INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp : 73-76

IOT SECURITY CHALLENGS AND PROBLEMS

Mr. Manzoor Ali[1]

[1]FCSA (Jawahar Navodaya Vidyalaya, Gharota, Jammu-1 (J&K), India.

ABSTRACT

The Internet of Things (IoT) is a modern, advanced technology that generates large amounts of data and new software applications. The methodological approaches for secure IoT development are receiving more and more attention from researchers and IoT developers. The Internet of Things (IoT) is the term used to describe the billions of physical objects that are linked together online in order to exchange and collect data. Anything can be made a part of the IoT as technology develops further. By 2025, the IoT will have generated $5.1 billion in global spending. As a result, more data will be used and more transactions will take place online. Additionally, there are smaller, more potent devices available for data exchange, interconnection, and a variety of software and hardware applications. In this aspect this component will require solutions to substantial security challenges. Wearable safety gadgets for women, healthcare, home automation, smart cities, smart agriculture, weather monitoring systems, natural disaster systems, smart cars, industrial automation, etc. are just a few of the applications where IoT is being employed. We benefit from IoT capabilities, but with them come security risks as well. It demonstrates a variety of security issues, such as protecting these devices' information, correspondence, and gadgets from unauthorized access. This study examines the security challenges and issues and the suggestions. A summary of security issues and challenges, suggestions are presented in this paper.

Keywords: Internet of Things (IoT), IoT Security Challenges and Issues

1. INTRODUCTION

The concept of Internet of Things (IoT) was introduced by Kevin Ashton, a Co-founder of the Auto-ID Center at MIT in 1998[1]. The idea of common physical objects being connected to the internet and having the ability to recognize other devices is referred to as the "internet of things" (IoT). Physical and virtual "things" have identities, physical attributes, virtual networks, and intelligent interfaces, and it has a dynamic global network architecture with self-configuring capabilities.

- **Self-configuring-** IoT devices has self-configuring capability which allows large number of devices to work together to work provide certain functionality they can change their networking and update the software automatically.
- **Interoperable Communication Protocol:** There are a variety of communication protocols that IoT devices can use to connect with one another without extra effort.
- **Unique ID:** Each Internet of Things (IoT) gadget has its own identity, which is distinguished by its own IP address.
- **Integrated into Information Network:** IoT devices are connected to the information network, enabling data exchange and communication with other systems and devices.

1.1. Physical Design of IoT Things in IoT

The term "Things" refers to Internet of Things (IoT) objects with distinct identities that are capable of remote sensing, actuation, and monitoring. These gadgets are able to exchange information and talk to one another. The Internet of Things (IoT) devices include a variety of wired and wireless interfaces for connecting to other devices, including the followings.

- I/O interfaces for sensors
- Interfaces for internet connectivity
- Memory and storage
- Audio and video interface

1.2. What is IoT?

The billions of physical objects that are integrated with sensors, software, and other technologies that are connected to the internet in order to connect and exchange the software, hardware, and datawith other objects and systems are referred to as "things" in the Internet of Things (IoT). These gadgets include basic household appliances and cutting-edge industrial gear. Anything can be made a part of the IoT as technology develops further. By 2025, the IoT will have generated $22 billion in global spending. Even while we may now accomplish things that were formerly thought to be impossible, digitizing everything has some drawbacks. The term "Internet of Things" (IoT) refers to a highly

distributed network that combines connections with tools and gadgets as well as sensors, monitors, and other devices.[1, 2]

1.3. Uses of IoT

- IoT is an interconnected network of computing and digital devices. Because people, machines, and data are all seamlessly connected, the Internet of Things (IoT) streamlines, improves, and automates operations. The integration of sensors, networking, and artificial intelligence has the potential to improve the performance of numerous systems. There are previously impractical techniques to cut costs and work hours.
- These devices can operate any number of functions, from sensors in thermostats and factory machines to printers, TVs, our mobile phones, and even refrigerators. IoT applications benefit businesses, individual consumers, and the government.
- **Examples of IoT devices** are smartphones, Home Automation, Fitbits, laptops, Farming, Shopping Malls, refrigerators, Smart Cars, Google Home, Wearable Health Monitors, coffee machines, Apple watches, etc. Devices equipped with an Internet connection and sensors can be used for IoT applications.

1.4 The Importance of IoT

In recent years, IoT has emerged as one of the most important 21st-century technologies. Thanks to embedded technology, which can connect everyday objects like thermostats, baby monitors, autonomous cars, robots, smart cities, smart wearable gadgets, and more to the internet, continuous connectivity and communication between people, processes, and things is now possible. Low-cost computers, the cloud, big data, analytics, and mobile technologies allow physical things to share and collect data with the least amount of human involvement. In today's hyperconnected society, digital systems have the ability to record, monitor, and alter every contact between connected entities. Though they collide, the physical and digital worlds coexist. Applications of IoT are as follows [7, 8]

1.5. Application Areas of IoT

- IoT Applications in Smart Home Appliances.
- IoT Applications in Smart Cities.
- IoT Applications in Smart Grid and Energy Saving.
- IoT Applications in Water and Waste Management.
- IoT Applications in Water Supply.
- IoT Applications in Maintenance Management.
- IoT Applications in Smart Pollution Control

2. LITERATURE SURVEY

In this literature survey we analyzed the challenges and issues of the IoT applications and technologies. And also analyzed the following topics: what is IoT Security, types of IoT Security, Security challenges and Issues, Importance of IoT Security and Suggestions and solutions to improve the IoT Security.

[6, 7]

2.1 What is IoT Security?

IoT security that addresses the plans, instruments, procedures, systems, and techniques employed to safeguard every facet of the internet of things. In order to guarantee the availability, integrity, and confidentiality of IoT ecosystems, it also involves the protection of software systems like robot automation systems, women's wearable gadgets, apps, data, and network connections.[5, 6]

2.2 Types of IoT Security

There are three types of IoT Security

- **Network Security:** Users need to protect their devices against unauthorized access and potential exploitation.
- **Embedded Security**: Nano agents provide on-device security for IoT devices
- **Firmware Assessment:** Firmware security starts with assessing the firmware of a protected IoT device.

2.3. Security challenges and Issues

2.3.1 The importance of IoT Security and How to improve it?

- IoT security of the internet's infrastructure is crucial because more IoT devices are interconnected via the internet. So IoT security is essential
- to protect our data, software, data privacy, and children from cybercrime, using various encryption techniques such as encryption, authentication, authorization. [3, 4].
- Hackers have access to production logic, control-loop settings, and the state of a hacked robot, which can be programmed to damage things it is making.

- IoT device security is essential to protect medical equipment from cyberattacks.
- IoT security is essential to protect IoT devices from unauthorized access, preventing them from leaking data or acting as a backdoor. [9, 10]

2.3.2 Security Issues:

IoT security issues are increasing due to lack of focus on organizational and methodological security concerns, lack of standards and regulations, and ignorance of the dangers and complexity of IoT systems[11,12]. Among the many IoT security issues are the following:

a) **Data privacy:** Data privacy is a major threat to IoT security, as it can be exploited by hackers.
b) **Ransomware:** Ransomware attacks on IoT devices are uncommon, but they may be in risk due to their increasing value.
c) **Lack of Visibility:** IT staff cannot create a precise inventory of all IoT devices connected to the network, making security personnel unable to prevent breaches.
d) **Limited Security Integration:** Due to their diversity and size, IoT devices can be challenging to incorporate into security systems, if not impossible.
e) **Lack of Physical Security:** IoT device makers must ensure physical security of their products, but developing secure transmitters and sensors can be challenging.
f) **Botnet Attacks :** Hackers can easily infect IoT devices and turn them into massively scalable botnets due to lack of security updates.
g) **Poor Testing:** The majority of Internet of Things (IoT) developers do not prioritise security, hence they do not effectively conduct vulnerability testing to find flaws in IoT systems.
h) **Open-source Code Vulnerabilities:** IoT device firmware frequently uses open-source software, which can have faults and vulnerabilities.
i) **Overwhelming Data Volume:** Data supervision, management, and protection are challenging due to the volume of data created by IoT devices.
j) **Unpatched Vulnerabilities:** For a variety of reasons, including the lack of fixes and challenges accessing and installing them, many IoT devices have vulnerabilities that have not yet been patched.
k) **Vulnerable APIs:** APIs are frequently used as points of access to command-and-control infrastructure from which attacks like SQL injection, distributed denial of service (DDoS), man-in-the-middle (MITM), and network intrusion are initiated.

3. SUGGESTIONS TO IMPROVE IOT SECURITY

IoT security solutions are being implemented to close security gaps and prevent security breaches, but a holistic approach is needed to effectively manage it. Three key capabilities for a robust IoT security solution are the ability to:

1. **Learn**: Take advantage of security solutions that provide network visibility to learn what the ecosystem encompasses at what the risk profiles are for each group of IoT devices.
2. **Protect**: Monitor, inspect, and enforce IoT security policies commiserate with activities at different points in the infrastructure
3. **Segment**: In the same way that networks are segmented, use segmentation based on policy groups and risk profiles to segment IoT systems. Any connected devices can be vulnerable to cyberattacks. Make sure to follow these tips to prevent potential attacks.

- **Unauthorized IoT device scans**: A person gains logical or physical access without permission to a network, system, application, data, or other resource.
- **Password Management**: Password management is a set of principles and best practices to be followed by users while storing and managing passwords in an efficient manner to secure.
- **Patch Management:** Patch management of applying vendor-issued updates to close security vulnerabilities and optimize the performance of software and devices
- **Security Gateways:** A secure web gateway is an on-premise or cloud-delivered network security service. Sitting between users and the Internet, secure web gateways provide advanced network protection by inspecting web requests against company policy to ensure malicious and websites are blocked and inaccessible.
- **Network Security**: Network security is a set of technologies that protects the usability and integrity of a company's infrastructure by preventing the entry or proliferation within a network of a wide variety of potential threats.
- **Network Traffic Monitoring Analysis**: It is a method monitoring network availability and activity to identify anomalies, including security and operational issues.

- **Use IoT security analytics:** Security analytics can help reduce IoT security concerns and vulnerabilities by gathering and analyzing data from multiple sources to identify and prevent potential risks.
- **Endpoint Detection and Response (EDR):** EDR technology enables security professionals to quickly spot malicious activities and gain direct access to devices, with automatic real-time blocking of questionable behaviour.
- **Secure APIs:** Organizations can prevent hackers from accessing IoT devices by implementing security best practises and testing.
- **Improve Network Visibility:** Organizations can prevent hackers from accessing IoT devices by implementing security best practises and testing.
- **Encrypted Communication:** By interfering with IoT communication, attackers can access gadgets. You must encrypt communication between IoT devices and interfaces like web apps and mobile apps to prevent data breaches. The most widely used encryption method for data transit today is SSL/TLS.
- **Authentication:** Comprehensive device authentication helps reduce IoT device vulnerabilities because hackers are always seeking for new ways to gain access to sensitive information. There are several authentication techniques for Internet of Things (IoT) devices, including biometrics, digital certificates, and multifactor authentication. It is crucial to ensure that unauthorised individuals cannot access your gadgets.

4. CONCLUSION

The Internet of Things (IoT) is the next step towards a ubiquitous connection to all communication- and computation-capable items, regardless of access technology, resource availability, or location. Deflecting hostile insiders to thwarting nation-state attacks are just a few of the IoT security problems. Attacks continue to expand in size and scope as a result of IoT devices' innate vulnerability and the extent of their deployment. Despite the IoT security difficulties, protecting connected devices is well worth the expenditure. In order for IoT devices to be as valuable as other technologies, improved security is a necessity. Both risks and profits will be reduced by it. In this review we discussed the suggestions to solve the IoT Security challenges and issues.

5. REFERENCES

[1] Vikas Hassija at el, “A Survey on IoT Security, Application Areas, Security Threats and Solution Architectures”, IEEE Access, Page No : 1-24,Volume x, 2019.

[2] S. Soursos, I.P. Žarko, P. Zwickl, I. Gojmerac, G. Bianchi, and G.Carrozzo, G., 2016, “Towards the cross-domain interoperability of IoTplatforms. In Networks and Communications (EuCNC),” European Conference on. IEEE, pp. 398-402, 2016.

[3] Daj, C. Samoila, and D. Ursutiu, "Digital marketing and regulatorychallenges of Machine-to-Machine (M2M) Communications, 9thInternational Conference on Remote Engineering and Virtual Instrumentation (REV), 2012.

[4] A. T.Capossele, V. Cervo, C. Petrioli, and D. Spenza, “Counteracting Denial-of-Sleep Attacks in Wake-up-radio-based Sensing Systems. In Sensing, Communication, and Networking (SECON),” 13th Annual IEEE International Conference on IEEE, pp. 1-9, 2016.

[5] Saad Albishi, Ben soh, Azmat Ullah, Fahad, Algarni “Challenges and Solutions for Applications and Technologies in the Internet of Things”, Elsevier.

[6] KrishnaKanth, Gupta and sappna shukla, “ Internet of Things : Security Challenges for next generation networks”, doi :10.1109/ICICCS.2016.7542301, pp : 315-318, February 2016.

[7] C. Bekara, “Security issues and challenges for the IoT-based smart grid”, Procedia Computer Science 34, pp. 532–537, 2014.

[8] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Champak, “Internet of things: Vision, applications and research challenges”, Ad HocNetworks, vol. 10, no. 7, pp. 1497–1516 , 2012

[9] F. A. Alaba, M. Othman, I. A. T Hashem, F. Alotaibi, "Internet of Things security: A survey." Journal of Network and Computer Applications 88 , pp. 10-28, 2017.

[10] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the Internet of Things: perspectives and challenges. Wirel. Netw. 20 (8), pp. 2481–2501, 2014.

[11] N. Agarwal, A. Rana, J.P. Pandey, A. Agarwal, “Secured sharing of data in cloud via dual authentication, dynamic unidirectional PRE, and CPABE" in International Journal of Information Security and Privacy, Vol 14, Issue 1, pp 44-66, 2020.

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

[13] https://blog.smartbear.com/iot-2/how-to-protect-iot-gateways-from-securityvulnerabilities/ (Online; accessed on 04 May 2018)