ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

ANALYSIS OF SECURITY THREATS, ATTACKS IN THE INTERNET OF THINGS

Afsana Anjum[1], Ayasha Siddiqua[1], Shaista Sabeer[1], Sunanda Kondapalli[1], Chamandeep Kaur[1] and Khwaja Mohd Rafi[2]

[1]Lecturer, Department of Computer Science, Jazan University, Saudi Arabia

[2]Director, Mewat Engineering College (Wakf), Nuh, Haryana, India

ABSTRACT

The concept of the Internet of Things is defined by the desire to connect everything to everything at any time (IoT). The Internet of Things (IoT) idea encompasses not just enabling connectivity but also permitting interaction between these connected objects. Though the term "internet of things" was coined in 1999, it has received a lot of attention in recent years. The rate at which new gadgets are integrated into the system will have a significant positive impact on the world, but it will also pose substantial security and privacy risks.

In its current state, IoT is vulnerable to a wide range of threats. Because data is exposed to a variety of attacks by attackers at each tier of IoT, one of the most pressing challenges of IoT is to provide security assurance for data flow. The Internet of Things is organized in layers, with each layer providing a service. Because each layer serves a particular purpose, the security requirements change from one another. This paper is to examine the numerous security and privacy issues associated with IoT. The paper briefly describes a number of existing security mechanisms that operate at various layers.

Keywords*: IoT, security, privacy, threat, attack, data flow.*

1. INTRODUCTION

With the development of Wireless Sensor Networks (WSN) and technologies such as Radio Frequency Identification (RFID), the Internet of Things (IoT) was born in 1999. (RFID). The Internet of Things (IoT) is based on the idea of connecting everything to everything at any given time. It employs sensors, actuators, and other items to make physical and virtual connections. IoT security is critical to the success of IoT infrastructure and applications. The Internet of Things (IoT) uses sensors to collect data from a large geographic area [1].

The Internet of Things (IoT) is going to become more popular. The idea behind IoT devices is that they must not only be connected, but also interactive. They should use context-based interactions as soon as possible [2]. The internet will have billions of interconnectivity points.

The Internet of Things (IoT) is a technology that connects individuals, persons and objects, things and things, and so on. Sensors and items are integrated into the IoT infrastructure for communications that can function without human intervention. Sensors are vital in the IoT because they are devices that not only gather but also monitor heterogeneous data [3], [4].

The purpose of the Internet of Things is to create a network infrastructure that allows sensor devices to communicate with other individuals and objects. The Internet of Things is organized in layers, with each layer providing a service. Because each layer serves a particular purpose, the security requirements differ from one layer to the next. In the IoT infrastructure, there are a number of difficulties that must be addressed. The following are the reasons:

a. Nature of smart objects

b. Usage of standard protocols

c. The bidirectional flow of information

The fundamental hurdles of the IoT infrastructure include security issues such as privacy, authorization, verification, access control, system setup, information storage, and management [6]. Without a doubt, security concerns must be addressed in order for IoT to become a reality. The internet of things (IoT) is the next generation of the internet.

1.1 The phases of the IoT lifecycle are as follows:

a. Create - Physical devices (sensors/actuators) collect data from their environment that can be used to generate insights.

b. Communicate – The acquired data is sent through the network to the intended place.

c. Aggregate - The collected data is aggregated by the devices.

d. Analyze - Patterns are generated by analyzing the pooled data.

e. Act – Based on the information, appropriate actions are taken.

2. RELATED WORK

The technology and security problems are the two sorts of security challenges. Wireless technology and the scattered nature of the IoT are among the technological obstacles. Authentication and secrecy concerns are addressed in the security [7]. Confidentiality, authentication, availability, heterogeneity, lightweight solutions, key managements, policies, and integrity are some of the major IoT principles.

The Internet of Things (IoT) has recently become a popular study area. As a result of the IoT's immense potential as a new way to endanger users' privacy, security, and a wide range of threats, attackers are taking use of it. This study will provide a thorough overview of IoT security threats and attacks. The paper includes existing security measures and analysis.

2.1 SCOPE

This paper examines the many security protocols that can provide privacy and security in IoT-based applications, with the goal of standardizing the security architecture for IoT. The most crucial feature of IoT applications is security, as it deals with intrusive devices whose security is critical for the user's safety and security. The most significant impediment to widespread adoption of IoT devices in everyday life is security. This paper will look at all of the current security strategies and protocols that can be used to protect IoT-based systems.

3. SECURITY REQUIREMENTS

Because the IoT infrastructure contains a lot of personal information like names, dates of birth, and locations, we need to take extra precautions to protect data and address privacy concerns. The use of a layered structure is used to overcome security difficulties. Confidentiality, authenticity, integrity, and availability are the four core security properties that must be implemented. Scale, IP Protocol-Based IoT, Heterogeneous IoT, and Lightweight Security are all security needs that are developed from the basic security criteria.

3.1 ANALYSIS OF SECURITY THREATS, ATTACKS IN THE IOT

The threats can extensively be labelled into 3 classes. The classes are seizing, disrupt and managing. The seize hazard approach shooting records or a device without authorization. The seize threats are such threats which are designed to advantage get admission to records this is both logical and bodily on a device. The disrupt hazard approach denies getting admission to or destroying a device. The manage hazard approach manipulates time collection data, identity, or the data.

a. Botnets

Cybercriminals can make use of botnets to assault IoT gadgets which are linked to numerous different gadgets including laptops, desktops, and smartphones.

Mirai botnet has displayed how risky IoT protection threats can be. The Mirai botnet has inflamed an predicted 2.five million gadgets, along with routers, printers, and clever cameras. Attackers used the botnet to release dispensed denial of carrier assaults on numerous IoT gadgets. After witnessing the effect of Mirai, numerous cybercriminals have advanced a couple of superior IoT botnets. These botnets can release state-of-the-art cyber assaults towards inclined IoT gadgets.

b. Denial of service

A denial-of-carrier (DoS) assault intentionally attempts to purpose an ability overload with inside the goal machine via way of means of sending more than one requests. IoT protection threats together with denial-of-carrier assaults can destroy the recognition of companies and have an effect on their revenue.

c. Man-in-the-Middle

In a Man-in-the-Middle (MiTM) assault, a hacker breaches the verbal exchange channel among person structures in a try and intercepts messages amongst them. Man-in-the-center assaults may be used to assault numerous IoT gadgets as they percentage facts in real-time. With MiTM, attackers can intercept communications among more than one IoT gadgets, main to essential malfunction. For instance, clever domestic add-ons inclusive of bulbs may be managed with the aid of using an attacker the use of MiTM to extrade its colour or flip it on and off. Such assaults can result in disastrous outcomes for IoT gadgets inclusive of business system and clinical gadgets.

d. Social engineering

Social engineering assaults may be less difficult to execute in case of IoT gadgets. IoT gadgets, particularly wearable, acquire massive volumes of for my part identifiable facts to increase a customized enjoy for his or her customers. Such gadgets additionally make use of non-public facts of customers to supply person-pleasant services, for example, ordering merchandise on-line with voice control. IoT safety threats which includes social engineering may be used to advantage unlawful get right of entry into person data.

e. Advanced persistent threats

Advanced continual threats (APTs) are a primary protection difficulty for numerous organizations. A superior continual danger is a focused cyber-attack, in which an outsider profits unlawful get right of entry to a community and remains undetected for an extended duration of time. Attacker’s intention to display community hobby and scouse borrow essential records the usage of superior continual threats. Such cyber assaults are hard to prevent, detect, or mitigate.

With the arrival of IoT, massive volumes of important records are effects transferred amongst numerous gadgets. A cybercriminal can goal those IoT gadgets to advantage get right of entry to private or company networks. With this approach, cybercriminals can scouse borrow private information.

f. Ransomware

Ransomware may be one of the maximum state-of-the-art IoT safety threats. Researchers have proven the effect of ransomware the usage of clever thermostats. With this approach, researchers have proven that hackers can flip up the temperature and refuse to head returned to the everyday temperature till they get hold of a ransom. Similarly, ransomware also can be used to assault IoT gadgets and clever domestic. For instance, a hacker can assault a clever domestic and ship a notification to the proprietor to pay a ransom.

g. Remote recording

Documents launched through WikiLeaks have proven that intelligence organizations understand approximately the life of zero-day exploits in IoT devices, smartphones, and laptops. These files mean that protection organizations had been making plans to report public conversations secretly. These zero-day exploits also can be utilized by cybercriminals to report conversations of IoT users. For instance, a hacker can assault a clever digital digicam in an employer and report video photos of normal enterprise activities. With this approach, cybercriminals can collect personal enterprise statistics secretly. Such IoT protection threats can even result in foremost privateness violations.

To mitigate their effects, enterprise leaders want to be up to date approximately IoT protection threats and create a holistic cyber security approach earlier than using IoT infrastructure for his or her employer. For this purpose, they could rent a devoted crew of cyber security experts who can cope with all protection concerns. Alternatively, if enterprise leaders desire to perform cyber security strategies independently, they could begin through making sure that everyone their personal facts is encrypted and their structures are often audited for protection purposes.

4. DISCUSSION

4.1 LIMITATIONS AND CHALLENGES

Although IoT gives many advantages in lots of regions and solves some issues in different sectors, it nevertheless faces a variety of various safety challenges and limitations.

Limitations

Below given are the limitations for IoT.

a. Primarily based totally on IoT Communication Devices, Devices of the IoT are sources constrained, and therefore, conventional protection mechanisms aren't unique in clever things.

b. Totally based on WSN Objects within the IoT are managed via microcontroller, reminiscence area and frequently within the strength intake as in wireless sensor networks.

c. Remote reprogramming may additionally now no longer be feasible for the gadgets of IoT because of protocols and working structures, so it can now no longer be capable of acquire codes and a brand new library. Embedded software program constraint: Operating structures of IoT which can be embedded in IoT gadgets have thin.

d. One of the maximum outstanding functions and traits of IoT gadgets is the mobility feature; this is suggest those gadgets be a part of a near and proximal community without preceding configuration. Because of this nature of mobility, we want to expand scalable protection algorithms and mechanisms in IoT gadgets to be well matched with mobility.

Challenges

Below given are the challenges for IoT

a. Lower power sources and capacity

b. Absence of expertise

c. Privacy protection

d. Cost vs. security trade-offs

e. Data storage in IoT devices

f. Varying security measures and requirements for IoT components

g. Complicated expanded system

h. Limited infrastructure resources

4.2 GAPS AND OPPORTUNITIES

Today, there are 8.6 billion IoT connections. By 2026, that range will almost triple to 23.6 billion, in step with ABI Research marketplace data.

This exponential increase will bring in a brand new generation of connectivity and productiveness within the years ahead. However, it's going to additionally bring about new hazard vectors and vulnerabilities which have initiated worries round protection. Among them:

a. Some gadgets are incapable of being secured because of restricted resources, processing capabilities, and computing power

b. Original Equipment Manufacturers (OEMs) and providers frequently pick to simply accept the risk, as opposed to remediate it for the duration of a Cost-Benefit Analysis (CBA), whilst many others pick now no longer to do a CBA at all

c. Functional safety-kind IoT gadgets prioritize availability and frequently can't concurrently make certain confidentiality

d. There is restricted IoT security solution inside the marketplace, due in big component to the fragmented nature of the IoT itself.

While those gaps pose a big assignment for groups and cease users, additionally they constitute a superb possibility or opportunity for players inside the IoT space, inclusive of IoT provider providers, providers, platform operators, and Information Technology (IT)/Operational Technology (OT) security organizations.

5. FUTURE PREDICTIONS

The basic challenges of the IoT are speedy emerging. One of the important thing of IoT deployment is safety. Following are the important safety situations for IoT infrastructure and services:

a. With the chance of device inside the infrastructure developing exponentially, it's far a huge challenge to identify, authenticate and stable the gadgets.

b. A centralised safety version may be very tough and costly to scale, maintain and manage.

c. A centralised safety infrastructure will introduce a single factor of failure and may be an easy aim for DDoS attack.

d. Centralised infrastructure may be tough to enforce in business setup wherein the threshold nodes are great geographically

Blockchain era appears to be a possible opportunity because of the strengths. It may be used to create secured mesh network to be able to permit IoT devices to attach securely and reliably averting the threats of device spoofing and impersonation.

6. CONCLUSION

In this paper we discussed about IoT, its infrastructure, difficulties, phases of IoT, security problems, scope, and security requirements. According to these data we analysed the different types of attack and some of the security problems like threats etc. Using these, we analysed the type of threats and its security issues and know the level of problem facing for IoT, Data is not very secured. Blockchain technology can be used to provide more security and reliability.

7. REFERENCES

1. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (Iot): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.

2. Roman, R., Najera, P., Lopez, J., 2011. Securing the internet of things. Computer 44 (9), 51_58.

3. Horrow, S., and Anjali, S. (2012). Identity Management Framework for Cloud Based Internet of Things. SecurIT '12 Proceedings of the First International Conference on Security of Internet of Things, 200– 203. 2012

4. Whitmore, A., Agarwal, A., and Da Xu, L. (2014). The Internet of Things: A survey of topics and trends. Information Systems Frontiers, 17(2), 261– 274.

5. Aazam, M., St-Hilaire, M., Lung, C.-H., and Lambadaris, I. (2016). PRE-Fog: IoT trace based probabilistic resource estimation at Fog. 2016 13th IEEE Annual Consumer Communications and Networking Conference (CCNC), 12– 17.

6. Jiang, H., Shen, F., Chen, S., Li, K. C., and Jeong, Y. S. (2015). A secure and scalable storage system for aggregate data in IoT. Future Generation Computer Systems, 49, 133– 141.

7. Li, S., Tryfonas, T., and Li, H. (2016). The Internet of Things: a security point of view. Internet Research, 26(2), 337– 359.

A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials, 17(4):2347–2376, Fourth quarter 2015.

8. Pongle, P., and Chavan, G. (2015). A survey: Attacks on RPL and 6LoWPAN in IoT. 2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015, 0(c), 0–5.

9. Tsai, C.-W., Lai, C.-F., and Vasilakos, A. V. (2014). Future Internet of Things: open issues and challenges. Wireless Networks, 20(8), 2201–2217.

10. V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol. 3, no. 1, pp. 11-17, 2015

11. D. Locke, "MQ telemetry transport (MQTT) v3. 1 protocol specification," IBM Developer Works Technical Library, 2010, http://www.ibm.com/developerworks/webservices/library/ws-mqtt/index.html

12. M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in Fifth International Conference on Communication Systems and Network Technologies (CSNT 2015), April 2015, pp. 746-751.

13. OASIS, "OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0," 2012, http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-complete-v1.0-os.pdf

14.] T. Winter, et al, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," IETF RFC 6550, Mar. 2012, http://www.ietf.org/rfc/rfc6550.txt

A. Aijaz and A. Aghvami, "Cognitive machine-to-machine communications for internet-of-things: A protocol stack perspective," IEEE Internet of Things Journal, vol. 2, no. 2, pp. 103-112, April 2015,

15. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7006643

16. Z. Zhou, B. Yao, R. Xing, L. Shu, and S. Bu, "E-CARP: An energy efficient routing protocol for UWSNs in the internet of underwater things," IEEE Sensors Journal, vol. PP, no. 99, 2015, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7113774

17. D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6TiSCH: Deterministic IP-enabled industrial internet (of things)," IEEE Communications Magazine, vol. 52, no. 12, pp. 36-41, December 2014, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6979984

18. M. Hasan, E. Hossain, D. Niyato, "Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches," in IEEE Communications Magazine, vol. 51, no. 6, pp. 86-93, June 2013, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6525600

19. Z-Wave, "Z-Wave Protocol Overview," v. 4, May 2007, https:// wiki.ase.tut.fi/courseWiki/imges/9/94/SDS10243_2_Z_Wave_Protocol_Overview.pdf

20. ZigBee Standards Organization, "ZigBee Specification," Document 053474r17, Jan 2008, 604 pp., http://home.deib.polimi.it/cesana/teaching/IoT/papers/ZigBee/ZigBeeSpec.pdf

21. O. Cetinkaya and O. Akan, "A dash7-based power metering system," in 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Jan 2015, pp. 406-411, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7158010

22. Zhang, Zhi-Kai, et al. "IoT security: ongoing challenges and research opportunities" Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. IEEE, 2014.

23. D. Migault, D. Palomares, E. Herbert, W. You, G. Ganne, G. Arfaoui, and M. Laurent, "E2E: An Optimized IPsec Architecture for Secure And Fast Offload," in Seventh International Conference on Availability, Reliability and Security E2E:, 2012.

24. Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on. IEEE, 2014.

25. B. L. Suto, "Analyzing the Accuracy and Time Costs of Web Application Security Scanners," San Fr., no. October 2007, 2010.

26. S. Alam, S. T. Siddiqui, F. Masoodi, M. Shuaib, "Threats to Information Security on Cloud: Implementing Blockchain", 3rd international conference on SMART computing and Informatics (SCI), 21-22 December 2018, Odisha. Springer. (2018).

27. M. Shuaib, A. S. and S. T. Siddiqui, “Multi-Layer Security Analysis for Hybrid Cloud”, 6th International Conference on System Modeling & Advancement in Research Trends, SMART-2017; IEEE, 29th -30th December, pp 526-531, (2017).

28. O. El Mouaatamid, M. LahmerInternet of Things security: layered classification of attacks and possible countermeasures Electron J (9) (2016).

29. https://en.wikipedia.org/wiki/Artificial_intelligence#Defining_artificial_intelligence