International Journal of Innovation in Computer Science and Information Technology
Vol.3, NO.3 , P: 31 - 34
Received : 25 June 2021
Accepted : 10 July 2021

An overview of IoT security challenges and solutions: A survey article

FatemehBahari*
M.Sc. Student, Department of Computer,
Faculty of Engineering, West Tehran Branch,
Islamic Azad University, Tehran, Iran
f.bahari16@gmail.com
ParisaDaneshjoo
Assistant Professor, Department of Computer
Science, Faculty of Engineering, Tehran West
Branch, Islamic Azad University, Tehran, Iran
Daneshjoo.p@wtiau.ir

Abstract

The Internet of Things is an advanced technology in which any creature, including objects, animals, humans, and tools, has the ability to send and receive data through communication networks, such as the Internet. In the IoT, any object has the ability to connect to the virtual world and thus can have a digital identity. Connecting billions of objects and tools to the Internet will bring many challenges which one of the most important of them is security. Investigating and identifying IoT vulnerabilities and providing solutions to reduce them will increase security and privacy. Therefore, the purpose of this review article is to examine the security challenges of this technology and provide appropriate solutions for it. In this review study, first, a 4-layer architecture for the Internet of Things is considered and then the appropriate security solutions for each layer are explained. This review article includes conference papers, related journal articles published during the last 10 years.

Keywords: Internet of Things, IoT, Security

Introduction

Internet of Things

The Internet of Things, as a fledgling technology, has brought dramatic changes in human life. With this technology, the presence of communication devices and information systems in human life has increased.

IoT is used for various purposes including communication, transportation, education, business development and etc. Using this technology, anyone can communicate and exchange data with any object at any time and in any place. (Ghorbani & Ahmadzadegan, 2018) The idea of the Internet of Things was first brought up in 1998 by Kevin Ashton to upgrade radio frequency (RFID) and has grown in popularity over time. (baghalzadeh nazila, 1395; Santhosh Krishna & Gnanasekaran, 2017) IoT The ubiquitous presence of various objects such as RFID tags, sensors, operators, smartphones, etc. around us that are able to interact with each other and provide services by networking and having unique addresses. The devices we use every day are becoming universal beings that can interact with humans or other devices. (Burhan et al., 2018; Santhosh Krishna & Gnanasekaran, 2017)

The total installed base of IoT connecting devices would increase to 75.44 billion globally by 2025 with an increase in growth in business, productivity, government efficiency, lifestyle, etc.,With such an expansion, the issue of IoT security will become an important issue. In this article, these security challenges will be discussed through a layered architecture, and solutions to prevent these challenges in each layer will be presented. (Ahmadi et al., 2018)

Security in Internet of Things

IoT security has long been an important issue and continues to be a major challenge, as any networked device can be a gateway to attack personal data.Therefore, concerns about the security and protection of personal data are very important. As the variety of connected devices expands and the complexity of the type of communication between these devices increases, the risk of IoT privacy breaches increases.Therefore, in implementing IoT, legal challenges, systemic approaches, technical challenges, etc. must be considered. (Ghorbani & Ahmadzadegan, 2018) IoT security must be considered from the earliest design stage to the last stage when the service is running.To better enforce IoT security requirements, a four-layer architecture is considered: Perception layer, network layer, middleware layer, and application layer; Each of these layers has its own security challenges. In the following, these layers will be introduced and their security challenges and solutions to prevent them will be provided. (Ahemd et al., 2017; baghalzadeh nazila, 1395; Pal et al., 2020)

perception layer

The perception layer in IoT architecture is known as the "sensors" layer and its purpose is to obtain environmental data through sensors. This layer is the lowest layer in the IoT architecture that identifies, collects, and processes information and then transfers it to the network layer. There are many measuring devices for collecting information from objects such as actuators, RFID tags, smart sensors, wearable measuring devices, and so on.

The sensors are grouped according to their unique purpose into environmental sensors, body sensors, home appliance sensors and vehicle meter sensors, etc. Many devices in this layer provide information storage and identification (such as RFID tags), data collection (such as sensors), and data processing (eg embedded processors). These sensors are generally smaller than computing and storage capabilities because they are simple and therefore do not have the processing power of sophisticated cryptographic algorithms for secure protection. Therefore, it is difficult to create a secure protection system. (Ahemd et al., 2017; baghalzadeh nazila, 1395)

Network layer

The next layer in the IoT architecture is the network layer. The network layer performs the function of data routing, transfer to various centers and devices via the Internet. At this level, cloud computing platforms, Internet gateways, switching, and routing tools work using some of the latest technologies such as WiFi, LTE, Bluetooth, Zigbee, etc. It should be noted that in this layer, error detection and correction, control of messages related to routing, and publishing and sharing are also performed.Network gateways act as intermediaries between different IoT nodes by collecting, filtering, and transmitting data to/from different sensors.

In general, this layer of IoT architecture is responsible for connecting to other smart devices, network devices, and servers, and is used to transmit and process sensor data.

Although this layer has secure protection, there are human attacks or fake attacks. unwanted emails, computer viruses, or large amounts of data sent to the network are other challenges related to this layer. As a result, the security mechanism at this layer is very important. (Ahmadi et al., 2018; baghalzadeh nazila, 1395)

Middleware layer

This layer works to combine the network layer and application layer. All the intelligent and cloud computing is done in this layer. Support layer functionality includes storage of data from lower-level layers to database and service management. On the basis of intelligent computing, this layer can compute information and process data automatically.) Ahemd et al., 2017; baghalzadeh nazila, 1395(

Application layer

The application layer is considered the highest layer of IoT architecture, which ensures the accuracy, integrity, and confidentiality of data. In this layer, the goal of the Internet of Things (creative environment) is achieved.This layer is responsible for delivering different types of special services and programs to different users in the Internet of Things. These programs can be from different sectors of the industry such as manufacturing, environment, healthcare, food, and medicine. At this level, security is different for different application environments, and data sharing, which is one of the characteristics of the application layer, causes problems with data privacy, access control, and information disclosure. (Ahemd et al., 2017; baghalzadeh nazila, 1395)

Solutions to prevent security challenges in the IoT layered architecture

Perception layer security challenges and solutions

- **Sensor network Security Policy**

Sensor network technology has limitations such as the physical capture of sensor nodes and gateway nodes, integrity and congestion attacks, DoS (Denial of Service) attacks, eavesdropping, and node repetition attacks. Creating a security framework for the sensor network requires security policies such as encryption algorithms, core distribution policies, intrusion detection mechanisms, and sensor data protection**.** (Ahemd et al., 2017; Santhosh Krishna & Gnanasekaran, 2017)

- **RFID security policy**

RFID security issues include leak information of tags and RFID users, sniffing attacks, middleman attacks, simulation, broadcasting, and manipulation of attacks. In most cases, RFID security is implemented using physical methods or code mechanisms, or sometimes both. RFID security protocols include LCAP, Hash Lock, Hash Chain, and Decryption protocols. (Ahemd et al., 2017; Santhosh Krishna & Gnanasekaran, 2017)

Network layer security challenges and solutions

In IoT architecture, the main task of the network layer is to transmit information across the network, since the IoT is implemented on a basic communication framework, subject to various attacks including Denial of Service (DoS), middle human attacks, gateway attacks, Storage attacks, etc. are located.

The network-level security strategy must maintain the authenticity, confidentiality, integrity, and availability of data whenever data is transmitted over the network. Key management, authentication, intrusion detection, and negotiation can be done to secure the network against such attacks. (Ahemd et al., 2017; Santhosh Krishna & Gnanasekaran, 2017)

Challenges and security solutions of the middleware layer

Some of the technical issues are related to privacy, security, and reliability in the middleware layer. Ensuring confidentiality and secure storage and the use of antivirus makes the middleware layer more secure. (Ahemd et al., 2017; Santhosh Krishna & Gnanasekaran, 2017)

Application layer security challenges and solutions

Privacy is the most important component in the security of the application layer, to ensure access and prevent unauthorized use of data, access permissions must be restricted.Data distortion technology and data encryption technology agents are common privacy technologies. To achieve data security, the backup and data recovery mechanism must be done properly. Some data privacy techniques are TLS, SSL, DNS, and so on. (Ahemd et al., 2017; Santhosh Krishna & Gnanasekaran, 2017)

Conclusion

In this paper, IoT security was examined in a four-layer architecture, as well as security features and requirements at the perceptual, network, middleware, and application layers.

Then, security solutions for each layer were presented, which include encryption algorithms, security portfolios, sensor data protection, authentication, key management.

By using these solutions, the security of this technology can be improved to a desirable level.

Resources

1. Ahemd, M. M., Shah, M. A., & Wahid, A. (2017). IoT security: A layered approach for attacks & defenses. International Conference on Communication Technologies, ComTech 2017, 104–110. https://doi.org/10.1109/COMTECH.2017.8065757
2. Ahmadi, P., Islam, K., Maco, T., & Katam, M. (2018). A survey on internet of things security issues and applications. Proceedings - 2018 International Conference on Computational Science and Computational Intelligence, CSCI 2018, 5(6), 925–934. https://doi.org/10.1109/CSCI46756.2018.00182
3. baghalzadeh nazila, nemati sajjad. (1395). security in IoT. The Second National Conference on New Approaches in Electrical and Computer Engineering, Islamic Azad University, Khorramabad Branch, 1–7.
4. Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. Sensors (Switzerland), 18(9). https://doi.org/10.3390/s18092796
5. Ghorbani, H. R., & Ahmadzadegan, M. H. (2018). Security challenges in internet of things: Survey. 2017 IEEE Conference on Wireless Sensors, ICWiSe 2017, 2018-Janua, 6–11. https://doi.org/10.1109/ICWISE.2017.8267153
6. Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020). Security requirements for the internet of things: A systematic approach. Sensors (Switzerland), 20(20), 1–34. https://doi.org/10.3390/s20205897
7. Santhosh Krishna, B. V., & Gnanasekaran, T. (2017). A systematic study of security issues in Internet-of-Things (IoT). Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017, 107–111. https://doi.org/10.1109/ISMAC.2017.8058318