Detecting and Preventing DoS Attacks Within IoT Environment Using AWS IoT Core

M. Nimavat Dhaval[1,2(✉)] and G. Raiyani Ashwin[3]

[1] RK University, Rajkot, India
dhaval.nimavat26730@paruluniversity.com
[2] Parul University, Vadodara, India
[3] Nirma University, Ahmedabad, India
ashwin.raiyani@nirmauni.ac.in

Abstract. Detecting and preventing cyber attacks within an IoT (Internet of Things) environment by AWS MQTT (Message Queuing Telemetry Transport) Broker involves implementing various security measures and best practices. MQTT preferred as lightweight messaging protocol commonly utilized in IoT applications for efficient communication between IoT devices and various cloud services. AWS IoT Core provides an MQTT broker service that allows secure communication between IoT devices and cloud resources. Detecting and preventing Denial of Service (DoS) attacks within an IoT environment using AWS MQTT Broker involves a combination of security measures and services provided by AWS. In this research paper, we studied a couple of cyber attacks, tools, and also demonstrated strategies and tactics to protect the AWS IoT Core environment in which we had implemented and configured custom digital certificate and policy from DoS attacks using various python scripts.

Keywords: IoT · Security · Types of Cyber Attack · DoS Attack

1 Introduction to Cyber Attacks

In today's world, various activities, including economic, industrial, cultural, social, and governmental, are conducted online. Our global society heavily relies on wireless technology, making safeguarding data from cyber-attacks a challenging task. Cyber-attacks are primarily aimed at stealing sensitive credentials, but in some cases, they may have military or political motivations. These attacks can cause various damages, such as viruses, data breaches, Distributed Denial of Service (DDS) attacks, and other sophisticated attack vectors. As a result, many companies and organizations employ diverse solutions to mitigate the impact of cyber-attacks [1, 2].

A cyber attack within the IoT (Internet of Things) refers to a malicious act targeted at exploiting vulnerabilities within IoT devices, networks, or services. The IoT is a vast network of interconnected devices that can include smart home appliances, wearables, industrial machines, medical devices, and more. The interconnected nature of these devices, combined with potential security weaknesses, makes them susceptible to various cyber threats. Here are some major types of cyber attacks within the IoT [3, 4] (Fig. 1):

O. Castillo et al. (Eds.): PerSOM 2023, LNICST 517, pp. 75–88, 2024.
https://doi.org/10.1007/978-3-031-66044-3_5

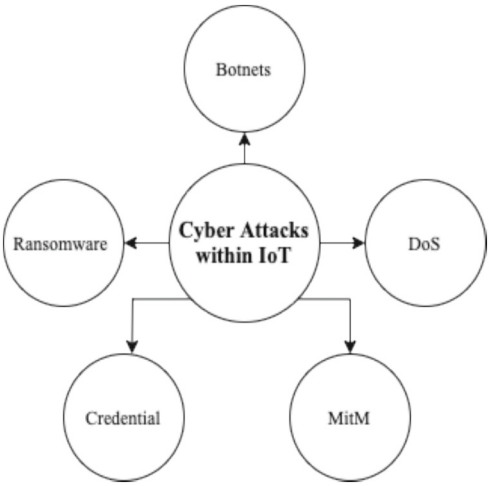

Fig. 1. Cyber Attacks within IoT

1.1 Botnets Attacks

A botnet attack in IoT (Internet of Things) refers to a cyber attack in which a network of compromised IoT devices is controlled by malicious actors to carry out various malicious activities. Botnets are groups of devices infected with malware and controlled remotely by a single entity, often referred to as the "botmaster" or "bot herder." These compromised devices, known as bots or zombies, are typically IoT devices with weak security measures [5].

1.2 DoS (Denial of Service) Attacks

A DoS (Denial of Service) attack in IoT (Internet of Things) involves flooding a network of interconnected devices with a massive amount of traffic or requests, overwhelming their resources and causing them to become unavailable to legitimate users. In the context of IoT, a DoS attack can interrupt the common functioning of IoT devices, leading to service outages and potential disruptions in various sectors where IoT devices are employed [6].

1.3 (MiM) Man-in-Middle Attacks

Man-in-Middle (MiM) attacks in IoT (Internet of Things) involve intercepting and potentially modifying the communication between IoT devices or between IoT devices and their central server. In a MitM attack, an unauthorized attacker positions themselves between the communicating parties and secretly relays or alters the messages passing between them, without the parties being aware of the intrusion [6, 7].

1.4 Credential Attacks

Credential attacks in IoT (Internet of Things) refer to cyber attacks that target the authentication credentials used by IoT devices, services, or users to gain unauthorized access to the system. These attacks focus on exploiting weak or stolen credentials, such as usernames and passwords, to compromise IoT devices or networks using brute force attack [6, 7].

1.5 Ransomware Attacks

A ransomware attack within IoT (Internet of Things) involves the deployment of ransomware on IoT devices to encrypt their data and demand a ransom from the device owner or the organization controlling the devices. Ransomware is a one of the type of malware that restricts access to a device or its data until a ransom is paid to the attacker, usually in cryptocurrencies, to obtain the decryption key and regain access to the locked data [6, 7].

1.6 Investigating Security Issues Related to Denial of Service (DoS) Attacks

To effectively investigate and mitigate DoS attacks, it's crucial to establish a baseline of normal network activity.

- Packets out and Bytes out: Unusually high levels of outgoing packets and bytes may indicate that your network is generating an excessive amount of traffic. This could be a sign of a DoS attack, as attackers often flood a target system with traffic to overwhelm it.
- Destination IP: Monitoring the destination IP addresses of incoming traffic can help you identify if there is an unusual concentration of traffic directed at a particular IP address. This could be a sign of a targeted attack.
- Listening TCP ports: An increase in the number of open TCP ports could indicate that services are being exploited, especially if these ports are not typically open. Attackers may be attempting to exploit vulnerabilities in open ports to launch an attack.
- Listening TCP port count: A sudden or significant increase in the number of listening TCP ports may be a sign of unwanted services running on your network. Such services could be exploited by attackers to facilitate a DoS attack.
- Listening UDP ports: Similar to TCP ports, a sudden increase in listening UDP ports may indicate unexpected or potentially vulnerable services. UDP-based DoS attacks are also possible, so monitoring these ports is essential.

Consider that despite the fact these indicators are useful, a more comprehensive security plan should include them. It's also critical to keep up with the most recent DoS attack methods and trends in order to can improve defensive measures appropriately.

2 Related Work

To address the security needs of an IoT system, various methods can be employed [8]. Among them, mutual authentication among the IoT device and the gateway within the resource-constrained environment of the IoT system is of utmost importance. In this

research paper, we propose enhancing security mechanisms using Amazon Web Services (AWS) Core Concepts and MQTT Broker as IoT Middleware. We introduce custom digital certification, private key, and custom policy to facilitate secure communication in the IoT environment. We also performed certain DoS attacks on local server like node-red (127.0.0.1) as well as our implemented IoT middleware model on AWS IoT Core to understand the impact of various DoS attacks [9–11].

2.1 Algorithm for Securing IoT Environment

Step 1: Connection with AWS IoT Core: Establish the connection between things (client or published or subscriber) to IoT core [9, 10] (Fig. 2).

```
"Version": "2023-05-17",
"Statement": [
        {
                "Effect": "Allow",
                "Action": "iot:Connect",
                "Resource": [
                        "arn:aws:iot:us-east-1:123456789012:RKU1/${iot:Connection.Thing.ThingName}"
                ]
        }
]
```

Fig. 2. Connection with AWS IoT Core

Step 2: Define Topic for IoT Devices : In order to transmit or receive message, Topic is essential to be created on cloud services (Fig. 3).

```
arn:aws:iot:aws-region:dhaval.nimavat:topic/Topic
```

Fig. 3. IoT Topic

Step 3: Implementing and assigning custom digital certificate to ensure authentication among IoT devices which includes own private key using OpenSSL (LibreSSL 2.8) (Figs. 4 and 5).

Step 4: Generate and define custom MQTT policy: AWS IoT Core policies are structured in JSON format, encompassing rules for establishing connections, message retention, message publishing, message receiving, and topic subscription. The custom policy on AWS, illustrated in the following figure [9–11] (Fig. 6).

Step 5: Assign certificate and policy to IoT Devices: In the context of AWS IoT, we had utilized Node-RED platform to implement and utilize digital signature and policy

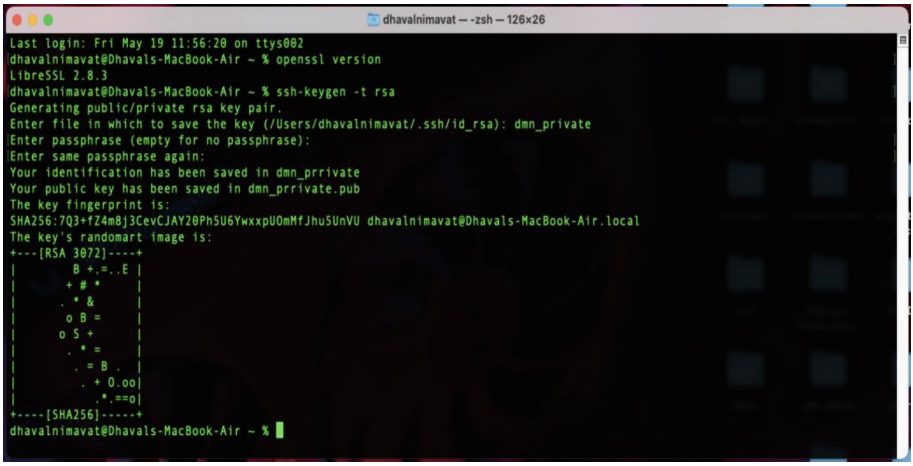

Fig. 4. Generated Private Key, OpenSSL

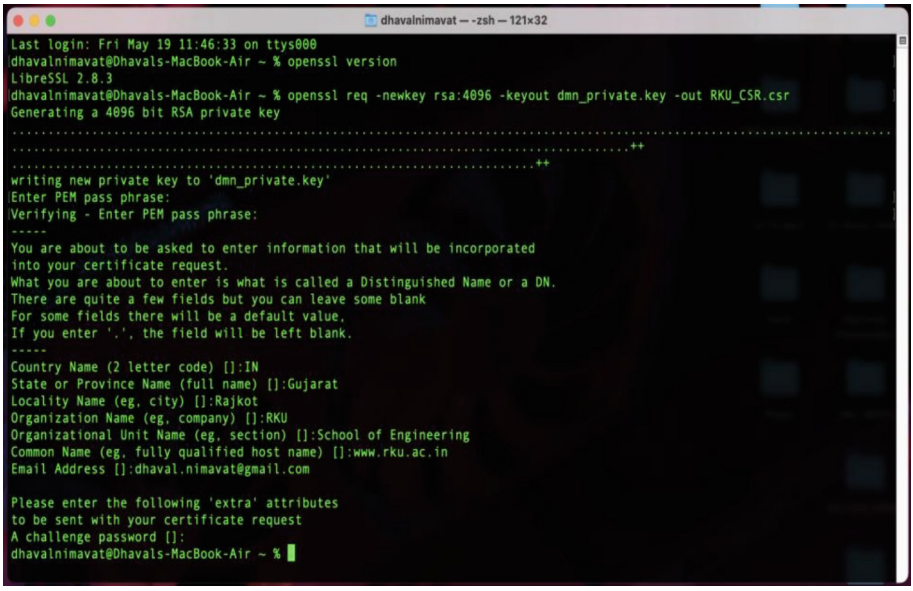

Fig. 5. Generated custom digital certificates using 4096 bit private key

techniques for a specific use case. Node-RED is a visual programming tool kit that allows users to design and deploy applications by connecting different nodes representing various services or functionalities. Within AWS IoT Environment, Node red architect can be employed to coordinate the required configurations for digital signatures and policies (Figs. 7, 8 and 9).

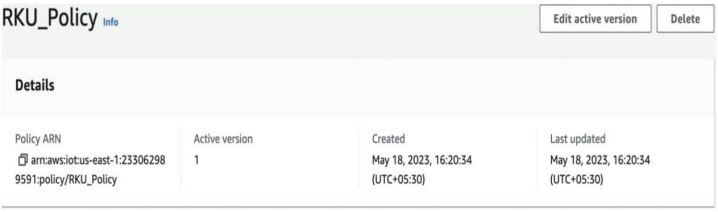

Fig. 6. Policy for IoT Devices

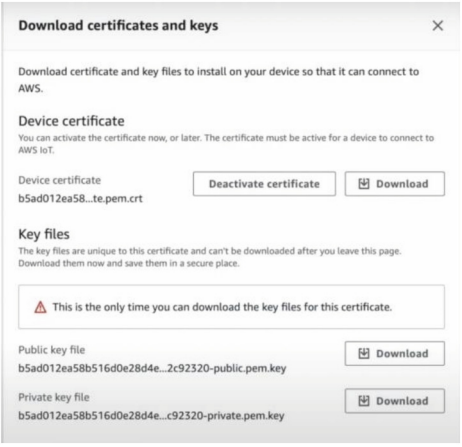

Fig. 7. Download certificate and private key

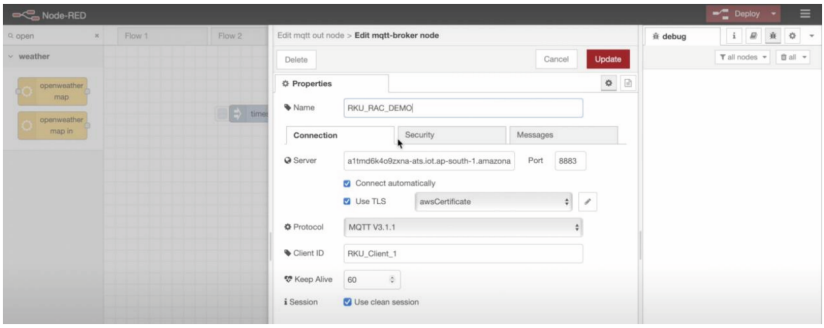

Fig. 8. MQTT Broker Configuration on Node-Red.

This case study involves utilizing the OpenWeatherAPI as the publisher and a subsciber running on https://127.0.0.1:1880. The implementation includes customized AWS IoT Core Concepts, utilizing the IoT Topic “MQTT/SensorData1”, a custom private key “dmn-private.key”, a generated digital certificate “RKU-CSR.csr”, and a policy named “RKU-Policy” [9–11].

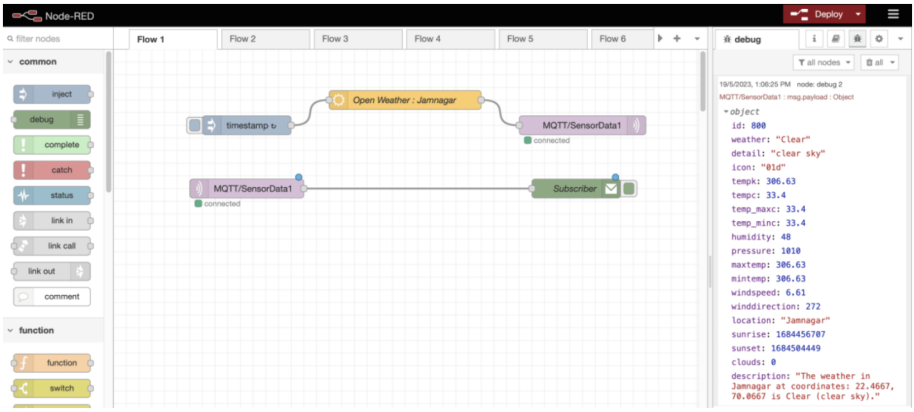

Fig. 9. Results of secured communication between pub (Open Weather API) and sub.

3 Results on DoS Attacks

In this research paper, we also find evidence of following assaults on the proposed AWS MQTT broker (Middleware Architecture) as well as the local server(Node-RED) and WiFi router. It is important to note that engaging in any form of cyber attack, including flood attacks, socket attacks, packet sniffing, or packet injection without explicit authorization is illegal and unethical. These attacks can cause significant harm to targeted systems and networks, and engaging in such activities may lead to serious legal consequences [4].

3.1 Flood Attack

A flood attack, also known as a denial-of-service (DoS) flood attack, aims to overwhelm a target system or network by sending a large volume of traffic or requests. The flood of traffic consumes the target's resources, causing service disruptions and making it unavailable to legitimate users. Here result of flood attacks shown in below figures to various local server, WIFI router and proposed middleware architecture [12, 13] (Figs. 10, 11 and 12).

3.2 Socket Attack

A socket attack involves targeting the communication channels known as sockets that are used to establish connections between devices or between a device and a server. In the context of attacks, it can refer to exploiting vulnerabilities in socket communication protocols to disrupt or manipulate data exchange. Here result of socket attacks shown in below figures to various local server, WIFI router and proposed middleware architecture [14] (Figs. 13, 14 and 15).

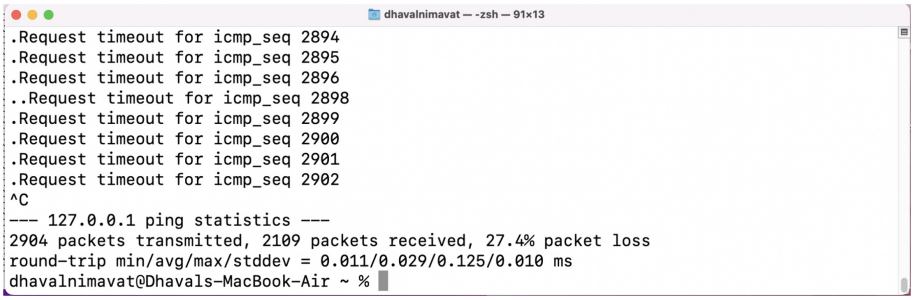

Fig. 10. Flood Attack on Node-Red 127.0.0.1

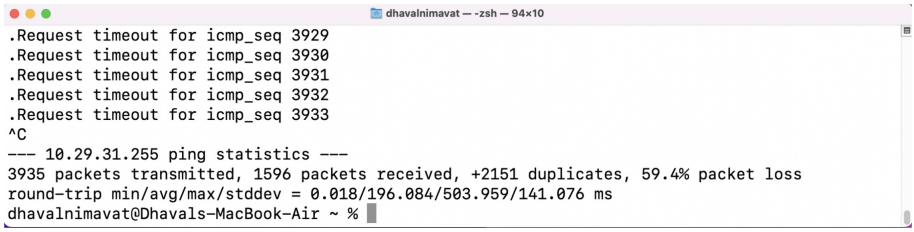

Fig. 11. Flood Attack on WIFI Router 10.29.31.25

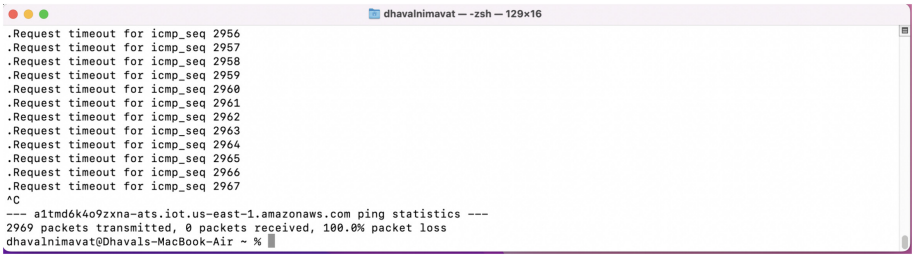

Fig. 12. Flood Attack on Proposed Middleware Architecture

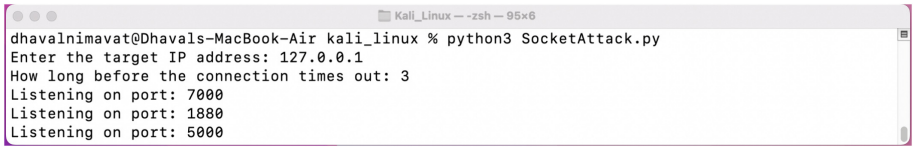

Fig. 13. Socket Attack on Node-Red 127.0.0.1

3.3 Packet Sniffing

Packet sniffing, also known as packet capturing, involves intercepting and monitoring network traffic to track and monitor the data packets that are transmitted over the network. This is often used for legitimate purposes like network troubleshooting, but it could also

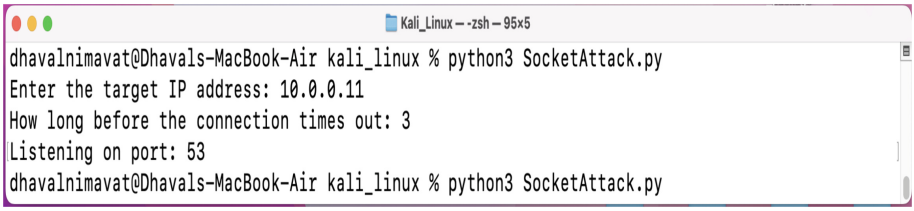

Fig. 14. Socket Attack on WIFI Router 10.29.31.25

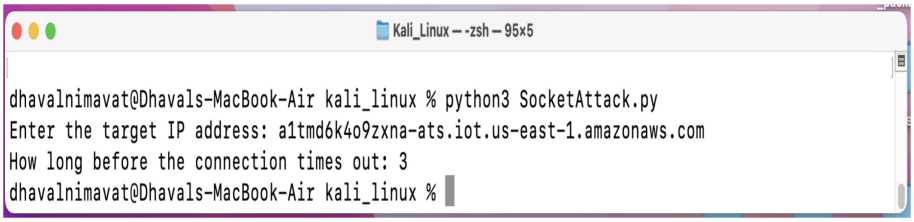

Fig. 15. Socket Attack on Proposed Middleware Architecture

be used maliciously to track sensitive information from the intercepted packets. Here result of packet sniffing attack shown in below figures to various local server, WIFI router [15] and proposed middleware architecture (Figs. 16, 17 and 18).

Fig. 16. Packet Sniffing Attack on Node-Red (127.0.0.1)

3.4 Packet Injection

Packet injection is a technique where an attacker sends forged or modified packets into a network to manipulate the communication between devices or disrupt network

Fig. 17. Packet Sniffing Attack on WIFI Router 10.29.31.25

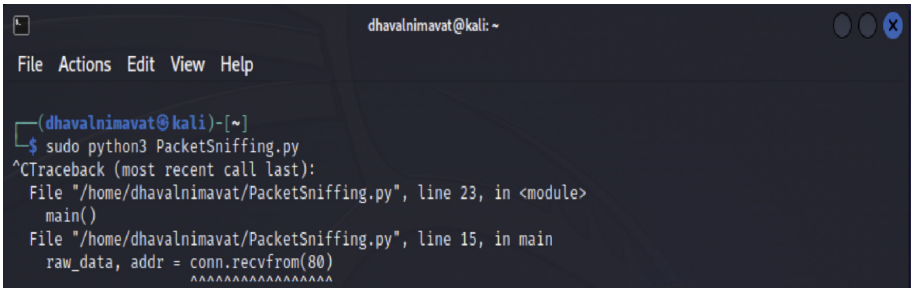

Fig. 18. Packet Sniffing Attack on Proposed Middleware Architecture

operations. This can be used for various purposes, such as inserting malicious data or altering legitimate traffic. Here result of packet inject attacks shown in below figures to various local server, WIFI router and proposed middleware architecture [16, 17] (Figs. 19, 20 and 21).

Fig. 19. Packet Inject Attack on Node-Red (127.0.0.1)

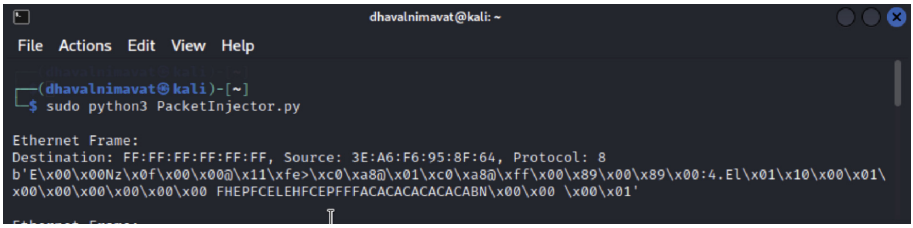

Fig. 20. Packet Inject Attack on WIFI Router 10.29.31.25

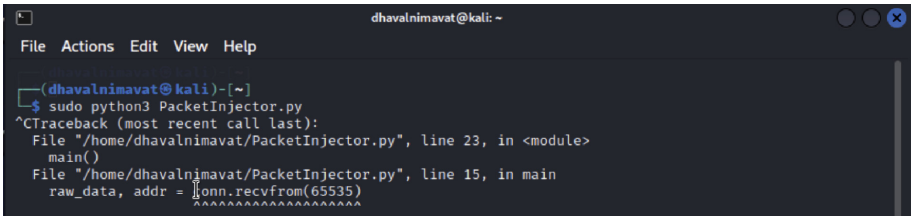

Fig. 21. Packet Inject Attack on Proposed Middleware Architecture

4 Impact of DoS Attacks

Cyber attacks on IoT (Internet of Things) can have far-reaching and severe impacts on individuals, organizations, and society as a whole. As IoT devices become increasingly integrated into various aspects of our lives, from smart homes and healthcare to industrial automation and critical infrastructure, the potential consequences of cyber attacks become more significant. A successful cyber attack on IoT devices can lead to privacy breaches and data manipulation. As these devices often collect and transmit sensitive personal data, attackers can feet vulnerabilities to get unauthorized access to personal information, location data, and other sensitive details. Moreover, manipulating the data collected by IoT devices can lead to inaccurate readings and misleading information, compromising decision-making processes in critical sectors. Below table describes the impact of DoS attacks such as flood, socket, packet sniffing and packet inject on various middleware architecture [18] (Table 1).

Table 1. Impact of Cyber Attacks on Middleware Architecture

Types of Attack	OS	Script	Packets	127.0.0.1	10.29.31.25	Proposed Middleware
Flood Attack	macOS	Python3	~3000	2109 Packet Received	1596 Packet Received	No Packet Received
Socket Attack	Kali-Linux	Python3	~3000	Found 3 Ports	Found 1 Ports	Port Not Found
Packet Sniffing Attack	Kali- Linux	Python3	–	Packets Observed	Packets Observed	No Packet Observed
Packet Injection Attack	Kali- Linux	Python3	–	Applied	Applied	Connection Aborted

5 Conclusion

In conclusion, detecting and preventing cyber attacks within an IoT environment using AWS MQTT Broker is of paramount importance to ensure the security and reliability of IoT systems. MQTT, being a lightweight messaging protocol, plays a crucial role in facilitating efficient communication among IoT devices and cloud services, making AWS IoT's MQTT broker service a valuable tool in this context. The research paper presented a comprehensive experimental results of different cyber attacks, tools, and demonstrated effective strategies and tactics to protect the AWS IoT Core environment. The implementation and configuration of custom digital certificates and policies were instrumental in fortifying the system against Denial of Service (DoS) attacks, which pose significant threats to IoT infrastructures. The combination of security measures and services provided by AWS is essential to safeguard IoT devices and cloud resources from potential threats. By employing proactive security practices, such as regular updates, network segmentation, authentication mechanisms, and continuous monitoring, organizations can significantly enhance the resilience of their IoT systems. As IoT technology continues to advance and become more ubiquitous, ensuring the security and integrity of IoT environments becomes increasingly crucial. The research and efforts dedicated to detecting and preventing cyber attacks within an IoT ecosystem will contribute significantly to creating a safer and more secure connected world. By staying vigilant and implementing best practices, stakeholders can mitigate the risks and potential damages caused by cyber attacks, ensuring the continued growth and advancement of the IoT landscape.

References

1. Sharma, A.K., Galav, R.K., Sharma, B.: A comprehensive survey of various cyber attacks. In: 2023 6th International Conference on Information Systems and Computer Networks (ISCON), pp. 1–4 (2023). https://doi.org/10.1109/ISCON57294.2023.10111998

2. Gururaj, H.L., Soundarya, B.C., Janhavi, V., Lakshmi, H., Prassan Kumar, M.J.: Analysis of cyber security attacks using kali Linux. In: IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics, ICDCECE 2022. Institute of Electrical and Electronics Engineers Inc. (2022). https://doi.org/10.1109/ICDCECE53908.2022.9793164
3. Kantimahanthi, S., Prasad, J.V.D., Chanamolu, S., Kommaraju, K.: Machine learning approaches in cyber attack detection and characterization in IoT enabled cyber-physical systems. In: 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), pp. 136–142 (2023). https://doi.org/10.1109/IDCIoT56793.2023.10053545
4. Lu, K.-D., Wu, Z.-G., Huang, T.: Differential evolution-based three stage dynamic cyber-attack of cyber-physical power systems. IEEE/ASME Trans. Mechatron. **28**(2), 1137–1148 (2023). https://doi.org/10.1109/TMECH.2022.3214314
5. Potrino, G., de Rango, F., Santamaria, A.F.: Modeling and evaluation of a new IoT security system for mitigating DoS attacks to the MQTT broker. In: 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6 (2019). https://doi.org/10.1109/WCNC.2019.8885553
6. Rao, G.S., Harshitha, M., Joshitha, V.R., Sravya, S.S., Priya, M.V.: DoS attack detection in wireless sensor networks (WSN) using hybrid machine learning model. In: 2023 10th International Conference on Signal Processing and Integrated Networks (SPIN), pp. 384–388 (2023). https://doi.org/10.1109/SPIN57001.2023.10117098
7. Wiranata, A., Karna, N., Irawan, A., Prakoso, I.A.: Implementation and analysis of network security in Raspberry Pi against DOS attack with HIPS snort. In: 2023 International Conference on Computer Science, Information Technology and Engineering (ICCoSITE), pp. 892–896 (2023). https://doi.org/10.1109/ICCoSITE57641.2023.10127741
8. Vachhani, S., Nimavat, D., Kalyani, F.: A comparitive analysis of different algorithms used in IoT based smart car parking systems (2020)
9. Nimavat, D.M.: Enhanced security by using AWS MQTT broker as middleware architecture for IoT environment section a-research paper enhanced security by using AWS MQTT broker as middleware architecture for IoT environment 1
10. Dhaval, N., Ashwin, R.: Study on security issues and threats for MQTT with IoT paradigm. www.rku.ac.in
11. Nimavat Dhaval, M., Raiyani Ashwin, G.: A study on MQTT protocol architecture and security aspects within IoT paradigm. In: Balas, V.E., Semwal, V.B., Khandare, A. (eds.) Intelligent Computing and Networking: Proceedings of IC-ICN 2022, pp. 61–72. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-0071-8_6
12. Patil, P.S., Deshpande, S.L., Hukkeri, G.S., Goudar, R.H., Siddarkar, P.: Prediction of DDoS flooding attack using machine learning models. In: 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), pp. 1–6 (2022). https://doi.org/10.1109/ICSTCEE56972.2022.10100083
13. Liu, B., Yao, X., Guo, K., Zhu, P.: Consortium blockchain based lightweight message authentication and auditing in smart home. IEEE Access **11**, 68473–68485 (2023). https://doi.org/10.1109/ACCESS.2023.3293401
14. Liu, T., et al.: MagBackdoor: beware of your loudspeaker as a backdoor for magnetic injection attacks. In: 2023 IEEE Symposium on Security and Privacy (SP), pp. 3416–3431 (2023). https://doi.org/10.1109/SP46215.2023.10179364
15. Manikanta Narayana, D.S., Bharadwaj Nookala, S., Chopra, S., Shanmugam, U.: An adaptive threat defence mechanism through self defending network to prevent Hijacking in WiFi network. In: 2023 International Conference on Advances in Electronics, Communication, Computing and Intelligent Information Systems (ICAECIS), pp. 133–138 (2023). https://doi.org/10.1109/ICAECIS58353.2023.10170470

16. Shinde, S., Mehta, H.: Defending marine ships against ethernet based cyberattacks. In: 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1–5 (2023). https://doi.org/10.1109/ICECCT56650.2023.10179830
17. Khalid, W., Ahmad, N., Khan, S., Saquib, N.U., Arshad, M., Shahwar, D.: FAPMIC: fake packet and selective packet drops attacks mitigation by merkle hash tree in intermittently connected networks. IEEE Access **11**, 4549–4573 (2023). https://doi.org/10.1109/ACCESS.2023.3235900
18. Siriyapuraju, S.J., Gowri, V.S., Balla, S., Vanika, M.K., Gandhi, A.: DoS and DDoS attack detection using mathematical and entropy methods. In: 2023 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing (PCEMS), pp. 1–6 (2023). https://doi.org/10.1109/PCEMS58491.2023.10136042