutions to encounter these attacks are discussed. Considering the importance of security in IoT applications, it is really important to install security mechanism in IoT devices and communication networks. Moreover, to protect from any intruders or security threat, it is also recommended not to use default passwords for the devices and read the security requirements for the devices before using it for the first time. Disabling the features that are not used may decrease the chances of security attacks. Moreover, it is important to study different security protocols used in IoT devices and networks.

REFERENCES

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Computer Networks*. 2015, doi: 10.1016/j.comnet.2014.11.008.

[2] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*. 2017, doi: 10.1016/j.jnca.2017.04.002.

[3] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," 2012, doi: 10.1109/ICCSEE.2012.373.

[4] A. Lele, "Internet of things (IoT)," in *Smart Innovation, Systems and Technologies*, 2019.

[5] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Commun. Surv. Tutorials*, 2015, doi: 10.1109/COMST.2015.2388550.

[6] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet Things J.*, 2017, doi: 10.1109/JIOT.2017.2694844.

[7] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," 2015, doi: 10.1109/SERVICES.2015.12.

[8] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, 2015, doi: 10.1109/ACCESS.2015.2437951.

[9] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, 2015, doi: 10.1007/s10796-014-9492-7.

[10] K. Zhao and L. Ge, "A survey on the internet of things security," 2013, doi: 10.1109/CIS.2013.145.