iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** V **Month of publication:** May 2021

DOI: https://doi.org/10.22214/ijraset.2021.34179

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

Prevention and Mitigation of Attacks on MQTT

Neenu Kuriakose[1], Lincy N L[2], Haritha Rajeev[3]
[1, 2, 3]*Research Scholar- Asst: Professor CS Dept- Asst. Professor CS Dept., St Paul's College Kalamassery -Kesari Arts &science College Paravur*

Abstract: ***The Internet of Things (IoT) is ready to transform the quality of life and offer new business opportunities with a variety of its applications. However, the benefits of this emerging paradigm go hand in hand with major cyber security issues. Lack of robust cyber security measures to protect IoT systems can lead to cyber-attacks targeting all levels of IoT infrastructure including IoT devices, IoT communication agreements and services that access IoT data. Various IoT malware such as Mirai, BASHLITE and BrickBot show attacks already based on IoT devices and the use of infected IoT devices to launch other cyber-attacks. However, as the ongoing deployment and operation of IoT depends largely on the implementation of effective data communication protocols, attacks on other layers of IoT construction are expected to increase. In the IoT country, the rule of publish / - subscribe based Message Queuing Telemetry Transport (MQTT) is very popular. Therefore, cyber security threats to the MQTT protocol are expected to grow in proportion to its increasing use by IoT manufacturers. The purpose of this paper is to explore and understand how security violations can be prevented and reduced in the MQTT protocol to increase its overall safety.***

Keywords: MQTT, Fuzzing, Machine Learning, DoS, DDoS

I. INTRODUCTION

Internet of Things (IoT) is a system that uses the Internet to connect smart devices and allow them to communicate, and is often used in education, business and the general public [1]. Io has grown rapidly and as a result has become part of daily life. For devices to connect and communicate, standards such as the Message Queuing Telemetry transport (MQTT) protocol can be made [1, 2]. Unfortunately, security breaches within IoT and MQTT are common [3, 4] and can lead to privacy violations. For this reason, it is important to obtain in-depth information on the various methods that can be used within the MQTT protocol to prevent and reduce security breaches.

II. INTERNET OF THINGS

In the late 90s, Kevin Ashton, director of AUTO-ID at the Massachusetts Institute of Technology (MIT), coined the name Internet of Things (IoT) [5]. Ashton explained that he wanted a program "that empowers computers through their data collection methods, so that they can see, hear and smell the world themselves, in all its random glory", in other words, IoT can be used to connect the physical world to the digital world via the Internet [5]. As of today, IoT is still evolving as more and more devices use the system [6]. The term "material" on the Internet of Things can be applied to all types of devices that can be used in everyday life while the term "internet" refers to wireless internet connection [7].

The main purpose of IoT is to connect multiple devices to each other and this can be done with the help of various technologies, such as: Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN) and Cloud Computing [6]. With IoT, people should be able to access and control their devices anytime and anywhere they want as long as they are connected to the internet [3]. For example, in a smart home, IoT devices can be used to control temperature and light.

III. MQTT PROTOCOL

The Message Queuing Telemetry Transport (MQTT) is a standard protocol developed in the late 90's by Arlen Nipper and Andy Stanford [9]. It is designed to improve communication between smart devices that use IoT and is used as a messaging protocol [9, 10]. In order to communicate this between IoT devices, MQTT is used in addition to IoT Transport Control Proto-col (TCP).

In addition, the MQTT protocol is particularly useful for devices with networks that are considered reliable and have low bandwidths. The MQTT protocol, since 2021, has been a relatively new protocol but has become one of the most widely used messaging methods worldwide, for example, MQTT protocols are used on websites like Facebook that allow its users to communicate [4, 11].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

IV. SECURITY BREACHES AND SECURITY MEASURES

This section examines the different attacks that occur within the MQTT protocol. These attacks are Brute force Authentication, Denial of service, SlowITe and Distributed Denial of service.

A. Brute Force Authentication

Brute Force Authentication (BTA) attack aimed at verifying the sys-tem of the MQTT vendor. Its main purpose is to find legitimate users, such as their username and password. Obtaining these credentials, for example, a violent power-up attack, is used to try as many combi-password countries as possible until the correct password is found. Once the correct password is found, the attacker can access IoT services.

B. Denial of Service

One of the most common security breaches within IoT and MQTT is called Denial of Service attack (DoS). This attack works by making actual users of the services unable to use them. This is done by creating interruptions for example, network bandwidth, which results in preventing legitimate users from accessing the service provided by the MQTT protocol. This disruption is often caused by bringing in attack packs.

Packages are data sets and are used to deliver messages between the publisher and the MQTT protocol registrar. However, once the MQTT protocol has been complied with, the attack packets will be replaced instead.

Attack packets are packages sent from illegal sources and their main function is to extract available resources and, thus, capture the official user from the service.

This is because an increasing number of packets, both valid and invasive, will overload traffic to and from the seller, which will create confusion as to which packets are actually valid and which packets are attack packets.

Another type of attack that can be used to identify the MQTT protocol is SlowITe which is considered a DoS attack in the novel. The main function of SlowITe is to keep all the connections, to and from the vendor, available simultaneously by building as many connections as possible.

The reason for the exe SlowITe attack is to eliminate the availability of MQTT vendor by making it too busy which will make it less efficient. The main difference between a standard DoS attack with SlowITe is that SlowITe detection does not require a lot of resources to be performed.

C. Distributed Denial of Service

A Distributed Denial of Service (DDoS) attack, an attack that identifies a system by sending attack packets from various sources, which acts similarly to the DoS by denying the user himself that he can use the services.

The difference between Dos and DDoS is that bad packets do not come from the same source but contain multiple sources at the same time which will make it difficult to reduce because all these malicious resources need to be stopped simultaneously to reduce further attacks. In addition, a large number of frequency attack packets mean significant ove-rall disruption to the network.

V. PREVENTION AND MITIGATION METHOD

This section will describe three different strategies that can be used to prevent or reduce risks within the MQTT protocol.

A. Fuzzing

Fuzzing, also known as fuzz testing, was developed in the early 90s by Miller et al. [18] and more recently it has become the standard method for detecting various bugs and potential vulnerabilities within software programs such as IoT and MQTT [19, 20]. For example, Fuzzing was developed by Go-ogle to find bugs in its browser, Google Chrome, and over the past eight years have been able to find more than 16,000 bugs [20].

Confusion is created by bringing the converted data input into the system and monitoring the result, as shown in Figure 1. the malicious input system will crash[18].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

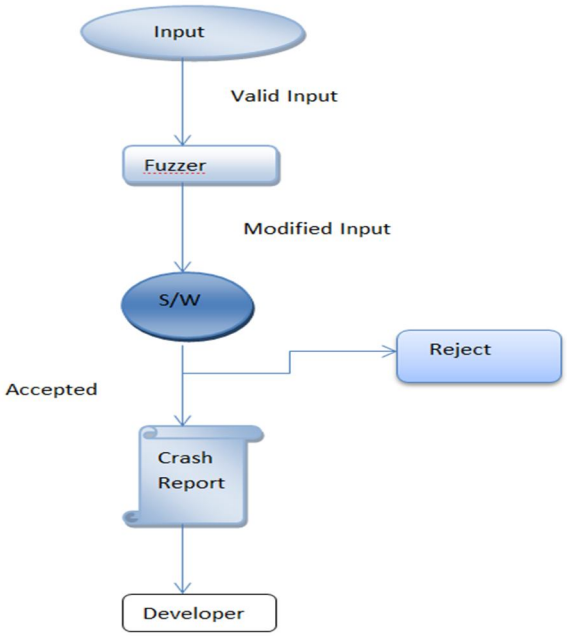


Figure 1: Fuzzing implementation

B. Fuzzy Logic

Fuzzy Logic presented by Zadeh et al. [15] and the basic premise of the opposite concept is to determine the category of the element. Fuzzy Logic is used to extend the use of Boolean (or crisp) values that can only be used to determine whether an item is true (1) or false (0). Fuzzy variables, however, are not limited to 0 or 1 and instead can take any value between 0 and 1, where 0 is completely false and 1 means absolutely true. In general, systemic fog systems are organized into three phases: Fuzzification, Fuzzing Disruption process, and Defuzzification [16]. The fuzzification phase is used to convert Boolean values into abstract variables. The Fuzzing pro-cess application uses IF-Then rules to determine the output value based on the input value. Finally in the defuzzification phase, the variable variable is converted back to the boolean variable. For safety, Fuzzy Logic can be used as a mitigation method because it can be used to determine whether nodes, for example in IoT or MQTT, are malicious or not [16,17].

C. Machine Learning

Another method that can be used to reduce potential attacks in areas such as MQTT protocols is Machine Learning algorithms. This approach trains the ability to identify potential attacks.

D. Prevention through Fuzzing

The word prevention, means means designed to detect vulnerability-lities prior to an attack. This means that an engineer can use appropriate methods to combat the risks identified before the system produces. This project proposes a lightweight intrusion detection system (IDS) acquisition system, labeled Fuzz-MQTT, which uses the Fuzzy Logic method to identify malicious initial interests in a MQTT vendor. This paper focuses on DoS attacks and how they interfere with message requests by keeping the merchant busy. The authors went on to explain that DoS attacks make it difficult for the seller to separate the standard CONNECT message packages (used by a client to request a contact with the seller) that are common to the unfamiliar ones. These requests are then approved by broker via CONNECTACK messages. For this reason, this paper focuses on capturing two types of messages.

Here, the input was the Connection Message Ratio (CMR), which describes a separate component of CONNECT messages for all messages received, and the Connection Ack-nowledgement Ratio (CAMR), which describes the number of customers actually connected. To make the analysis, these two inputs were first converted into a complex variable in the fuzzification phase, then the CMR in-put results and CMAR inputs were determined by IF-THEN rules, which they calculated by calculating statistics from actual traffic.

If something goes wrong, the seller will discard the packaging. Alternatively, standard packages are sent to the subscriber. Based on the flexibility of CMR and CAMR input, the fuzzy inference engine creates unambiguous rules in the form of IF-THEN statement. An example of the law is given as follows:

1) IF CMR = Low and CAMR = Low THEN anomaly = Normal
2) IF CMR = Low and CAMR = Medium THEN anomaly = Abnormal
3) IF CMR = High and CAMR = Medium THEN anomaly = Attack

Fuzzy logic can be very useful in terms of reducing the ongoing attacks on the MQTT protocol. This means that the use of Fuzzy Logic can help increase overall security in the MQTT protocol.

E. Mitigation Through Machine Learning

In this proposed project MQTT attacks have been identified with a tech-nique novel selection of firefly-based features and random forest, Decion tress methods and Naive bayes separation methods. The function also focuses on enable-based encoding.

Method	Accuracy	F1 score	Detection time
Decision tree	99.32	99.32	5.6
Naïve bayes	98.79	98	4.3
Random forest	99.8	100	2.37

Table 1.Performance Comparison of different classifiers

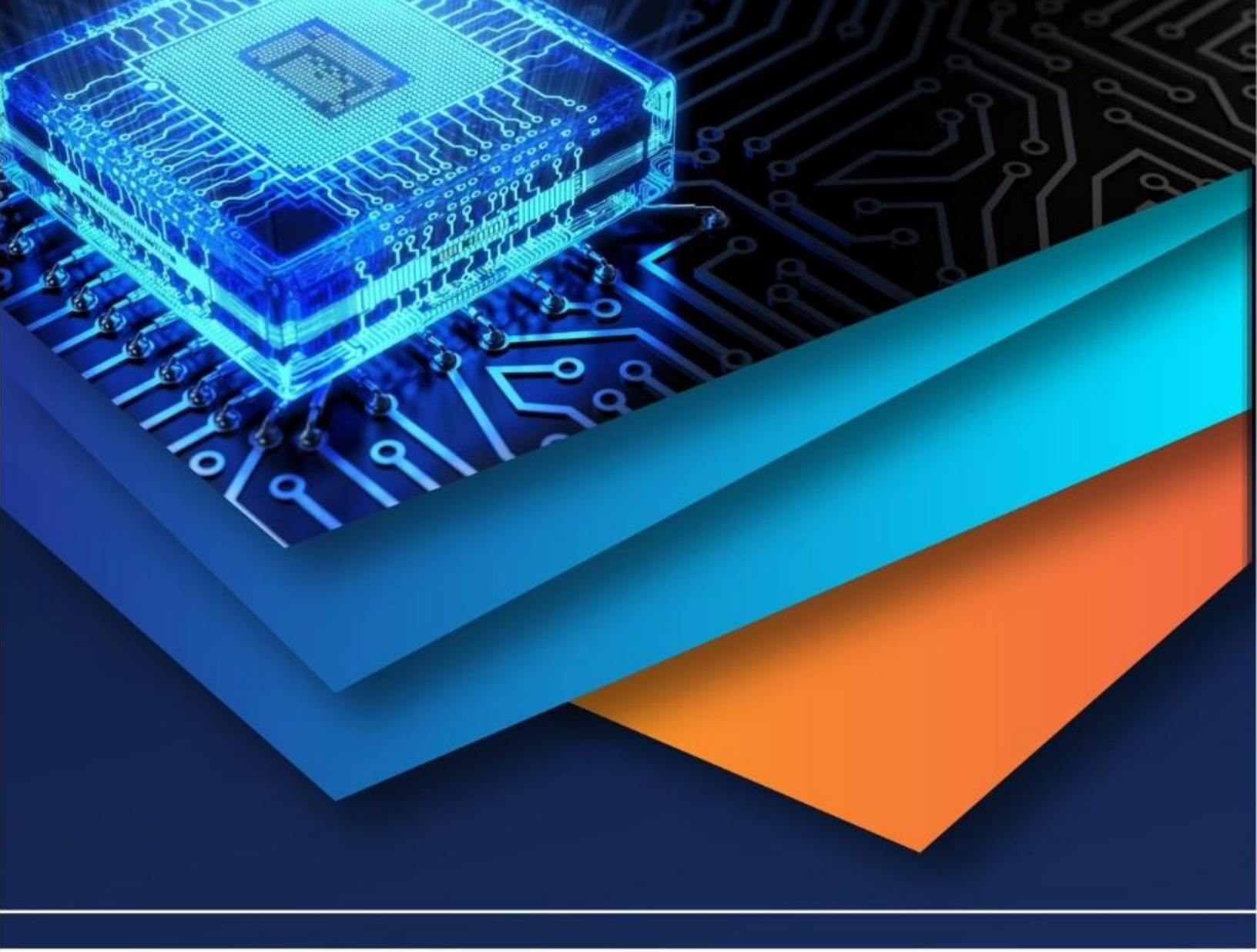
VI. CONCLUSION

Fuzzing is an excellent prevention strategy, which means that if an engineer wants to use a risk-taking approach by finding and repairing it while the MQTT protocol is still developing, Fuzzing can be a very good decision. The main advantage of demolition is that it can be used while the system is developing, which means that any vulnerabilities detected can be repaired before placing the system online. With regard to reducing further attacks on the MQTT protocol, the use of both Fuzzy Logic and Machine learning was found to be effective methods. This means that the implementation of Fuzzy Logic or Machine Learning can be good for detecting and responding to attacks that occur on the MQTT protocol while in operation.

REFERENCES

[1] Soni, U. S. & Talwekar, R. H.,” Internet of Things in Smart Grid: An Overview”, i-Manager's Journal on Communication Engineering and Systems, vol 8 (1), 2019, ss 28-36.
[2] Kashyap, M.; Sharma, V.; Gupta, N., “Taking MQTT and NodeMcu to IoT:Communication in Internet of Things”, Procedia Computer Science, vol 132, 2018, ss 1611-1618.
[3] Ali, B & Awad, I. A., “Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes”, Sensors (Basel), vol 18(3), 2018, ss 817.
[4] Casteur, G.; Aubaret, A.; Blondeau, B. ; Clouet. V.; Quemat, A.; Pical, V.; Zitouni, R., “Fuzzing attacks for vulnerability discovery within MQTT protocol”, 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020, ss 420-425.
[5] Ben-Daya. M.; Hassini. E.; Bahroun. Z.,” Internet of things and supply chain management: a literature review”, International Journal of Production Research, vol 57(3),2017, ss 1-24.
[6] Gawali, S. K. & Deshmukh, M. K., “Energy Autonomy in IoT Technologies”, Energy Procedia, vol 156, 2019, ss 222-226.
[7] Hussain, F.; Hussain, R.; Hassan, S. A.; Hossain, E., “Machine Learning in IoT Security: Current Solutions and Future Challenges”, IEEE Communications Service & Tutorials, vol 22(3), 2020, 1686-1721.
[8] Lee, S., Kim, G., Kim, S., “Sequence-order-independent network profiling for detecting application layer DDoS attacks”, J Wireless Com Network, vol 50, 2011.
[9] Mishra, B. & Kertesz, A., “The Use of MQTT in M2M and IoT Systems: A Survey” IEEE Access, vol 9, ss 201071-201086.
[10] Dinculeană, D. & Cheng. X., “Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices”, Applied Sciences, vol 9(5), 2019, ss 848.
[11] Hwang, H. C.; Park, J.; Shon, J. G., “Design and Implementation of Reliable Message Transmission System Based on MQTT Protocol İn IoT”, Wireless Pers Commun, vol 92(4), 2016, ss 1765-1777.
[12] Zeng, Y.; Lin, M.; Gue, S.; Shen, Y.; Cui, T.; Wu, T.; Zheng, Q.; Wang, Q.,“MultiFuzz: A Coverage-Based Multiparty-Protocol Fuzzer for IoT Publish/Subscribe Protocols”, Sensors (Basel), vol 20(18), 2020, ss 5194.
[13] Vaccari, I.; Chiola, G.; Aiello, M.; Mongelli, M.; Cambiaso, E., “MQTTset, a New Dataset for Machine Learning Techniques on MQTT”, Sensors, vol 20(22), 2020, 6578.
[14] Stiawan, D., Idris, M. Y., Firsandaya, M., Nurmainim S., Alsharif, N., Budiarto.,“Investigating Brute Force Attack Patterns in IoT Network”, Journal of Electrical and Computer Engineering, vol 2019, 2019, ss 1-13.
[15] Haripriya, A. P. & Kulothungan, K., “Secure-MQTT: an efficient fuzzy logic-basedapproach to detect DoS attack in MQTT protocol for internet of things”, EURASIP Journal on Wireless Communications and Networking, vol 90(2019), 2019.

[16] Alshehri, M. D. & Hussain, F. K., "A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT)" Computing, vol 101, 2019, ss 791-818.
[17] Hunkeler, U.; Truong, H. L.; Standford-Clark, A., "MQTT-S — A publish/subscribe protocol for Wireless Sensor Networks" 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE '08), 2008, ss 791-798.
[18] Liang, H., Pei, X., Jia, X., Shen, W., Zhang, J., "Fuzzing: State of the Art," in IEEE Transactions on Reliability, vol. 67(3), 2018, ss 1199-1218.
[19] Munea, T. L.; Luk-Kim, I.; Shon, T., "Design and Implementation of Fuzzing Framework Based on IoT Applications" Wireless Pers Commun, vol 93, 2017, ss 365-382.
[20] Boehme, M.; Cadar, C.; Roychoudhry, A., "Fuzzing: Challenges and Reflections", IEEE Software, 2020.
[21] Lincy N. L and Neenu Kuriakose, "A MACHINE LEARNING APPROACH TO DETECT BOTNET TRAFFIC", Int. j. innov. eng. res. technol., vol. 8, no. 05, pp. 61–63, May 2021



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY