Security of MQTT Protocol: A Brief Overview

Hayette Zeghida[1,*], Mehdi Boulaiche[1,†] and Ramdane Chikh[1,†]

[1] Dept. of Computer Science, LICUS Lab, Université 20 août 1955-Skikda, Algeria.

Abstract

The rapid evolution of the Internet of Things (IoT) technology has enabled the seamless connection of countless devices and sensors, allowing them to efficiently gather and transmit data to centralized networks. Currently, the number of devices connected to the Internet has surpassed the global human population, with projections indicating that this figure will likely double in the next few years. Despite this explosive growth, a unified global IoT framework is still lacking and no universal standards or protocols have been established to integrate the diverse components of the IoT ecosystem. Various communication protocols are in use today, with the Message Queuing Telemetry Transport (MQTT) protocol standing out as one of the most widely adopted. Designed specifically for sensor traffic on low-bandwidth and resource-limited networks, MQTT is highly suitable for supporting automated IoT systems. This paper delves into the structure and functionality of the MQTT protocol, offering a detailed analysis of potential attack vectors that could threaten its security. In addition, it reviews recent advancements in security solutions and relevant studies from the literature to provide a comprehensive understanding of MQTT's vulnerabilities and defenses. By building a solid knowledge base on MQTT security, the paper aims to be an invaluable resource for the current IoT community and future developers. Furthermore, the paper serves as a foundation for future research, helping streamline the process of identifying, selecting, and implementing appropriate security measures for MQTT in diverse IoT applications.

Keywords

Attack, Deep learning, Machine learning, MQTT, IoT.

1. Introduction

The rapid and significant increase in smart devices, encompassing everything from vehicles and household appliances to advanced healthcare gadgets and various industrial controllers, has spurred a remarkable development of numerous innovative internet of things solutions. These unique solutions typically rely on a low-cost, lightweight protocol that is designed specifically for efficient network communication, such as the widely used MATT. This protocol facilitates seamless communication among devices reliably and efficiently, which is essential for the proliferation of smart technologies.

The MQTT protocol was developed in the late 1990s by Andy Stanford-Clark of IBM and Arlen Nipper of Arcom (later acquired by Eurotech); the MQTT was introduced as an extension to commercial messaging systems. The Organization for the Advancement of Structured Information Standards (OASIS) developed the MQTT IoT standard, which was subsequently approved for release by both the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). MQTT 3.1.1 was approved by the ISO and IEC Joint Technical Committee on Information Technology (JTC1), receiving the designation "ISO/IEC 20922" [1], with MQTT 5.0 being the latest version [2].

The MQTT protocol operates with three main components: the publisher, the subscriber, and the broker (Figure 1). The publisher gathers data from various sources, such as sensors embedded in machinery, wearables, or mobile devices. Subscribers use mobile applications to subscribe to specific topics generated by the publisher (Figure 2). The broker serves as the central element of the MQTT protocol, acting as an intermediary between publishers and subscribers. It stores messages in the cloud and can handle the reception and transmission of multiple messages simultaneously [3].

TACC'2024, The 4th Tunisian-Algerian Conference on applied Computing, December 17-18, 2024, Constantine, Algeria

[*] Corresponding author.

[†] These authors contributed equally.

h.zeghida@univ-skikda.dz (H. Zeghida); boulaiche.mehdi@yahoo.fr (M. Boulaiche); r.chikh@univ-skikda.dz (R. Chikh)

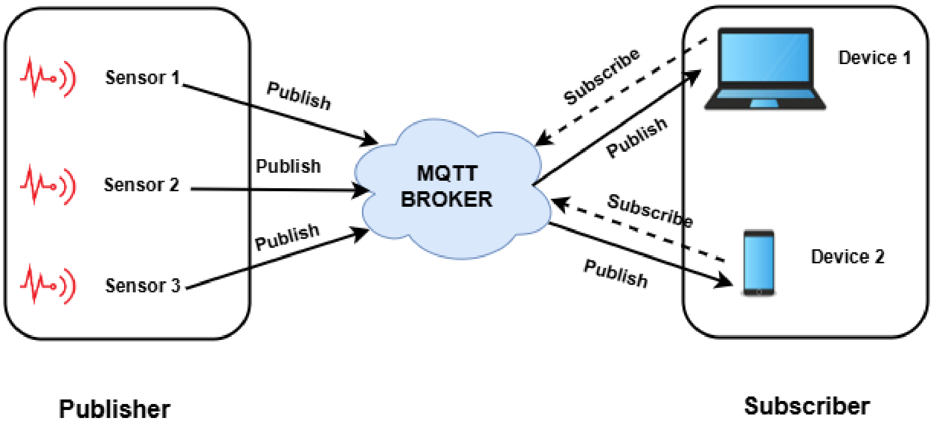

Figure 1: MQTT Architecture

The protocol includes a Quality of service (QoS) feature to ensure reliable message delivery from the publisher to the subscriber, offering three levels of QoS:

- Level 0: also known as ”at most once” delivery, the default option where the message is sent only once without guarantees.
- Level 1: or ”at least once” delivery, which provides basic delivery assurance with the option to resend if necessary.
- Level 2: or ”exactly once” delivery, where the message remains with the broker until it is confirmed to have been received by the subscriber.

Although the MQTT protocol provides significant advantages, it faces certain risks, including data leakage, message tampering, and forwarding vulnerabilities. Additionally, the broker is susceptible to well-known Denial of Service (DoS) attacks. As a result, it is essential to identify effective and efficient security measures to safeguard this protocol.

The remainder of the paper is organized as follows: Section II focuses on the use cases of MQTT protocol in IoT. Section III addresses Common Security Threats in the MQTT Protocol, while Section IV outlines the MQTT security enhancement measures. The paper concludes in Section V by highlighting future research opportunities.

2. Use Cases of MQTT protocol in IoT

Several IoT areas have benefited from and used the MQTT protocol’s characteristics in their operations. Kouicem et al. [3] summarized the following fields:

- Smart Healthcare: The introduction of intelligent sensors has made the healthcare system competent. The publisher uses the MQTT protocol to detect blood pressure, heart rate, EEG, and ECG and transmit the data to the subscriber.
- Smart Home: A smart home includes sensors, light, gas, temperature, and camera sensors. These sensors are all connected by microprogrammers, which gather data and transmit it to the homeowner via the MQTT protocol.
- Smart weather monitoring: Using the MQTT protocol, several sensors, including air pressure sensors, temperature sensors, humidity sensors, and sensors that measure wind speed and solar radiation, work together to deliver real-time weather data.
- Smart Parking: A user can rapidly ascertain whether or not the parking place is available using a smart parking system. Through the use of Radio Frequency IDentification (RFID) technology, he is provided with parking information. An RFID reader reads the tag and then broadcasts the information to the cloud via MQTT.

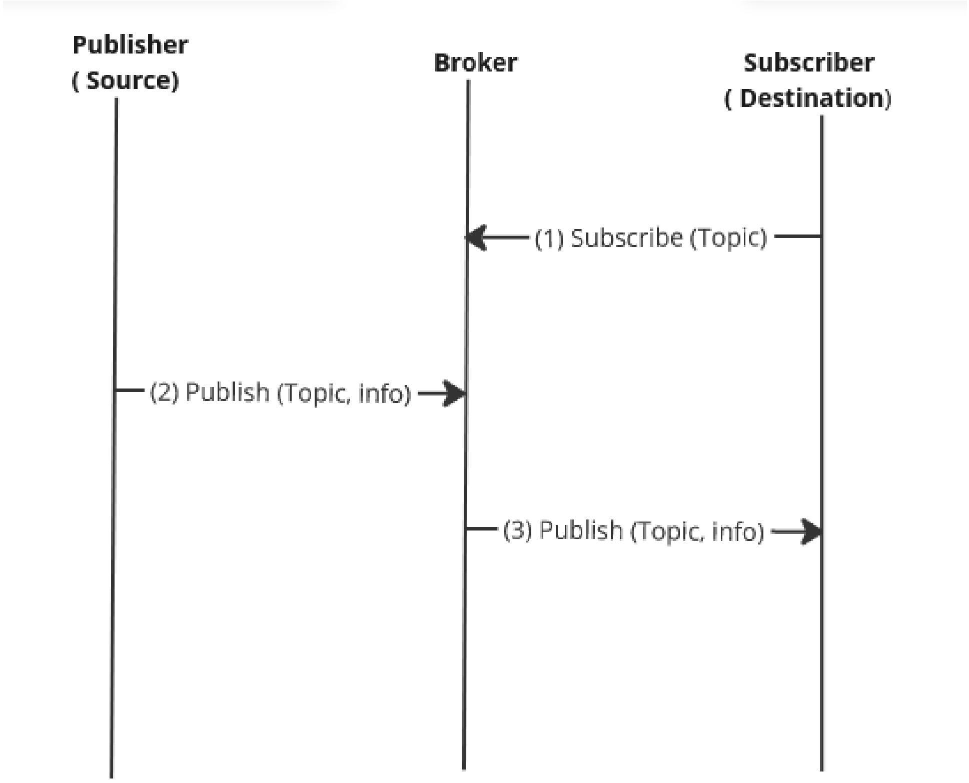

Figure 2: The MQTT publish/subscribe process

- Smart Industry: MQTT is essential to the smart industry because it enables direct machine-to-machine communication, which can reduce material requirements, speed up decision-making, as well as identify necessary items, which are some of today's industry's most pressing demands.

3. Common Security Threats in MQTT Protocol

In the rapidly evolving landscape of the IoT, the MQTT protocol stands out for its efficiency and simplicity in facilitating message exchange. MQTT clients typically communicate with brokers using TCP/IP (Transmission Control Protocol/Internet Protocol) port 1883 for unencrypted data exchanges, while port 8883 is reserved for encrypted communications via SSL/TLS (Secure Sockets Layer and Transport Layer Security) [17]. Despite the encryption option, the MQTT protocol remains vulnerable because developers focus on lightweight solutions and bandwidth usage rather than prioritizing security. This leaves the system exposed to various threats. Physical attacks, for instance, can disable IoT devices like mobile phones, routers, cameras, and sensors. Additionally, cyber-attacks may compromise wireless networks, allowing malicious actors to manipulate and jeopardize connected devices. This section explores the most critical attacks targeting the MQTT protocol.

- **Unauthorized Access :** Unauthorized access to MQTT installations poses a significant threat, as it can compromise the integrity of data exchanged between MQTT clients (publishers or subscribers) and brokers. Attackers can exploit weak credentials, insecure permissions, or web vulnerabilities to gain unauthorized access, allowing them to send or manipulate messages. Once compromised, attackers can interfere with the communication between MQTT brokers and clients, leading to data manipulation and compromised system integrity [19]. Many real-world incidents of unauthorized access to MQTT brokers are often caused by weak or leaked credentials, such as using default usernames and passwords like ”admin/admin123.” To prevent such attacks, strict security measures should be implemented.

- **Message tampering:** Message tampering poses a significant security threat in the MQTT protocol, where attackers alter message contents during transmission, leading to misinformation or unintended data leaks. This can destabilize devices and infrastructure and diminish trust in the system. Common techniques include IP/DNS (Internet Protocol/Domain Name System) spoofing, DHCP (Dynamic Host Configuration Protocol) starvation, and buffer overflow, resulting in message modification or delays. Attackers may manipulate messages on networks or within client/server applications. To counter this, integrity checks, encryption, and digital signatures are employed to ensure data integrity from origin to destination. These measures help detect tampering and secure end-to-end communication [21].
- **Denial of Service (DoS)**: Denial of Service (DoS) attacks aim to disrupt MQTT systems by depleting resources like connection handling or CPU (Central Processing Unit) capacity. Attackers can overload the server by creating excessive connections or repeatedly sending client authentication data, preventing legitimate connections and services.
  DoS attacks can be individual, where a single attacker sends numerous requests, or distributed, where compromised hosts across the Internet generate overwhelming traffic. The consequences include reduced system capacity, service failures, and potential cascading failures affecting the broader network [20]. In some cases, the attacker may use higher QoS levels along with large payloads to strain the broker's resources. For example, QoS level 2 requires the broker to store messages until they are successfully delivered, which can lead to resource depletion if messages fail to transmit [5]. Common DoS attacks include Mirai, flooding, and SlowITe [20].
- **Man-in-the-Middle:** One of the most deadly attacks, the attacker intercepts data transmitted between two connection points and tricks them into believing they are directly linked. Then, it may obtain and assess published data before editing and disseminating it to subscribers. The attacker may introduce messages containing remote control orders, such as ”RESTORE FACTORY SETTINGS” or ”OFF” directives to disable specific devices [6].
- **Brute Force attack:** This kind of attack lacks a clear plan and concentrates on trying every possible key to subscribe to the broker. A suitable key may be created by cleverly converting the ciphertext to plaintext. Although it takes a while, the attacker's full access to network resources breaches privacy and increases the chance that connected equipment may be damaged [7].
- **Ransomware:** Also called phishing. This type of attack often begins with an email asking recipients to perform some actions, including clicking on a malicious link or downloading a malicious file, to get sensitive information. The ransomware scams may also use text messages, phone calls, and social networking sites to deceive victims into supplying personal information. The Ransomware locks users out of their workstations or encrypts data after gaining user information like login passwords and credit card numbers. After that, the victim is prompted to hand over a ransom to end the siege on the device and the services it offers [8].

4. MQTT security enhancement measures

The MQTT protocol, a popular messaging system used in many networked environments, faces several security challenges. One of the main issues is the use of open network ports, which can be easily accessed and exploited by unauthorized users. Additionally, the protocol allows users to freely subscribe to and publish on any topic, creating opportunities for malicious activities. Another vulnerability arises from sending data in unencrypted, plain text format, making it easy for interceptors to access sensitive information. Moreover, many users often need to pay more attention to the importance of changing the default username and password provided by the factory, leaving their systems vulnerable to attacks. Implementing robust security measures, such as encryption using Secure Transport Layer (STL), is also hampered by the limited resources available in many MQTT environments. Recent research has focused on enhancing MQTT security to combat these vulnerabilities. These efforts primarily involve applying advanced Machine Learning (ML) and Deep Learning (DL) techniques. These methodologies offer promising solutions for detecting and mitigating security threats in MQTT systems, thus significantly improving their overall security posture. (Table 1) summarizes the strengths and weaknesses of contemporary studies.

Table 1: Comparison between strengths and weaknesses of some research papers about MQTT protocol.

Paper	Strengths	Weaknesses
Kim et al [9]	the paper provided a comprehensive review of IoT security threats and deep learning studies used in IoT security. In addition, it presented detailed experimental results to demonstrate the effectiveness of the proposed model.	The paper focused on detecting botnet attacks on IoT devices and did not address other attacks. As well as, the experimental results are based on a limited dataset, and it was unclear how well the proposed model would perform on larger or more diverse datasets.
Syed et al[10]	The paper provided valuable insights into the security challenges faced by IoT devices against DoS attacks. Additionally, The experimental results showed that the proposed framework can successfully detect DoS attacks in a physical IoT deployment, demonstrating its practical applicability.	The paper focused specifically on DoS attacks on the MQTT protocol but did not address other security threats that may affect IoT devices. Also, the proposed framework has yet to be compared with other approaches for detecting DoS attacks, which could help evaluate its effectiveness and performance.
Vaccari et al [11]	The introduction of a new dataset, MQTTset, which can be used to train machine learning models to detect security threats in MQTT networks. as well as the satisfactory results given in the proposed model showed that it can be used in the real world.	A more detailed analysis of the performance of the ML models trained on the MQTTset dataset is needed. Specifically, it lacks a comparative evaluation, where the results could be benchmarked against those from other studies focused on detecting security threats in the IoT networks.
Alaiz-Moreton et al [12]	the proposed IDS on the created dataset gave very satisfactory results, which indicated that the proposed models and techniques (XGBoost, LSTM, GRU) had the potential for real-world applications.	The paper did not provide a detailed analysis of the limitations and potential biases of the proposed datasets used in the research. Additionally, The proposed models and techniques differed from other existing approaches for detecting attacks on IoT systems, which could give more information about their effectiveness.
Mosaiyebzadeh et al [13]	The accuracy and F1-score that had been achieved demonstrated the effectiveness of the proposed approach. The authors shared their experiments on GitHub, which guarantees the reproducibility of the research and allows other researchers to build upon their work.	The paper should have compared the proposed approach with other state-of-the-art IDS approaches for IoT networks, which may limit the readers' ability to assess the novelty and competitiveness of the proposed approach. In addition, The paper did not discuss potential limitations or challenges in deploying the proposed IDS in real-world IoT networks, such as scalability, robustness to adversarial attacks, or privacy concerns.

Continued on the next page

Paper	Strengths	Weaknesses
Hindy et al [14]	Creating a fresh IoT-MQTT dataset and making it available to the public, allowing other academics to utilize it to investigate the issues of IoT intrusion detection further. The research emphasized the significance of leveraging flow-based characteristics to distinguish MQTT-based attacks from benign traffic, which has practical implications for developing successful IDS in IoT networks.	The authors used a simulated dataset for their model evaluation, which may need to capture the complexity and variability of real-world IoT traffic fully. In addition, The paper did not compare the performance of the proposed model with other existing models, which could provide valuable insights into the effectiveness of the proposed approach.
Zeghida et al [15]	the ensemble learning techniques demonstrated excellent results compared to single learning strategies. Also, processing data to have balanced data is essential for better outcomes.	The proposed method was applied only to the MQTT protocol, and it was unclear whether this method could be used for other types of IoT protocols.
Dewantaz et al[16]	The SibProMQTT scheme is designed to be lightweight and efficient, making it suitable for IoT devices with low computational resources. The experimental results showed minimal computational cost addition, making it a practical solution for IoT systems.	Focus on Sybil attacks in MQTT protocols without addressing other IoT security issues and the lack of comparative analysis with other MQTT security solutions. Furthermore, there was a restriction to a few devices in the experimental step, potentially not reflecting larger IoT systems.
Zeghida et al [17]	Provided an in-depth analysis of MQTT protocol vulnerabilities, and created a novel approach using DL techniques to develop a hybrid DL intrusion detection system for MQTT-based systems and demonstrated the superiority of this approach over traditional ML methods.	The work Focused on identifying a singular category of IoT attacks while disregarding alternative potential threats and restricting the comparison of results to a solitary study rather than incorporating multiple relevant works.
Im, Y., & Lim, M. [18]	Introduced a new mechanism that tackles the issue of end-to-end communication in MQTT by incorporating request-response patterns to facilitate direct communication between a publisher and subscribers and including experiments to benchmark its performance against standard MQTT. The experimental findings consistently indicated that E-MQTT surpasses traditional MQTT in terms of delay.	The experiments and evaluations were limited to simulated or controlled environments, and there was a lack of real-world deployment and testing of E-MQTT in practical IoT or communication systems.

Continued on the next page

Paper	Strengths	Weaknesses
Alasmari & Alhogail [22]	evaluation of 22 ML algorithms, resulting in a model that achieves 100% accuracy in intrusion detection. The use of automatic feature engineering enhanced performance, increasing accuracy by 38.9% and reducing classification time by 67.7%.	Reliance on a single dataset may limit the generalizability of the results, and the focus solely on the MQTT protocol potentially restricted its relevance to other IoT environments. Additionally, the absence of comparative analysis with existing systems limited the understanding of the proposed model's advantages.

Kim et al [9] developed a comprehensive IoT security framework that identifies multiple IoT and botnet attacks utilizing the N-BaIoT dataset. Their model was proposed to identify attacks on IoT devices using a combination of five ML techniques; Naive Bayes (NB), K-Nearest Neighbors (K-NN), Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), and three DL algorithms; Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM). The ML models, specifically DT and RF, demonstrated superior performance in detecting the Mirai and Bashlite botnets inside the N-BaIoT dataset. According to the F1-score metric, the CNN model outperformed all other DL models.

Syed et al [10]. developed a new MQTT dataset with three types of attacks: denial proposed an ML-based framework for detecting DoS attacks in IoT devices. The authors focus on the MQTT protocol, commonly used in IoT communication, and present an attack model for DoS attacks on this protocol. To analyze network traffic and detect anomalies that may indicate a DoS attack, three machine learning techniques were applied: Average One-Dependence Estimator (AODE), derived from Naive Bayes; C4.5, built on decision trees; and Multilayer Perceptron (MLP), rooted in artificial neural networks. These algorithms were used to assess the classifiers' effectiveness in distinguishing between normal and attack categories, using count-based flow characteristics and field length variables. The empirical findings demonstrate that their suggested methodology may efficiently identify DoS assaults with a notable level of precision.

Vaccari et al [11] introduced MQTTset, a novel dataset that focuses on the MQTT protocol, which is extensively used in IoT networks. The new dataset was used to train ML models, including RF, NB, DT, Neural Network (NN), Gradient Boosting (GB), and MLP, in order to develop detection methods for safeguarding IoT environments. The authors also emphasize the significance of detection systems in the field of cyber-security and underscore the necessity for tailored datasets to train these models.

Alaiz-Moreton et al [12] created a new MQTT dataset containing three types of attacks: denial of service, man-in-the-middle, and intrusion. Their focus was on identifying attacks targeting IoT systems that utilize the MQTT protocol. They suggested models for an Intrusion Detection System (IDS) that can quickly identify network intrusions and security threats by using ensemble ML and DL algorithms; Extreme Gradient Boosting (XGBoost), LSTM, and Gated Recurrent Unit (GRU) to categorize the frames an IDS might assign as attack or normal. Their work provides valuable insights into detecting assaults on IoT devices utilizing various methods.

Mosaiyebzadeh et al [13] proposed a Deep Learning-based network intrusion detection system trained using " MQTT-IoT-IDS2020," a public dataset containing MQTT attacks. The proposed DNN, CNN-RNN-LSTM, and LSTM models were evaluated using standard performance metrics such as accuracy, precision, recall, F1-score, and weighted average. The performance assessment yielded very accurate findings and an F1-score in the CNN-RNN-LSTM model.

Hindy et al [14] created a new dataset called "MQTT-IoT-IDS2020" that includes both regular and attack situations in the context of IoT-MQTT. They made this dataset available to the public. The researchers developed a model that utilized six distinct ML approaches, including LR, k-NN, DT, RF, SVM, and NB, to detect intrusions in IoT networks. The researchers extracted three levels of features from the raw data (uniflow, biflow, packet features) and evaluated the significance of using high-level (flow-based) features to build their IDS. The findings demonstrated the efficacy of flow-based characteristics in identifying assaults.

Zeghida et al [15] introduced an IDS-based Ensemble Learning model to defend against cyber-attacks on IoT devices. They first generated a balanced binary dataset from the MQTTset dataset for training and testing the IDS. Then, they proposed and assessed three ensemble learning techniques—bagging, boosting, and stacking—for identifying intrusions in IoT systems through MQTT traffic analysis. The results confirmed the effectiveness of their approach, where accuracy exceeded 95%.

Dewantaz et al[16] introduced "SibProMQTT", a security scheme for enhancing the MQTT protocol in IoT devices. It focuses on defending against Sybil, message falsification, replay, and impersonation attacks. The scheme uses timestamps, session keys, and encryption for secure data transmission. It is proven effective through security analyses and experiments. SibProMQTT is notable for its lightweight, efficient approach to ensuring data protection and resistance to various attacks, thereby improving MQTT communication security in IoT systems.

Zeghida et al [17] proposed a deep learning (DL)-enabled IDS designed to detect DoS attacks in MQTT-enabled IoT device interactions. They employed a publicly available dataset known as the 'MQTT dataset.' Initially, they used individual algorithms such as LSTM, CNN, and GRU. Later, they integrated several DL algorithms to maximize their capabilities. So, hybrid DL models like CNN-RNN, CNN-LSTM, and CNN-GRU were created. The results of this study were excellent, with an accuracy rate of more than 99% and a meager loss rate of 0.072.

In their study, Im, Y., & Lim, M. [18] introduced a new mechanism called "E-MQTT" to specifically tackle the fundamental End-to-End communication issue seen in MQTT. E-MQTT enhances the capability of request-response patterns for seamless communication between a publisher and subscribers, allowing for the verification of the exact instant when subscribers get the message. The system facilitates bidirectional communication in two modes based on the configuration of the minimal number of answer packets: synchronous and asynchronous modes. The researchers deployed E-MQTT and conducted a comparative analysis with MQTT, demonstrating that E-MQTT effectively decreases the latency of end-to-end request-response communication.

Alasmari & Alhogail [22] conducted a a a thorough research that presented an effective ML-based IDS tailored to safeguard smart home IoT devices against MQTT assaults. Their study used an extended two-stage assessment technique to analyze 22 machine learning algorithms, finally determining that the Generalized Linear Model (GLM) paired with random oversampling is the most successful option, obtaining 100% accuracy and F-score. Notably, their study provided autonomous feature engineering strategies that improve model performance while decreasing detection time, solving the key issue of class imbalance in intrusion detection.

CONCLUSION

The IoT has revolutionized connectivity, allowing a vast array of services, devices, and systems to be interconnected. This has led to the integration of numerous protocols and applications tailored to different use cases. Among these, MQTT stands out as a particularly suitable protocol for IoT scenarios. Its significance is primarily due to its lightweight nature, making it ideal for environments where resources like electricity, processing power, memory, and bandwidth are constrained. Additionally, MQTT's open-source nature and ease of use add to its appeal in these settings. Recent research has increasingly focused on the security aspects of MQTT, recognizing it as a critical area of concern. This article provides a comprehensive overview of the MQTT protocol, including its various applications in the IoT landscape. It delves into the security challenges associated with MQTT, offering an in-depth analysis of the protocol's vulnerabilities.

Furthermore, the article presents a summary of the most up-to-date research on the detection of attacks targeting MQTT. This includes a critical evaluation of the strengths and limitations of current methodologies in identifying and mitigating these security threats. As part of ongoing and future initiatives, there is a clear intention to continue this research to advance MQTT security. Future efforts aim to develop more resilient and adaptive solutions capable of effectively protecting MQTT in the rapidly evolving and interconnected IoT ecosystem.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Roman, Rodrigo, Pablo Najera, and Javier Lopez. ”Securing the internet of things.” Computer 44.9 (2011): 51-58.

[2] Belkhiri, Hamza, et al. ”Security in the internet of things: recent challenges and solutions.” Proceedings of the 4th International Conference on Electrical Engineering and Control Applications: ICEECA 2019, 17–19 December 2019, Constantine, Algeria. Springer Singapore, 2021.

[3] Kouicem, Djamel Eddine, Abdelmadjid Bouabdallah, and Hicham Lakhlef. ”Internet of things security: A top-down survey.” Computer Networks 141 (2018): 199-221.

[4] Dinculeană, Dan, and Xiaochun Cheng. ”Vulnerabilities and limitations of MQTT protocol used between IoT devices.” Applied Sciences 9.5 (2019): 848.

[5] Firdous, Syed Naeem, et al. ”Modelling and evaluation of malicious attacks against the iot mqtt protocol.” 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2017.

[6] Chen, Fu, et al. ”A review on the study on MQTT security challenge.” 2020 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2020.

[7] Makhija, Jigar, Akhil Appu Shetty, and Ananya Bangera. ”Classification of attacks on MQTT-based IoT system using machine learning techniques.” International Conference on Innovative Computing and Communications: Proceedings of ICICC 2021, Volume 3. Springer Singapore, 2022.

[8] Patel, Rushi. ”Cyber Security in Domain of IoT: A Review Threats and Security.” (2020).

[9] Kim, Jiyeon, et al. ”Intelligent detection of iot botnets using machine learning and deep learning.” Applied Sciences 10.19 (2020): 7009.

[10] Syed, Naeem Firdous, et al. ”Denial of service attack detection through machine learning for the IoT.” Journal of Information and Telecommunication 4.4 (2020): 482-503.

[11] Vaccari, Ivan, et al. ”MQTTset, a new dataset for machine learning techniques on MQTT.” Sensors 20.22 (2020): 6578.

[12] Alaiz-Moreton, Hector, et al. ”Multiclass classification procedure for detecting attacks on MQTT-IoT protocol.” Complexity 2019 (2019).

[13] Mosaiyebzadeh, Fatemeh, et al. ”A network intrusion detection system using deep learning against mqtt attacks in iot.” 2021 IEEE Latin-American Conference on Communications (LATINCOM). IEEE, 2021.

[14] Hindy, Hanan, et al. ”Machine learning based IoT intrusion detection system: An MQTT case study (MQTT-IoT-IDS2020 dataset).” Selected Papers from the 12th International Networking Conference: INC 2020. Cham: Springer International Publishing, 2021.

[15] Zeghida, Hayette, Mehdi Boulaiche, and Ramdane Chikh. ”Securing MQTT protocol for IoT environment using IDS based on ensemble learning.” International Journal of Information Security (2023): 1-12.

[16] Dewantaz, F., Wahidah, I., Hertiana, S. N., Sanjoyo, D. D., & Ariffin, S. H. S. (2023, September). SibProMQTT: Protection of the MQTT Communication Protocol Against Sybil Attacks Applied for IoT Devices. In 2023 International Conference on IC Design and Technology (ICICDT) (pp. 108-111). IEEE.

[17] Zeghida, H., Boulaiche, M., & Chikh, R. (2023, May). Detection of DoS Attacks in MQTT Environ-

ment. In International Conference on Intelligent Systems and Pattern Recognition (pp. 129-140). Cham: Springer Nature Switzerland.

[18] Im, Y., & Lim, M. (2023). E-MQTT: End-to-End Synchronous and Asynchronous Communication Mechanisms in MQTT Protocol. Applied Sciences, 13(22), 12419.

[19] Kant, D., Johannsen, A.,& Creutzburg, R. (2021). Analysis of IoT security risks based on the exposure of the MQTT protocol. Electronic Imaging, 33, 1-8.

[20] Vaccari, I., Aiello, M., & Cambiaso, E. (2020). SlowITe, a novel denial of service attack affecting MQTT. Sensors, 20(10), 2932.

[21] Chen, F., Huo, Y., Zhu, J., & Fan, D. (2020, November). A review on the study on MQTT security challenge. In 2020 IEEE International Conference on Smart Cloud (SmartCloud) (pp. 128-133). IEEE.

[22] Alasmari, R., & Alhogail, A. A. (2024). Protecting Smart-Home IoT Devices From MQTT Attacks: An Empirical Study of ML-Based IDS. IEEE Access, 12, 25993-26004.