Inspira-Journal of Commerce, Economics & Computer Science (JCECS)
ISSN : 2395-7069, Impact Factor: 6.289, Volume 08, No. 02, April-June, 2022, pp. 77-80

INTERNET OF THINGS (IOT) SECURITY CHALLENGES AND COUNTERMEASURES: A LITERATURE REVIEW ON CURRENT RESEARCH

Priyanka Nama[*]

ABSTRACT

In today's world Internet of Things (IoT) devices can be found everywhere in homes, offices, agriculture, healthcare, insurance, transportation etc. These devices have brought significant changes in our daily lives, society and industry. But securing these IOT devices has become utmost important for manufacturers as well as their consumers. Because human factors are intertwined with IoT infrastructure, it's critical to think about data security and device functionality. Traditional security methods can't be applied to these devices due to their heterogeneity and resource constraints. Distributed Denial of Service (DDoS), Man In The Middle (MITM), and replay attacks are some of the most common types of attacks. This literature review paper intends to analyze recent research in IOT security from 2018 to 2021. Goal of this paper is to provide researchers information about IoT security research, challenges and countermeasures, open issues, datasets and simulation models used for IoT Security.

***KEYWORDS**: Internet of Things (IoT), Distributed Denial of Service (DDoS), Man in The Middle (MITM).*

Introduction

The Internet of Things (IoT) is a network of billions of connected gadgets that can exchange data over the internet. The number of connected devices is continuously increasing, giving enemies greater opportunities to acquire access to devices and utilise them to conduct large-scale attacks. Self-driving vehicles (SDV) for automated vehicular systems, microgrids for distributed energy resource systems, and Smart City Drones for surveillance systems are some examples of existent IoT systems. Integrating the physical and cyber spheres really makes you more vulnerable to assaults. Currently, the offered strategies and security methods are primarily based on traditional network security methods. Due to the variety of IoT devices, implementing security methods in an IoT system is more difficult than in a traditional network.[7]

This paper offers an overview of previous research on IoT security concerns and solutions. Security is becoming one of the most crucial problems surrounding IoT and technology in general as the number of "things" grows. The heterogeneous nature of IoT poses significant problems that must be overcome in order to fully fulfil the IoT's potential. Protecting consumer privacy, vital infrastructure, and websites from large-scale attacks requires securing networked IoT devices. The goal of this systematic research review is to give a thorough examination of the numerous research papers and methodologies utilised by researchers to safeguard IoT devices.[1]

Background

This section summarizes some of the important topics and phrases used in this article in a concise manner. Each section of the paper describes the necessary topics; nonetheless, we believe that this section will assist readers in better understanding and comprehending the content in the article.

IoT Security Challenges

The Internet of Things architecture is made up of three layers: a perception/hardware layer, a network/communication layer, and a layer of interfaces/services. Hardware/devices, communication/messaging protocols, and interfaces/services are the components of an IoT system.

[*] Assistant Professor (Computer Science), SRP Government PG College, Bandikui, Dausa, Rajasthan, India.

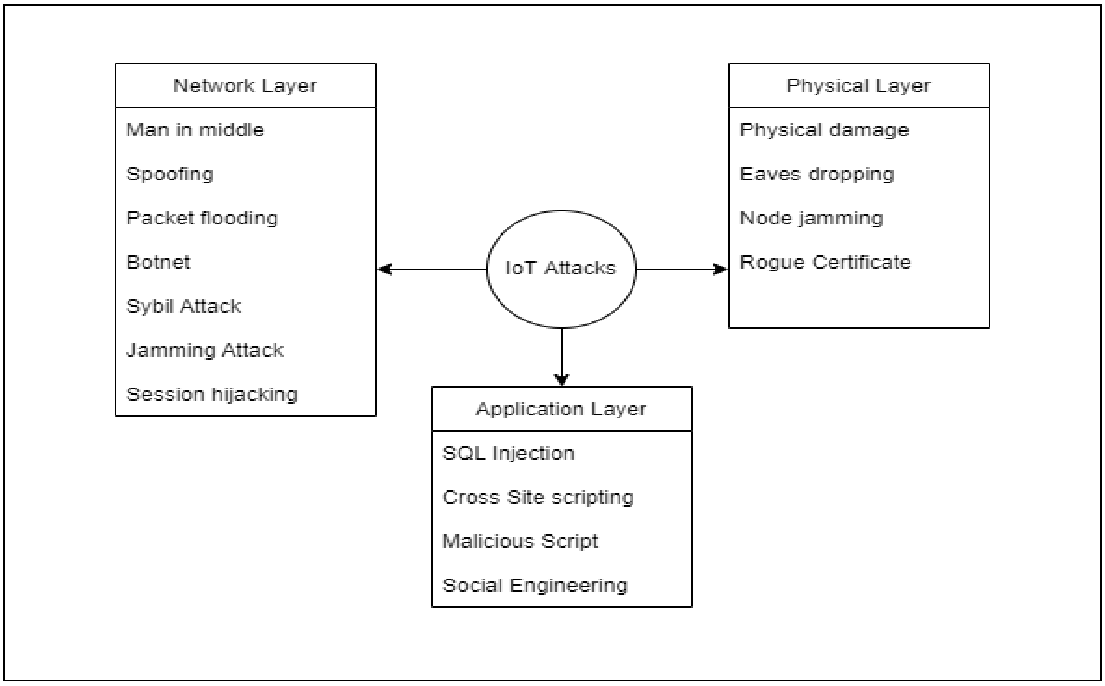

Fig.1: Possible IoT Attacks

- **Botnet Attacks**

A botnet is a collection of computers that can be controlled from afar. A hacker or a piece of command-and-control software produced by them controls all computers in a botnet remotely. In 2016, the "Mirai" botnet attack, one of the most well-known large-scale IoT botnet attacks, rendered high-profile websites such as Twitter, the New York Times, GitHub, Netflix, and others inaccessible.

- **Packet Flooding Attack**

These attacks occur as internet-facing hosts have no control over the packets they receive. The UDP flooding assault, in which UDP datagrams flood and congest the network [19], is an example of a flooding attack. ICMP flooding is another attack in which a constant stream of ping packets is broadcast to the target without waiting for a response, overloading network resources.

- **Ddos Attack**

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt a targeted server's, service's, or network's normal traffic by flooding the target or its surrounding infrastructure with Internet traffic. This type of attack tries to clog up the Internet by absorbing all available bandwidth between the target and the rest of the world.

- **SQL Injection**

One of the most prevalent web attack tactics used by attackers to steal sensitive data from organisations is SQL injection. SQL injection (SQLi) is a technique for manipulating SQL code in order to get access to restricted resources, such as sensitive data, or to execute malicious SQL commands.

- **Sybil Attack**

A Sybil Attack is a form of online security threat in which a person attempts to seize control of the network by creating several accounts, nodes, or computers. Sybil attacks are used to maliciously manipulate systems on the IoT.

- **Eavesdropping**

Eavesdropping is an unlawful real-time attack in which an attacker intercepts private communications such as phone calls, text messages, fax transmissions, or video conferences. It aims to steal data that is being sent via a network.

Literature Review

The goal of this study is to look into existing and suggested solutions for securing IoT systems. To assist the aforesaid investigation, the following research question has been established.

RQ1: What are the most significant security issues that make IoT devices vulnerable to adversary attacks?

RQ2: What are the various ways for securing IoT systems?

A survey of IoT architectural concerns and security vulnerabilities was conducted by Burhan M et al.[2] They highlighted IoT architectural issues and associated solutions, with one of their main concerns being security and privacy. They discussed security vulnerabilities based on layers that can impair IoT performance and recommended a new six-layer layered architecture to secure the IoT infrastructure.

Al-Garadi et al. presented a number of issues, difficulties, and future possibilities for employing machine learning and deep learning to address security flaws. Data-driven IoT systems, learning methodologies, IoT contexts, intrinsic ML and DL challenges, potential to connect ML/DL with other technology, computational complexity difficulties, and security vs. other trade-off requirements are all discussed[1]

Ahmad Khan et al. [3] discuss how blockchain, the underlying technology for bitcoin, can be a crucial facilitator in addressing numerous IoT security issues. In addition, the article addresses open research concerns and difficulties in the field of IoT security. . For the low-level, intermediate-level below transport layer, intermediate-level involving transport layer, and high-level security threats, a comparative study of the dangers and their viable remedies is provided.

Potential Security Solutions

This section provides an overview of the major security solutions offered in the literature.

- Machine and deep learning techniques are well-known AI techniques that can assist IoT devices in learning from their experiences, which are represented as data, and acting appropriately. Learning models are often made up of a set of rules, procedures, or sophisticated 'transfer functions' that can be used to identify and anticipate behaviour in IoT data, as well as find pertinent security incident trends [4].
- A novel Chinese Remainder Theorem based Reversible Sketch (CRT-RS) is proposed for detecting DDoS flooding attacks. CRT-RS is capable of not only compressing and fusing large amounts of network traffic, but also of detecting abnormal keys in the reverse direction. [5].
- Blockchain smart contracts can offer decentralised authentication rules and logic to an IoT device, allowing for single and multi-party authentication. Furthermore, data privacy can be protected using smart contracts, which define the access rules, circumstances, and timeframes that allow a specific person or group of users or machines to own, control, or access data in transit or at rest.[3]
- In this paper, a trust-based authentication and encryption approach called Counter with Cipher Block Chaining-Message Authentication Code (CCM) is suggested. The attack detection probability is used to estimate each device's trust value, and the token expiration time is calculated in terms of each sender's trust value[9].

Open Challenges and Future Research Directions

Future research opportunities and directions in the topic of IoT security include the following:

- Collecting security data in the IoT environment is difficult. Because of the dynamic aspects of IoT, such as heterogeneity, vast amounts of data can be generated at a high frequency from many domains. To allow further inquiry, it is necessary to collect and manage relevant IoT-generated data for target applications, such as security in smart city applications. As a result, a more in-depth review of data collection methods is required when working with IoT-generated data.[8]
- In terms of data storage, computing, data processing, and decision-making, as well as communication resources, there should be a trade-off between security and device capabilities. As a result, a thorough analysis is required to determine the best machine or deep learning methods.

- Proposing new lightweight solutions for IoT devices that take current data patterns into account, and eventually constructing a recency-based IoT security model, is another significant task.
- As low-cost, low-power devices become more common, the IoT architecture may become more vulnerable to hardware flaws. It's not just about physical failure; the implementation of security algorithms in hardware, as well as routing and packet processing methods, must all be tested before IoT deployment.

Conclusion

Because of the variety of devices and communication protocols used in IoT systems, as well as the many interfaces and services available, typical IT network solutions are not ideal for implementing security mitigation. IoT devices nowadays are unsecure and unable to defend themselves. This is due to a lack of secure hardware and software design, development, and deployment in IoT devices, as well as limited resources in IoT devices, immature standards, and the lack of secure hardware and software design, development, and deployment. Due to the diversity of resources in IoT, efforts to define a robust global strategy for protecting the IoT layers are also hampered.

We surveyed and reviewed key IoT security challenges in this study. We review the strategies proposed in the literature for exploiting IoT security in a concise manner. In order to create reliable, efficient, and scalable IoT security solutions, the article also highlights and identifies future and open research concerns and difficulties that must be addressed by the research community.

This survey aims to provide a useful manual that can encourage researchers to advance the security of IoT systems from simply enabling secure communication among IoT components to developing intelligent end-to-end IoT security based approaches.

References

1. M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani.(2020). A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685. https://doi.org /10.1109/COMST.2020.2988293.
2. Burhan M, Rehman RA, Khan B, Kim B-S(2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors*. 18(9):2796. https://doi.org/10.3390/s18092796
3. Minhaj Ahmad Khan, Khaled Salah (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems,Volume 82. 395-411 https://doi.org/10.1016/j.future.2017.11.022.
4. Nadia Chaabouni, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, and Parvez Faruki. Network intrusion detection for iot security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3):2671–2701, 2019.
5. Xuyang Jing, Zheng Yan, Xueqin Jiang, and Witold Pedrycz. Network traffic fusion and analysis against ddos flooding attacks with a novel reversible sketch. Information Fusion, 51:100–113, 2019.
6. Doshi R, Apthorpe N, Feamster N (2018) Machine learning ddos detection for consumer internet of things devices. In: 2018 IEEE security and privacy workshops (SPW). IEEE, pp 29–35
7. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 29(7):1645–1660
8. Rajmohan, T., Nguyen, P.H. & Ferry, N. A decade of research on patterns and architectures for IoT security. *Cybersecurity* **5,** 2 (2022). https://doi.org/10.1186/s42400-021-00104-7
9. Sudhakaran, P, C, M. Energy efficient distributed lightweight authentication and encryption technique for IoT security. *Int J Commun Syst*. 2022; 35 (2):e4198. https://doi.org/10.1002/dac.4198.

❑❑❑