A Study on Security Requirements of IoT

Amrita Prakashi[1], Ravi Kumar Singh Pippal[2]
[1]MTech Scholar, [2]Professor
[1]Department of Computer Science and Engineering, Vedica Institute of Technology, Bhopal, India
[2]Department of Computer Science and Engineering, Vedica Institute of Technology, Bhopal, India
amrita.bca@patnawomenscollege@gmail.com[1] ravesingh@gmail.com[2]

Abstract: In technology, Internet technologies have been faster than other technologies. However, the fast pace of the Internet has kept the Internet's full potential and, in the meantime, poses many threats to data security. The growing dimension of the Internet was IOT, which needed to connect devices and systems more than ever. The space that worried about the devices and systems interconnected in the biological system was the security of the Internet of Things. Although IOT plays an important role in society and technology, there are fundamental threats such as security and data protection. Things (in the processing devices of the IOT ecosystem and in the integrated systems) have been able to collect, send and receive data by communicating on the network because they have a unique identifier. This document is a summary document on the security aspects of IOT. He deals with security problems based on security architecture and protocol, RFID technologies, WSN integration and RFID technologies for security problems.

Keywords: IOT, RFID, challenge, protocol.

I. Introduction

The term Internet of Things (IoT), which refers to clearly identifiable objects, things and things in an Internet-like structure, was first proposed in 1998 [1]. In recent years, the IoT concept has become particularly popular thanks to some representative applications (for example, intelligent monitoring of greenhouses while reading electricity meters, monitoring of telemedicine and intelligent transport). Typically, the IoT has four main components- acquisition heterogeneous access information processing, applications and services as well as additional components such as data security and protection.

Nowadays, the IoT is widely known as a slogan. The following industrial applications related to IoT will emerge, for example cybernetic transport systems (CTS), cyber-physics systems (CPS) and machine-to-machine communication (M2M) [2].

In terms of security, IoT will face more serious problems Challenges. The reasons are as follows:

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 this ‘internet’, and
3) These ‘things’ will communicate with each other. Therefore, the new security and privacy problems will arise. We should pay more attention to the research issues for confidentiality, authenticity, and integrity of data in the IOT.

II. LITERATURE REVIEW

Jebah Jayakumar et al [3] proposed a strategy for a safe state in the IOT regarding RFID innovations [7]. In this article, they used RFID innovation for data security and protection. You are considering a situation using a safe state using IOT regarding RFID. To do this, they assign a unique item code (UPC) to each item. The Electronic Product Code (EPC) could replace the UPC in which MIT's automatic focus ID operates. Each glossy label would include an article manufacturer, an article name and a 40-bit serial number along with 96-bit data. A system called Object Naming Service was responsible for Scharfsinn's correspondence in this context. The item data will be restored from this database and immediately on the manufacturer's PCs. They proposed a "murder password" and an "access password" to ensure validation, classification of information and reliability of information at different levels of correspondence.

Mohamed Abomhara and et al. [4] IOT security in relation to vulnerabilities, threats, filters and attacks on digital security. The basic motivation of this document was to differentiate the different types of gatecrasher that involve security risks in IOT. Intruders can be described as single attacks, organized rallies and inspection offices. Expertise, capital grants, inspiration and risk resistance would be different in every situation. It was less demanding to see what dangers could abuse which deficiencies in the frame by viewing and recording all the dangers and some characters on the screen. Despite some limited physical compromises, IOT hackers generally had full DY filter functionality. Physical bargain attacks would affect a small population of the total number of IOT devices under the most adverse conditions. In order to distinguish these events and equip themselves with cheap devices, IOT engineering should coordinate these problems. To achieve their goals, the attackers used various strategies, devices and procedures to abuse their vulnerabilities in a context. With this in mind, it is essential that an association understands the attacker's intentions and abilities to counter potential damage. Finally, further research should reduce both potential threats and their outcomes.

Hui Suo et al. [5] The Internet of Things (IoT) has been studied for ten years. Security and data protection are the main problems of IoT applications and still face huge challenges. To facilitate this emerging field, we briefly review the progress of IoT research and pay attention to security. A detailed analysis of the architecture and safety functions indicates the safety requirements. On this basis, we discuss the state of research of key technologies such as the encryption mechanism, communications security, sensor data protection and cryptographic algorithms and briefly describe the challenges.

Nishant Kumar et al. [6] The Internet of Things (IoT) is a concept in which billions of devices (such as smartphones, sensors and alternative network devices) can be connected together to communicate with each other. The IoT can be a system in which the objects integrated in the detector technology interact with each other via a wireless communication medium in order to develop, exchange and transmit knowledge without human interaction. This connection is relevant in many ways, for example for timely coordination with many simple devices such as sensors, thermostats, fitbit, routers, etc. Due to the open and heterogeneous nature of these networks, they are very sensitive to vulnerable attacks. Data protection and data security are therefore the main concerns of this technology. This document focuses on common IoT vulnerabilities such as denial of service (DDoS) and attacks against background data changes. Addresses privacy and security issues in various segments such as web interface vulnerabilities, device connections, spam, data storage issues, IoT network issues such as Sybil attacks, cloud connectivity considerations and industrial IoT attacks. The purpose of this document is to present the data security and data protection concerns of the IoT environment, as well as the existing protection mechanisms.

III. PROPOSED METHODOLOGY

Jebah Jaykumar, Abishlin Blessy	For validation, the secrecy of the information and the sincerity of the information were used on the various levels of correspondence "murder of secret words" and "passwords"
Mohammed Abomhara and Geir M. Koien	It mainly explains cyber-attacks on IOT devices. Intruders are mainly divided into individual attacks, organized groups and secret services. To overcome cyber-attacks, the IOT architecture is designed to recognize intruders.
Hui Suo	research the status of key technologies, including the encryption mechanism, communication security, sensor data protection and cryptographic algorithms, and briefly summarize the challenges
Nishant Kumar	It focuses on common IoT vulnerabilities such as denial of service (DDoS) and attacks against background data changes. Addresses privacy and security issues in various segments such as web interface vulnerabilities, device connections, spam, data storage issues, IoT network issues such as Sybil attacks, cloud connectivity considerations and industrial IoT attacks.

IV.SECURITY REQUIREMENTS

Based on the above analysis, we can summarize the safety requirements for each level below, as shown in Fig. 1.

A. Perceptual Layer

First, node authentication is required to prevent illegal access to the node. Second, to protect the confidentiality of information transfer between nodes, data encryption is essential and before the agreement on the data encryption key is an important process in advance; The stronger the security measures, the more resources are used. To solve this problem, light encryption technology, which includes the light encryption algorithm and the light encryption protocol, becomes important. At the same time, the integrity and authenticity of sensor data becomes a research goal. We will address this issue in more detail in the next section..

B. Network Layer

At this level it is difficult to apply existing communication security mechanisms. Identity authentication is a type of mechanism for preventing illegal nodes and is a prerequisite for the security mechanism. Confidentiality and integrity are of equal importance. Therefore, we also need to set up a confidentiality and data integrity mechanism. In addition to the Distributed Denial of Service (DDoS) attack, it is a particularly serious common network attack method on the Internet. Therefore, there is another problem that needs to be resolved at this level to prevent the DDOS attack for the vulnerable node.

C. Support Layer

The level of support requires much of the application security architecture, such as cloud computing and secure multi-stakeholder processing, almost all powerful encryption algorithms and protocols, enhanced system security technology and antivirus.

D. Application Layer

To solve the security problem at the application level, we need two aspects. One is authentication and the key agreement in the heterogeneous network, the other is the protection of user privacy. Furthermore, education and management are of great importance for information security, in particular for password management [7] - [9].

In summary, IoT security technology is very important and full of challenges. In addition, laws and regulations are also important. We will discuss this issue below.

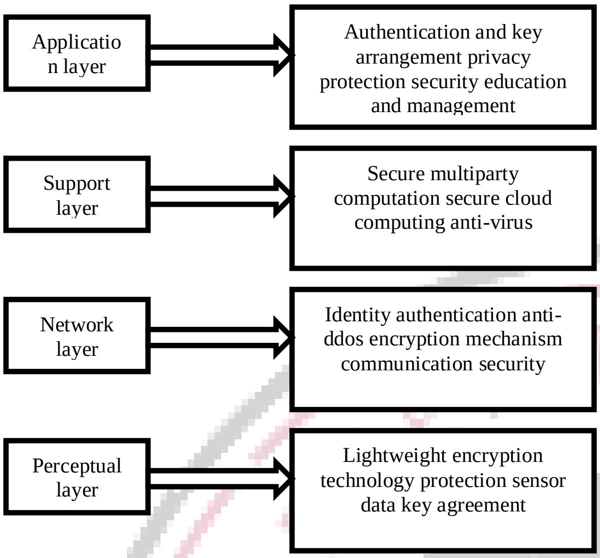

Fig. 1. Security requirement of layer

V. IOT SECURITY- DATA AUTHENTICATION

Data authentication was one of the problems, although we protected the data with encryption. If the data cannot be protected authentically, security has been compromised. Authentication problems may not be straightforward, but they are undoubtedly a security risk. In the side attacks, he focused heavily on the information presented, less on the information. Possibility of safety for the situation of the equipment for the rest. There was the IOT idea of connecting gadgets. Such devices were not developed with data communication security as a priority [10]. The old operating system and integrated software patch of the United Nations create devices vulnerable to hackers. The IOT security solution was to start at the corporate level. To reduce security risks, ordinary people and traders must be properly trained and trained to protect their IOT devices. This article has outlined security concerns with various technologies.

VI. SECURITY ISSUES

Focusing on the valuable benefits of IOT does not mean first examining the gaps in a technology. The development of IOT has slowed down over the years due to inactive development and a poor improvement derived from IOT security. The concept of data encryption in IOT collects tons of data due to the different uses of IOT. In the IOT environment, the data was collected and processed globally. SSL (Secure Socket Layer Protocol) can be used for IOT security when data is available online. However, to use wireless data transmission, we had to use a wireless protocol with integrated encryption.

VII. CONCLUSION

IOT technology offers various possibilities and new applications. However, this is important for security and privacy. In this article, the main challenges related to security and data protection have been examined from different angles such as RFID technology, algorithms, architecture, etc. Security and privacy issues are minimized through the use of various algorithms and technologies, but cannot be fully resolved. Research on this concept is still ongoing. Once graduated, IOT will become a boom in both technology and social development.

References

[1] R R. H. Weber, "Internet of things – new security and privacy challenges," Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[2] J. F. Wan, H. H. Yan, H. Suo, and F. Li, "Advances in cyber-physical systems research," KSII Transactions on Internet and Information Systems, vol. 5, issue 11, pp. 1891-1908, 2011.

[3] Jaykumar, J. and Blessy, A. "Secure smart environment using IOT based on RFID". International Journal of Computer Science and Information Technologies, vol. 5, issue 2, pp. 2493-2496, 2014.

[4] Abomhara, M. "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks". Journal of Cyber Security and Mobility, vol. 4, issue 1, pp. 65-88, 2015.

[5] Hui Suo, Jiafu Wan "Security in the Internet of Things: A Review" 2012 International Conference on Computer Science and Electronics Engineering, 2012.

[6] Nishant Kumar, J. Madhuri "Review on security and privacy concerns in Internet of Things" 2017 International Conference on IoT and Application (ICIOT), pp. 1-25, 2017.

[7] 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.

[8] C. P. Mayer, "Security and privacy challenges in the internet of things," Electronic Communications of the EASST, vol. 17, 2009.

[9] C. Ding, L. J. Yang, and M. Wu, "Security architecture and key technologies for IoT/CPS", ZTE Technology Journal, vol. 17, no. 1, Feb. 2011.

[10] Weber, R.H. and Studer, E. "Cyber security in the Internet of Things: Legal aspects". Computer Law & Security Review,