Enhancing Security in MQTT-Based IoT Networks: A Review of ML-Based Detection Methods and Future Directions

Jaspreet Kaur[1], Jaswinder Singh[2],Sandeep Sood[3]
Department of Computer Science, Guru Nanak Dev University, Amritsar

Abstract: The widespread adoption of the Internet of Things (IoT) led to the interconnection of numerous devices, resulting in an increased need for secure and reliable communication protocols. In response to this demand, the Message Queuing Telemetry Transport (MQTT) protocol emerged as a popular choice for IoT communication due to its lightweight design. In this review paper, we delved into the application of machine learning (ML) techniques in MQTT-based IoT networks to detect communication attacks, discussing the MQTT protocol, its vulnerabilities, and potential attacks. Additionally, an overview of existing literature on machine learning-based detection methods, outlining their contributions and limitations has been provided. Subsequently, the future directions for enhancing the detection of MQTT-based IoT communication attacks have been elaborated after identification of research gaps.

Keywords: MQTT, IoT networks, ML-based detection methods, Communication attacks, Security mechanisms, Feature engineering, Real-time detection, Scalable algorithms

1. Introduction

The rapid growth and widespread adoption of the Internet of Things (IoT) transformed the way we interacted with our environment. IoT technology enabled the interconnection of numerous devices, ranging from small sensors to large-scale industrial systems, facilitating seamless communication and data exchange [Chen et al., 2020]. This interconnected network of devices provided unprecedented convenience and efficiency, revolutionizing various industries such as healthcare, transportation, agriculture, and manufacturing.

As the protocol for communicating with IoT networks, MQTT stood for Message Queuing Telemetry Transport. To provide the integrity and privacy of data exchanged within the network, significant security challenges had to be addressed. MQTT-based IoT networks have been compromised by malicious actors exploiting vulnerabilities created by the proliferation of IoT devices [Sanjuan et al., 2020]. Consequently, enhancing the security of MQTT-based IoT networks became a critical concern for researchers, practitioners, and policymakers alike. MQTT was a lightweight, publish-subscribe messaging protocol designed to be efficient, reliable, and suitable for constrained devices and low-bandwidth, high-latency, or unreliable networks. It was commonly used in IoT environments to facilitate communication between devices and enable efficient data exchange within IoT networks.

As one of the most widely used internet of things communication protocols, Message Queuing Telemetry Transport (MQTT) emerged. With its lightweight and efficient design, MQTT is an ideal protocol for resource-constrained devices in the Internet of Things [Ong et al., 2021]. It followed a publish-subscribe messaging pattern, where devices published data to topics, and other devices subscribed to those topics to receive the data. MQTT's simplicity and scalability made it a popular choice for connecting IoT devices, enabling seamless communication and efficient data transfer [Erlikaya & Gokhan Dalkiltc, 2018].

Despite its widespread use, the lightweight nature of the MQTT protocol also introduced security challenges. MQTT lacked built-in security features such as authentication and encryption, making MQTT-based IoT networks vulnerable to various threats and attacks. For example, attackers could intercept MQTT messages, manipulate data, or gain unauthorized access to the network. Additionally, MQTT did not provide mechanisms to validate the integrity and authenticity of published messages, opening up opportunities for message spoofing and tampering [Rahman et al., 2018].

To address these security concerns, researchers and practitioners explored various approaches, and machine learning (ML) emerged as a promising technique. ML techniques leveraged the power of data analysis and pattern recognition to identify anomalies, detect malicious activities, and enhance the overall security posture of IoT networks. ML-based detection methods showed significant potential in mitigating security threats in MQTT-based IoT networks [Sicari et al., 2015].

The objective of this paper was to use machine learning to detect threats in MQTT-based IoT networks. Analyzing and evaluating existing approaches, identifying their strengths and limitations, outlining future directions, and identifying potential advancements in ML-based security solutions were the primary goals.

The remainder of this paper was organized as follows: Section 2 provided an overview of the MQTT protocol and its security challenges. It discussed the fundamental components of MQTT, the publish-subscribe messaging pattern, and the security vulnerabilities associated with MQTT-based IoT networks. Section 3 presented a review of the existing ML-based detection methods for securing MQTT-based IoT networks. The review categorized these methods based on their approach and techniques, highlighting their key features and contributions.

The paper then explored different machine learning techniques for attack detection, including supervised learning, unsupervised learning, deep learning, and reinforcement learning approaches. It discussed their application in MQTT-based IoT networks and addressed evaluation metrics and performance analysis.

The review of existing literature in Section 5 provided a comprehensive overview of studies on detecting DoS attacks, Man-in-the-Middle attacks, eavesdropping attacks, and message tampering attacks in MQTT-based IoT networks. The paper also compared the findings of these studies. Section 6 identified research gaps and challenges associated with existing machine learning-based detection methods, such as limitations, real-world deployment challenges, scalability, performance, interpretability of models, and addressing false positives and false negatives.

Section 7 outlined future research directions, including enhanced feature engineering, integration of multiple security mechanisms, development of explainable and interpretable machine learning models, real-time detection and response capabilities, and the need for scalable and resource-efficient algorithms. Finally, the conclusion summarized the key findings of the paper, emphasizing the importance of machine learning-based detection methods for securing MQTT-based IoT networks and providing recommendations for future research. The review paper provided valuable insights into existing knowledge about machine learning techniques for detecting communication attacks in MQTT-based Internet of Things networks, which would be useful to researchers, practitioners, and policymakers interested in IoT security.

1.1 Background

The Message Queuing Telemetry Transport (MQTT) protocol has emerged as a popular choice for IoT communication due to its lightweight design and efficient publish-subscribe messaging model. MQTT is widely adopted in various domains, including smart homes, healthcare, transportation, and industrial automation [Sicari et al., 2015]. A publish-subscribe paradigm is used, where devices publish data to a broker and other devices subscribe to relevant topics to receive the information. This simplicity and flexibility make MQTT an attractive choice for IoT deployments.

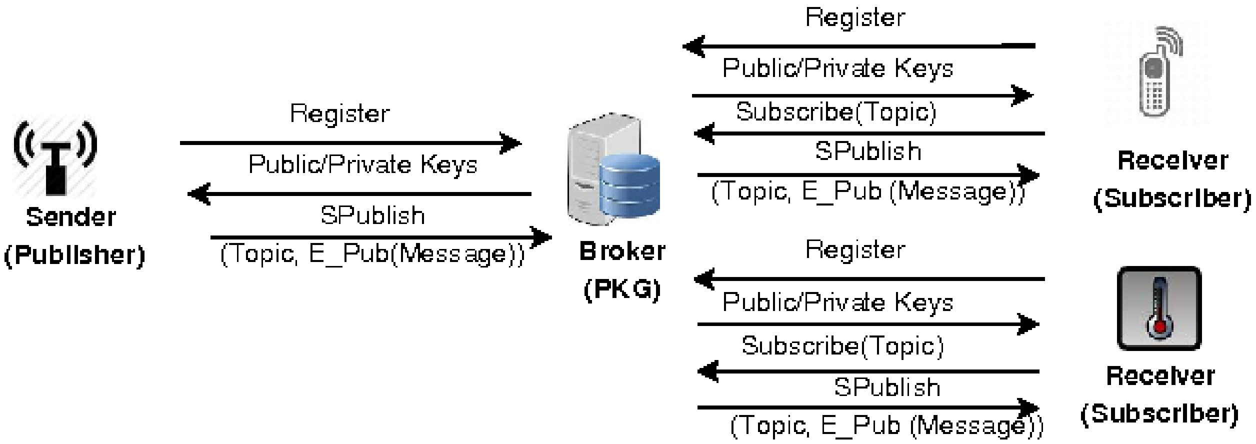

Figure 1:- Architecture of the scheme [Singh et al., 2015]

However, the lightweight nature of MQTT also introduces inherent vulnerabilities that can be exploited by malicious actors. A number of vulnerabilities can be exploited, including insufficient authentication, encryption, and weak access control mechanisms. As the number of IoT devices and MQTT deployments continue to grow, the need for effective security measures to protect these systems from communication attacks becomes increasingly crucial [Rahman et al., 2018].

1.2 Motivation

As IoT networks using MQTT-based communication continue to grow in popularity, addressing their inherent security vulnerabilities becomes increasingly important. This review paper aims to address these concerns. It has been reported that traditional security mechanisms, such as encryption and access control, are insufficient to detect and prevent sophisticated communications attacks [Al-Fuqaha et al., 2015]. Machine learning (ML) techniques have shown great promise in addressing security challenges in various domains, and their application in the context of MQTT-based IoT networks holds immense potential.

The motivation to explore ML-based detection methods for communication attacks in MQTT-based IoT networks arises from the advantages ML offers over traditional rule-based approaches. ML algorithms can analyze large volumes of data and identify patterns that may not be apparent to human operators. They have the ability to learn from historical data and adapt their models to detect novel attack patterns, providing a proactive defense against emerging threats [Hussein & Nhlabatsi, 2022]. By leveraging ML, it is possible to develop robust and scalable detection mechanisms capable of identifying communication attacks in real-time.

1.3 Objectives

This review paper aims to accomplish the following objectives:

i. Analyzing the vulnerabilities associated with the MQTT protocol in the context of IoT networks. This includes understanding how MQTT is designed, its architecture, and the vulnerabilities attackers can exploit.

ii. Reviewing and evaluating the existing literature on machine learning-based detection techniques for securing MQTT-based IoT networks. This involves categorizing the methods based on their approach and techniques, highlighting their key features and contributions.

iii. Identifying the limitations and challenges of existing ML-based detection methods for communication attacks in MQTT-based IoT networks. This includes discussing issues such as interpretability and explainability of ML models, scalability and performance concerns, and addressing the problem of false positives and false negatives.

iv. Proposing future directions and recommendations for improving the detection of communication attacks in MQTT-based IoT networks. This includes suggesting enhanced feature engineering and data preprocessing techniques, advocating for the integration of multiple security mechanisms, and emphasizing the need for real-time detection and response capabilities.

By accomplishing these objectives, this review paper aimed to contribute valuable insights to the existing body of knowledge related to machine learning techniques that can be used to detect communication attacks in IoT networks based on MQTT. It aimed to be a useful resource for IoT security researchers, practitioners, and policymakers interested in enhancing the security of MQTT-based IoT networks.

IoT security researchers, practitioners, and policymakers will gain valuable insights from this review paper as it contributes to the existing body of knowledge related to machine learning techniques that can be used to detect communication attacks in IoT networks based on MQTT.

2. MQTT Protocol and Communication Attacks

2.1 MQTT Protocol Overview

IoT devices communicate efficiently with each other with the MQTT (Message Queuing Telemetry Transport) protocol. This model is published-subscribed, with devices publishing messages to a broker, and other devices subscribing to relevant topics to receive those messages [Firdous et al., 2017]. The protocol operates on top of TCP/IP, making it suitable for constrained devices with limited resources and low bandwidth.

MQTT uses a simple packet structure consisting of a fixed header and variable-length payload. The fixed header contains control information, such as the message type and quality of service (QoS) level, while the payload carries the application-specific data [Yassein et al., 2017]. The protocol supports three levels of QoS: QoS 0 (at most once), QoS 1 (at least once), and QoS 2 (exactly once), providing different levels of message delivery guarantees.

2.2 Vulnerabilities in MQTT-Based IoT Networks

Despite its simplicity and efficiency, the MQTT protocol introduces certain vulnerabilities that can be exploited by attackers. One common vulnerability is the lack of encryption and authentication by default [A. P. & K., 2019]. MQTT allows anonymous connections, which can lead to unauthorized access to the broker and intercepted messages. Insecure connections can expose sensitive data, compromising the privacy and integrity of the transmitted information.

Another vulnerability is the weak access control mechanisms in MQTT. The protocol does not provide robust mechanisms for access control, relying primarily on the use of username and password authentication. However, these credentials can be easily compromised if not properly managed, leading to unauthorized access and potential attacks on the IoT network [Hussein & Nhlabatsi, 2022].

Additionally, MQTT is susceptible to Denial of Service (DoS) attacks [Hernández Ramos et al., 2018]. Attackers can flood the broker with a high volume of malicious messages, overwhelming the system's resources and causing it to become unresponsive. Such attacks can disrupt the functioning of the IoT network, impacting critical operations and leading to financial losses or even safety hazards.

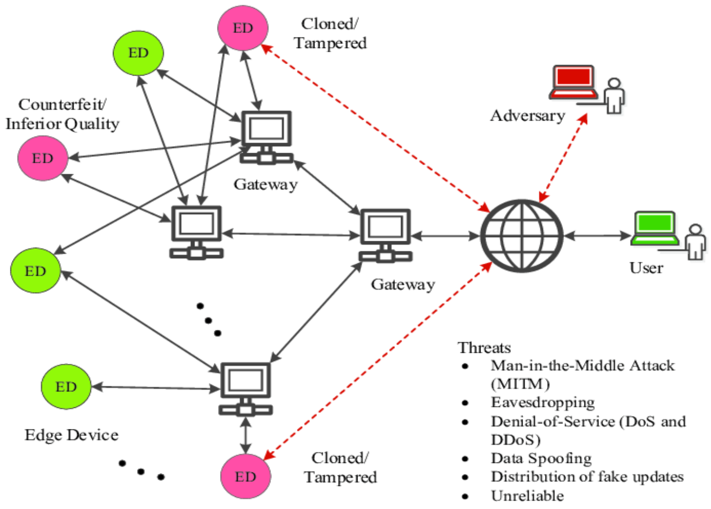

Figure 2:- Vulnerabilities in MQTT-Based IoT Networks (ResearchGate, 2015)

2.3 Communication Attacks in MQTT-Based IoT Networks

Communication attacks in MQTT-based IoT networks can have severe consequences, compromising the security and reliability of the system [Al-Fuqaha et al., 2019]. These attacks target various components of the MQTT communication flow and can be categorized into several types.

One common attack is message tampering, where an attacker intercepts and modifies the MQTT messages exchanged between devices and the broker. By altering the content of the messages, attackers can manipulate sensor data, inject malicious commands, or mislead the intended recipients [Khan et al., 2021].

Another attack is message replay, where an attacker intercepts and resends previously captured MQTT messages [Khan et al., 2018]. By replaying legitimate messages, attackers can trick devices or the broker into taking unwanted actions or repeating previous operations, leading to unexpected system behavior or unauthorized access.

MQTT-based IoT networks are also susceptible to man-in-the-middle (MitM) attacks. In these attacks, the attacker positions themselves between the sender and receiver, intercepting and potentially modifying the MQTT messages [Khan et al., 2021]. This allows the attacker to eavesdrop on sensitive information, tamper with the communication, or impersonate legitimate devices.

Other communication attacks include message flooding, where attackers flood the broker with a large volume of messages, consuming its resources and causing service disruption, and unauthorized topic subscription, where attackers subscribe to sensitive topics to gain access to confidential information [Aitzhan et al., 2018].

To address these communication attacks, machine learning techniques can be employed for attack detection and prevention. By leveraging ML algorithms, it is possible to analyze the patterns and anomalies in MQTT communication data to identify potential attacks in real-time. Continuing with our discussion of MQTT-based IoT attacks, we will examine different machine-learning techniques.

Table 1:- Table outlining some common communication attacks in MQTT-based IoT networks [Sicari et al., 2015]

Attack Type	Description
Eavesdropping	Attackers intercept and listen to the MQTT messages exchanged between IoT devices and the broker, potentially gaining access to sensitive information such as passwords, user data, or

	control commands.
Message Tampering	Attackers modify the content of MQTT messages in transit, altering the intended message or injecting malicious commands or data into the communication, leading to unauthorized actions or data corruption.
Replay Attack	Attackers capture and retransmit MQTT messages to the broker or IoT devices at a later time, attempting to deceive the system into executing the same action multiple times or replaying outdated or invalid data.
Denial of Service	Attackers flood the MQTT network with a high volume of malicious traffic or requests, overwhelming the resources of the broker or IoT devices, causing disruption, slowdown, or complete unavailability of the system.
Man-in-the-Middle	Attackers position themselves between the MQTT client and broker, intercepting and manipulating the communication flow. They can eavesdrop, modify, or inject MQTT messages, leading to unauthorized access or data manipulation.
Spoofing	Attackers impersonate a legitimate MQTT client or broker by forging their identities, allowing them to gain unauthorized access, perform malicious actions, or manipulate the MQTT network's integrity and availability.
Hijacking	Attackers take control of an existing MQTT session by stealing the session identifier or credentials, enabling them to impersonate the legitimate user and gain unauthorized access or manipulate the communication.

3. Machine Learning Techniques for Attack Detection

3.1 Overview of Machine Learning

Without explicit programming, machine learning allows systems to learn and improve from experiences automatically. It involves the development of algorithms and statistical models that allow computers to analyze data, identify patterns, and make predictions or decisions based on the observed information [Zekri et al., 2017]. Machine learning techniques have gained significant attention in cybersecurity for their capability to detect and mitigate threats across a broad range of domains, including IoT networks.

3.2 Supervised Learning Algorithms

Data points are grouped into classes or categories when trained with supervised learning algorithms. These algorithms learn from the labeled examples to classify new, unseen instances. When training supervised learning algorithms for detecting attacks in MQTT-based IoT networks, historical data can be used that includes both normal and attack instances [Moller et al., 1993]. The algorithms learn to distinguish between the two and can subsequently identify attacks in real-time by analyzing the characteristics of incoming MQTT messages.

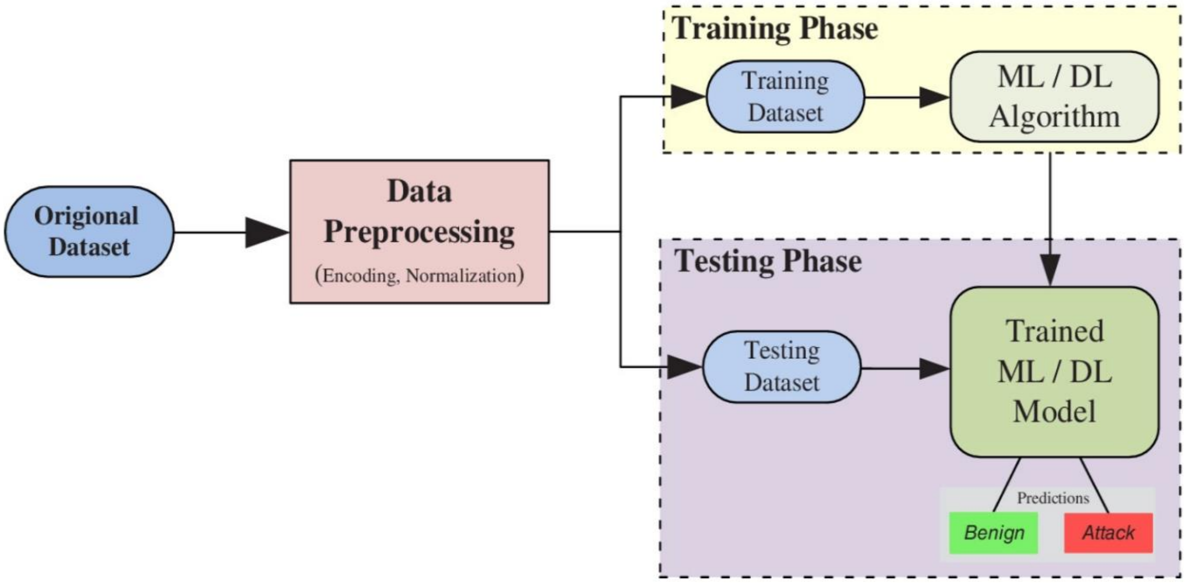

Figure 3:- Machine Learning Techniques for Attack Detection (Ali et al., 2023)

Supervised learning algorithms, such as decision trees, random forests, support vector machines (SVMs), and neural networks, play a crucial role in attack detection [Hosseini et al., 2019]. By leveraging labeled training data, these algorithms construct models capable of capturing the underlying patterns and anomalies present in MQTT communication. This process enables the accurate detection of attacks and enhances the security of the system.

3.3 Unsupervised Learning Algorithms

Unlike supervised learning, unsupervised learning algorithms do not require labeled data for training. By identifying patterns and structures in the data, they identify attack patterns without knowing the attack instance [Celebi et al.,2016]. Unsupervised learning algorithms are well-suited for anomaly detection, as they can identify deviations from normal behavior based on the statistical properties of the data.

There are various clustering algorithms that are commonly used in unsupervised learning for attack detection, such as k-means clustering and hierarchical clustering. These algorithms group similar MQTT messages together, allowing the identification of abnormal clusters that may indicate potential attacks [Sathya et al., 2013]. Additionally, outlier detection techniques, such as the isolation forest algorithm or the local outlier factor, can be employed to identify individual MQTT messages that deviate significantly from the normal communication patterns.

3.4 Deep Learning Techniques

A number of fields, including image recognition, natural language processing, and cyber security, have demonstrated impressive results using machine learning techniques, such as deep learning [Hesamian et al., 2019]. Data can be automatically analyzed for patterns and dependencies using these models. There are several types of deep learning models, including deep neural networks, convolutional neural networks, and recurrent neural networks (RNN).

In the context of attack detection in MQTT-based IoT networks, deep learning techniques can be utilized to analyse the content and structure of MQTT messages, identifying malicious patterns or anomalies [Koroniotis et al., 2019]. It is possible, for example, to train neural networks to extract features from MQTT message payloads, which capture the underlying characteristics of normal and attack messages. The network can then classify incoming messages in real-time, alerting the system to potential attacks.

3.5 Reinforcement Learning Approaches

An application of reinforcement learning is the training of agents to make sequential decisions in an environment in which rewards are maximized. As part of the attack detection strategy in IoT networks based on MQTT, reinforcement learning can be used to develop intelligent agents for detecting and responding to attacks [Wang et al., 2018].The agent interacts with the MQTT network, observing the current state and taking actions to mitigate attacks or prevent further compromise. Through trial and error, the agent learns to optimize its actions based on the feedback received in the form of rewards or penalties. Reinforcement learning approaches enable the development of adaptive and proactive defense mechanisms, where the system can autonomously respond to emerging threats in real time.

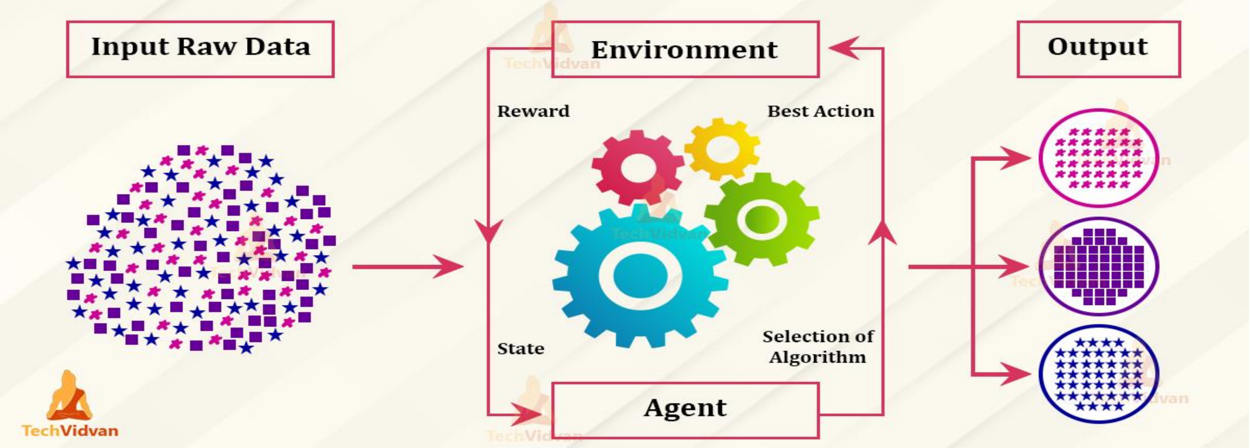

Figure 4:- Reinforcement Learning Approach (Kadari, 2021)

It is possible to enhance the detection capabilities of MQTT-based IoT networks by combining machine learning techniques, such as unsupervised learning, deep learning, and reinforcement learning. These approaches enable the system to identify known attack patterns, detect anomalies in communication, analyze message content, and dynamically adapt to new attack strategies to effectively detect and mitigate attacks in MQTT-based IoT networks [Tesauro et al., 2006]. These machine learning techniques provide the following benefits:

Supervised learning algorithms leverage labelled training data to build models that can accurately classify MQTT messages as normal or malicious [Hassija et al., 2019]. By learning from historical data that includes both normal and attack instances, these algorithms can identify patterns and characteristics associated with different types of attacks. Decision trees, random forests, support vector machines (SVM), and neural networks are commonly used supervised learning algorithms for attack detection in MQTT-based IoT networks.

Data that is not labelled is not used in unsupervised learning algorithms. They analyze the statistical properties of MQTT messages to detect anomalies and identify potential attacks. It is possible to identify abnormal clusters associated with attacks by clustering similar MQTT messages, such as using k-means clustering or hierarchical clustering. Outlier detection techniques like the isolation forest algorithm and local outlier factor can identify individual MQTT messages that deviate significantly from normal communication patterns.

Data patterns and dependencies can be learned more efficiently and quickly with deep neural networks, convolutional neural networks, and recurrent neural networks. By analyzing the content and structure of MQTT messages, these models can identify malicious patterns or anomalies. Deep neural networks can be trained to extract features from message payloads, capturing the underlying characteristics of normal and attack messages. This enables real-time classification of incoming messages, providing timely alerts for potential attacks.

Reinforcement learning approaches focus on training intelligent agents to make sequential decisions in response to attacks. These agents learn by interacting with the MQTT network, observing the current state, and taking actions to mitigate attacks or prevent further compromise. Through trial and error, the agents optimize their actions based on feedback received in the form of rewards or penalties. Reinforcement learning enables the development of adaptive and proactive defense mechanisms, allowing the system to autonomously respond to emerging threats in real-time [Tesauro et al., 2006].

By combining these machine learning techniques, MQTT-based IoT networks can benefit from enhanced attack detection capabilities. Known attack patterns can be identified through supervised learning, anomalies in communication can be detected using unsupervised learning, deep learning can analyze message content, and reinforcement learning can provide adaptive defense mechanisms. These approaches enable the system to dynamically adapt to new attack strategies and protect the integrity and security of MQTT-based IoT networks.

4. Detection of Communication Attacks in MQTT-Based IoT Networks

4.1 Supervised Learning-Based Approaches

For supervised learning-based approaches to detecting communication attacks in MQTT-based IoT networks, labelled datasets with normal and attack instances are used to train machine learning models. These models learn from the labelled examples to classify new MQTT messages as either normal or malicious [Hindy et al., 2021]. It is possible to perform this task using many different supervised learning algorithms, including decision trees, random forests, support vector machines (SVM) and neural networks.

In this approach, a training dataset is created by capturing MQTT network traffic and labelling each message as normal or an attack. The features extracted from the MQTT messages, such as message size, topic, and payload content, are used as inputs to the supervised learning algorithm. The algorithm then learns the patterns and characteristics of different attack types and can accurately classify new incoming messages in real-time [Koroniotis et al., 2019].

Supervised learning-based approaches work best when the labelled dataset and algorithm are both good. The training dataset should be diverse and representative of the various attack scenarios that can occur in MQTT-based IoT networks. Additionally, feature selection and extraction techniques play a crucial role in capturing the relevant information from MQTT messages.

4.2 Unsupervised Learning-Based Approaches

MQTT-based IoT networks do not require labelled training data for unsupervised learning-based approaches to detecting communication attacks. Instead, these approaches analyze the statistical properties of MQTT messages to detect anomalies and identify potential attacks. A common approach to clustering is to use k-means clustering and hierarchical clustering algorithms.

In unsupervised learning-based approaches, MQTT messages are clustered based on their similarities [Zantalis et al., 2019]. Messages that deviate significantly from the normal communication patterns form abnormal clusters, indicating potential attack instances. Additionally, outlier detection techniques, such as the isolation forest algorithm or the local outlier factor, can be employed to identify individual MQTT messages that exhibit abnormal behaviour.

One advantage of unsupervised learning-based approaches is their ability to detect unknown and emerging attacks, as they do not rely on predefined attack patterns. However, they may also produce false positives due to the inherent complexity and variability of MQTT-based IoT networks [Hussain et al., 2020]. Therefore, fine-tuning and optimization of the anomaly detection thresholds are necessary to achieve an optimal balance between detection accuracy and false positive rates.

4.3 Deep Learning-Based Approaches

MQTT-based IoT networks can be protected against communication attacks using deep learning approaches. These approaches analyze the content and structure of MQTT messages, extracting features and patterns that can indicate malicious activities. Convolutional neural networks (CNN) and recurrent neural networks (RNN) are commonly used architectures in this context.

Deep learning models can automatically learn and represent complex relationships between MQTT message features [Koroniotis et al., 2019]. For example, a CNN can extract spatial features from message payloads, while an RNN can capture temporal dependencies in message sequences. By training these models on large datasets containing normal and attack instances, they can effectively learn to differentiate between different types of attacks and normal MQTT communication.

The main advantage of deep learning-based approaches is their ability to handle high-dimensional and unstructured data, such as message payloads, which may contain critical information for attack detection [Tran et al., 2022]. However, deep learning models often require a large amount of labelled training data and considerable computational resources for training and inference.

4.4 Hybrid Approaches

By combining supervised learning, unsupervised learning, and deep learning, hybrid approaches can improve the accuracy and robustness of attack detection in MQTT-based IoT networks. These approaches aim to leverage the strengths of different techniques while mitigating their limitations.

For example, a hybrid approach may involve using unsupervised learning techniques to identify anomalous clusters or outliers in MQTT message data, followed by a supervised learning model to classify the identified instances as specific attack types [Mohamad Noor et al., 2019]. A combination of these technologies allows for detection of known and unknown attacks, enhancing the effectiveness of the detection process. Another hybrid approach could be utilizing deep learning models to extract high-level features from MQTT message payloads and combining them with a supervised learning algorithm for attack classification.

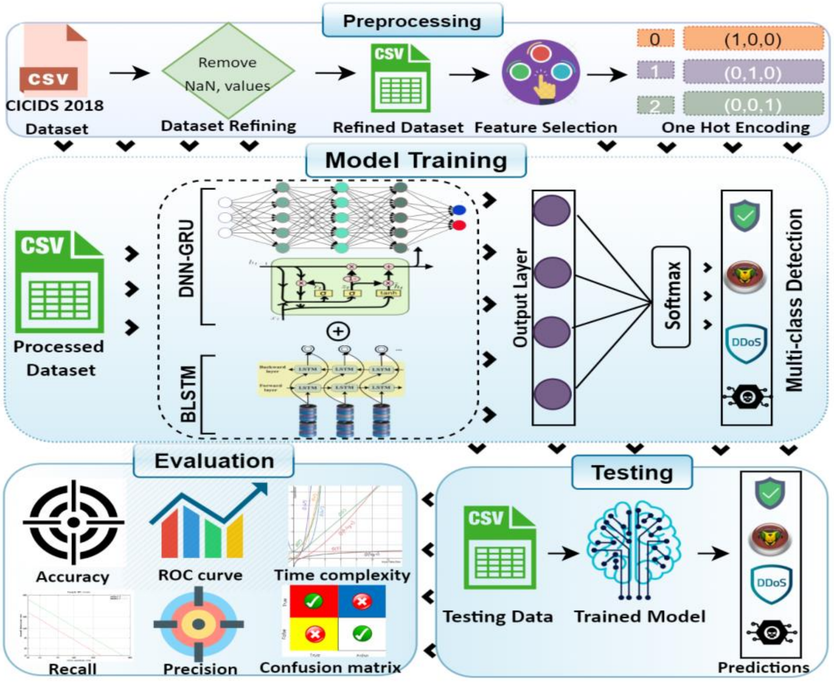

Figure 5:- Proposed hybrid detection framework [Javeed et al., 2021]

The benefit of hybrid approaches is that they can handle a wide range of attack scenarios and adapt to new attack patterns. By combining multiple techniques, these approaches can enhance detection accuracy, reduce false positives, and provide a more comprehensive defense mechanism against communication attacks in

MQTT-based IoT networks [Mohamad et al., 2019]. To achieve optimal performance, different techniques should be carefully integrated and optimized.

4.5 Evaluation Metrics and Performance Analysis

To assess the effectiveness of communication attack detection techniques in MQTT-based IoT networks, appropriate evaluation metrics and performance analysis are essential [Mineraud et al., 2016]. These metrics provide quantitative measures of detection accuracy, efficiency, and robustness, enabling researchers and practitioners to compare different approaches and understand their strengths and limitations.

Common evaluation metrics for attack detection include:

1. There are two types of True Positive Rates (TPRs): True Positive Rate (TPRs) measure the proportions of attacks correctly identified, while False Positive Rates (FPRs) measure the proportion of normal events misclassified as attacks by the system [Chicco et al., 2020]. A balance between TPR and FPR is crucial to minimize both missed detections and false alarms.

2. Precision and Recall: An attack's precision is the percentage of instances that are correctly classified as attacks, while an attack's recall is the proportion of instances that are correctly identified as attacks. High precision indicates a low false-positive rate, while high recall indicates a low false-negative rate.

3. F1 Score: The F1 score is the harmonic mean of precision and recall. It provides a single measure that balances both precision and recall, giving an overall assessment of the detection performance.

In addition to these metrics, performance analysis should also consider computational efficiency, scalability, and the ability to handle real-time detection requirements. The computational resources required for training and inference, the time taken to process MQTT messages, and the scalability of the approach with increasing network size should be evaluated.

Furthermore, it is important to assess the robustness of the detection techniques against evasion attacks or adversarial manipulations. Adversaries may attempt to modify MQTT messages to bypass detection systems, and evaluating the ability of the techniques to detect such attacks is crucial.

Performance analysis should be conducted using representative datasets that capture a variety of attack scenarios and network conditions (Mineraud et al., 2016). The datasets should include both known attacks and novel attack patterns to assess the generalization capability of the detection techniques.

By utilizing appropriate evaluation metrics and performing thorough performance analyses of MQTT-based IoT networks, researchers and practitioners can identify strengths and weaknesses of detection techniques. Using this knowledge, we can develop more robust and effective detection systems that contribute to further advancements in this field.

Table 2:- Table summarizing the evaluation metrics and performance analysis for enhancing security in MQTT-based IoT network [Sicari et al., 2015]

Evaluation Metrics	**Description**
Authentication	Verifying the identity of clients and servers
Authorization	Granting or denying access to specific MQTT topics
Data encryption	Encrypting MQTT messages to protect data confidentiality
Message integrity	Ensuring the integrity of MQTT messages
Message replay protection	Preventing replay attacks by detecting and rejecting duplicate messages

Resource utilization	Analyzing the impact of security measures on resource consumption
Scalability	Assessing the ability to handle increasing numbers of IoT devices and clients
Latency	Measuring the time delay in message delivery
Throughput	Evaluating the rate of message transfer
Overhead	Analyzing the additional network traffic caused by security measures
Complexity	Assessing the complexity of implementing security measures
Robustness	Evaluating the resilience of the system against attacks
Energy efficiency	Analyzing the impact of security measures on IoT device energy consumption

By combining supervised learning, unsupervised learning, and deep learning, hybrid approaches can improve the accuracy and robustness of attack detection in MQTT-based IoT networks. These approaches aim to leverage the strengths of different techniques while mitigating their limitations.

For example, a hybrid approach may involve using unsupervised learning techniques to identify anomalous clusters or outliers in MQTT message data, followed by a supervised learning model to classify the identified instances as specific attack types. A combination of these technologies allows for detection of known and unknown attacks, enhancing the effectiveness of the detection process. Another hybrid approach could be utilizing deep learning models to extract high-level features from MQTT message payloads and combining them with a supervised learning algorithm for attack classification [Mineraud et al., 2016].

The benefit of hybrid approaches is that they can handle a wide range of attack scenarios and adapt to new attack patterns. By combining multiple techniques, these approaches can enhance detection accuracy, reduce false positives, and provide a more comprehensive defense mechanism against communication attacks in MQTT-based IoT networks. Integrating different techniques is crucial to achieving optimal performance, but needs to be carefully planned and optimized.

5. Review of Existing Literature

5.1 Review of Studies on Detection of DoS Attacks

A review of the existing literature shows that researchers and practitioners have proposed different techniques and approaches for detecting DoS attacks in MQTT-based IoT networks. DoS attacks aim to disrupt the normal operation of IoT devices by overwhelming the network with a flood of malicious traffic or resource exhaustion.

Studies have proposed different detection methods for DoS attacks in MQTT-based IoT networks [Soomro et al., 2016]. These methods include traffic analysis, anomaly detection, machine learning-based approaches, and network-level defences. Traffic analysis techniques focus on monitoring and analyzing network traffic patterns to identify abnormal behavior indicative of a DoS attack. Anomaly detection approaches aim to identify deviations from normal traffic patterns by modelling the behaviour of the IoT network. Machine learning-based approaches utilize supervised or unsupervised learning algorithms to learn attack patterns and classify incoming traffic. Network-level defenses involve mechanisms such as rate limiting, traffic filtering, or traffic prioritization to mitigate the impact of DoS attacks.

The review of literature highlights the strengths and limitations of different detection methods. Traffic analysis techniques can effectively identify sudden increases in network traffic or unusual traffic patterns, but they may struggle with distinguishing legitimate traffic from malicious traffic. Anomaly detection methods can detect previously unseen DoS attacks but may generate false positives due to the complexity and variability of IoT networks. Machine learning-based approaches can achieve high accuracy in detecting DoS attacks but require substantial training data and computational resources [Soomro et al., 2016]. Network-level defenses provide a proactive defense mechanism but may not be effective against sophisticated DoS attacks.

Overall, the review of studies emphasizes the need for a multi-faceted approach to detect DoS attacks in MQTT-based IoT networks. Combining different techniques, such as traffic analysis, anomaly detection, and machine learning, can enhance the detection accuracy and robustness. Moreover, researchers have identified the importance of real-time detection and the need to address the resource constraints of IoT devices while designing DoS detection mechanisms.

5.2 Review of Studies on Detection of Man-in-the-Middle Attacks

IoT Man-in-the-Middle (MitM) attacks have been the subject of considerable interest in the literature [Kang et al., 2019].MitM attacks involve an adversary intercepting and manipulating MQTT communications between IoT devices, potentially leading to data leakage, unauthorized access, or unauthorized control over devices.

Researchers have proposed several detection approaches for MitM attacks in MQTT-based IoT networks. These approaches include cryptographic techniques, authentication mechanisms, secure key exchange protocols, and anomaly detection methods [U.Farooq et al., 2015]. Cryptographic techniques, such as secure communication protocols and encryption algorithms, aim to protect the confidentiality and integrity of MQTT messages. Authentication mechanisms, such as digital certificates or biometric authentication, help verify the identities of MQTT clients to prevent unauthorized access [Kang et al., 2019]. Secure key exchange protocols, such as Diffie-Hellman key exchange, establish secure communication channels between MQTT clients. Anomaly detection methods leverage the analysis of MQTT message patterns, traffic behavior, or deviations from normal communication to identify potential MitM attacks.

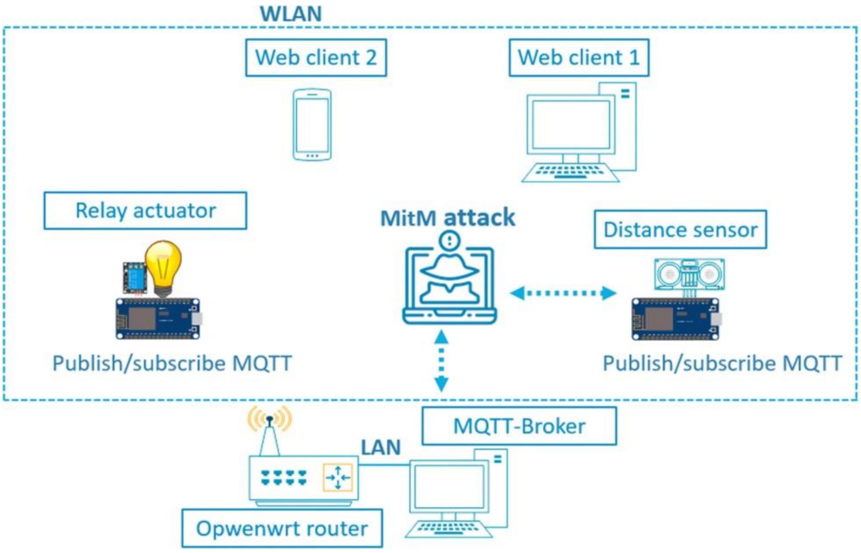

Figure 6:- A method to detect man-in-the-middle attacks over the internet of things [Álvaro Michelena Grandío et al., 2023]

The review of literature highlights the challenges in detecting MitM attacks in MQTT-based IoT networks. The resource-constrained nature of IoT devices and the need for efficient cryptographic algorithms and protocols pose significant challenges. Additionally, IoT networks are dynamic and have a variety of attack scenarios, making detection of MitM attacks difficult. Researchers have emphasized the importance of end-to-end security, strong authentication mechanisms, and continuous monitoring to detect and prevent MitM attacks.

It is evident from the review that a combination of preventive measures, secure communication protocols, and anomaly detection techniques can improve the detection of MitM attacks in MQTT-based IoT networks

[U.Farooq et al., 2015]. However, the trade-off between security and resource constraints remains a crucial consideration in the design and implementation of MitM detection mechanisms.

5.3 Review of Studies on Detection of Eavesdropping Attacks

The detection of eavesdropping attacks in MQTT-based IoT networks has been a subject of considerable research and investigation. Eavesdropping attacks involve an unauthorized entity intercepting and accessing MQTT communications between IoT devices, potentially leading to the exposure of sensitive information or unauthorized surveillance.

Numerous studies have proposed detection methods and techniques to address the challenge of detecting eavesdropping attacks in MQTT-based IoT networks. These methods encompass cryptographic protocols, secure communication mechanisms, traffic analysis, and anomaly detection approaches [Hoang et al., 2020]. Cryptographic protocols, such as Transport Layer Security (TLS), can be employed to encrypt MQTT messages and ensure the confidentiality and integrity of the communication. Secure communication mechanisms, such as secure key exchange algorithms, authentication, and access control mechanisms, are crucial for preventing unauthorized access to MQTT messages. Traffic analysis techniques involve monitoring network traffic patterns and analyzing data to identify suspicious activities or unauthorized access attempts. Anomaly detection approaches leverage machine learning algorithms or statistical models to identify deviations from normal communication behaviour, enabling the detection of potential eavesdropping attacks.

In an analysis of literature, robust security measures for MQTT-based IoT networks are emphasized as crucial to detecting and preventing eavesdropping attacks. Researchers highlight the importance of end-to-end encryption, strong authentication mechanisms, and secure communication protocols [Hoang et al., 2020]. Additionally, the need for continuous monitoring and real-time analysis of network traffic patterns is underscored to identify and respond promptly to eavesdropping attempts.

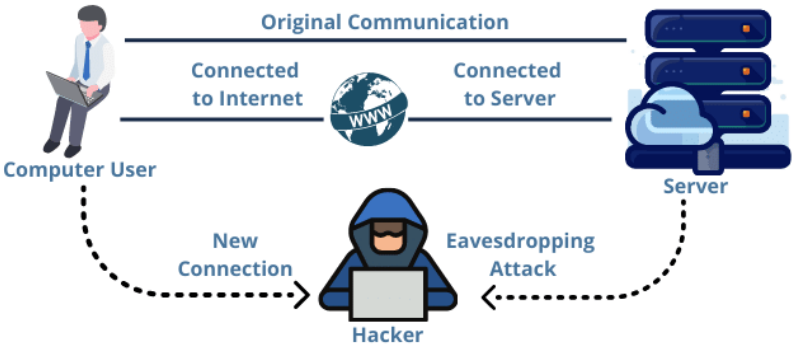

Figure 7:- Detection of Eavesdropping Attack Network (*Detection of Eavesdropping Attack Network Projects*,)

Considering what is evident from the review, detecting eavesdropping attacks in MQTT-based IoT networks requires a comprehensive approach that combines cryptographic protocols, secure communication mechanisms, traffic analysis, and anomaly detection techniques. Nonetheless, these measures should be implemented in a way that balances efficiency with security for IoT devices.

5.4 Review of Studies on Detection of Message Tampering Attacks

The detection of message tampering attacks in MQTT-based IoT networks has garnered considerable attention in the existing literature. Message tampering attacks involve unauthorized modification or alteration of MQTT messages, which can result in the manipulation of data, unauthorized control over IoT devices, or the dissemination of false information.

Researchers have proposed various approaches for detecting message tampering attacks in MQTT-based IoT networks [Zahra et al., 2015]. These approaches encompass cryptographic techniques, integrity checking mechanisms, digital signatures, and anomaly detection methods. Cryptographic techniques, such as message authentication codes (MACs) or digital signatures ensure the integrity and authenticity of MQTT messages, making it possible to detect any unauthorized modifications. Integrity checking mechanisms involve verifying the integrity of MQTT messages by comparing message hashes or checksums. Digital signatures provide a means to verify the sender's identity and ensure the integrity of the message content. Anomaly detection methods analyze message patterns, behaviour, or content to identify any deviations from the expected behaviour and identify potential message tampering attacks [Zahra et al., 2015].

Message tampering attacks in MQTT-based IoT networks can be detected and mitigated with robust security measures, according to the literature review. Message integrity and authentication, as well as strong cryptographic algorithms, as well as secure key management practices, are key factors emphasized by researchers. Furthermore, continuous monitoring of message traffic and anomaly detection techniques can aid in the early detection of message tampering attempts.

Overall, the review suggests that a combination of cryptographic techniques, integrity checking mechanisms, digital signatures, and anomaly detection methods is crucial for effective detection of message tampering attacks in MQTT-based IoT networks. However, the implementation should consider the computational and resource constraints of IoT devices to ensure practicality and efficiency.

5.5 Comparison of Literature Review

The comparison of the literature review on the detection of DoS attacks, Man-in-the-Middle attacks, eavesdropping attacks, and message tampering attacks in MQTT-based IoT networks highlights common themes, challenges, and varying approaches among these different types of attacks as given in table below.

Table 3: Comparison of Detection Methodologies for Different Types of Attacks in MQTT-Based IoT Networks

Ref	Methodology	Research Metrics	Remarks
[Zantalis et al., 2019]	Detection of DoS Attacks	Detection methods: Traffic analysis, anomaly detection, machine learning-based approaches, and network-level defenses	Strengths: Effective identification of abnormal traffic patterns. Limitations: Struggle with distinguishing legitimate and malicious traffic. Challenges: Requires substantial training data and computational resources.
[Mineraud et al., 2016]	Attack detection using man-in-the-middle techniques.	Detection approaches: Cryptographic techniques, authentication mechanisms, secure key exchange protocols, and anomaly detection methods	Challenges: Resource-constrained IoT devices, efficient cryptographic algorithms and protocols, dynamic nature of IoT networks, and trade-off between security and resource constraints.
[Hoang et al., 2020]	Detection of Eavesdropping Attacks	Detection methods: Cryptographic protocols, secure communication mechanisms, traffic analysis, and anomaly detection approaches	Challenges: End-to-end encryption, strong authentication mechanisms, secure communication protocols, continuous monitoring, and balancing efficiency with security for IoT devices.

[Zahra Jafargholi et al., 2015]	Detection of Message Tampering Attacks	Detection approaches: Cryptographic techniques, integrity checking mechanisms, digital signatures, and anomaly detection methods	Challenges: Message integrity and authentication, strong cryptographic algorithms, resource constraints of IoT devices, and computational efficiency.

6. Research Gaps and Challenges

6.1 Limitations of Existing ML-Based Detection Methods

While machine learning (ML)-based detection methods show promise in detecting communication attacks in MQTT-based IoT networks, they are not without their limitations. Research gaps must be filled in order to improve the effectiveness of ML-based detection methods.

One limitation is the reliance on labelled training datasets. ML models require large amounts of accurately labelled data to achieve high detection accuracy [Mineraud et al., 2016]. However, acquiring labelled datasets that encompass various attack scenarios and cover the evolving threat landscape can be challenging. The availability of diverse and representative training data is crucial for training ML models to generalize well and accurately detect both known and unknown attacks.

Another limitation is the vulnerability of ML models to adversarial attacks. Adversarial attacks involve intentionally manipulating input data to mislead ML models and bypass detection mechanisms [Mineraud et al., 2016]. Adversaries can exploit vulnerabilities in ML models and their underlying algorithms, leading to potential false negatives or false positives. Developing ML models that are robust against adversarial attacks and can withstand various evasion techniques is a significant research challenge.

Furthermore, the resource constraints of IoT devices pose limitations on the computational capabilities required for ML-based detection methods [Rizvi et al., 2018]. ML models often require substantial computational resources and memory, making their deployment on resource-constrained IoT devices challenging. Research efforts are needed to develop lightweight ML models that can be efficiently implemented on IoT devices without compromising detection accuracy.

6.2 Challenges in Real-World Deployment

Deploying detection methods for communication attacks in real-world MQTT-based IoT networks presents several challenges. One challenge is the heterogeneity and diversity of IoT devices, networks, and protocols. MQTT-based IoT networks often consist of a wide range of devices with varying capabilities and configurations [Rizvi et al., 2018]. Adapting detection methods to different IoT environments and ensuring interoperability is a complex task.

Another challenge is the need for real-time detection and response. MQTT-based IoT networks require timely detection and mitigation of communication attacks to minimize the potential damage. However, the limited computational resources and latency constraints of IoT devices may hinder real-time detection. Efficient algorithms and optimized detection mechanisms are needed to meet the real-time requirements of IoT networks.

Moreover, the scalability of detection methods is a significant challenge. MQTT-based IoT networks can encompass thousands or even millions of devices, generating massive amounts of network traffic [Sicari et al., 2015]. Scalable detection methods that can handle the increasing volume of traffic and adapt to the dynamic nature of IoT networks are crucial for effective deployment.

6.3 Scalability and Performance Issues

Scalability and performance are critical considerations when deploying detection methods for MQTT-based IoT networks. It is crucial that the detection system scales appropriately as IoT devices and MQTT traffic increase.

One scalability challenge is the efficient processing of large-scale MQTT message streams. Detection methods need to be able to analyze and classify incoming messages in real-time without significant delays. Scaling ML models and algorithms to handle the increasing traffic volume and maintaining a low detection latency is a research area that requires attention.

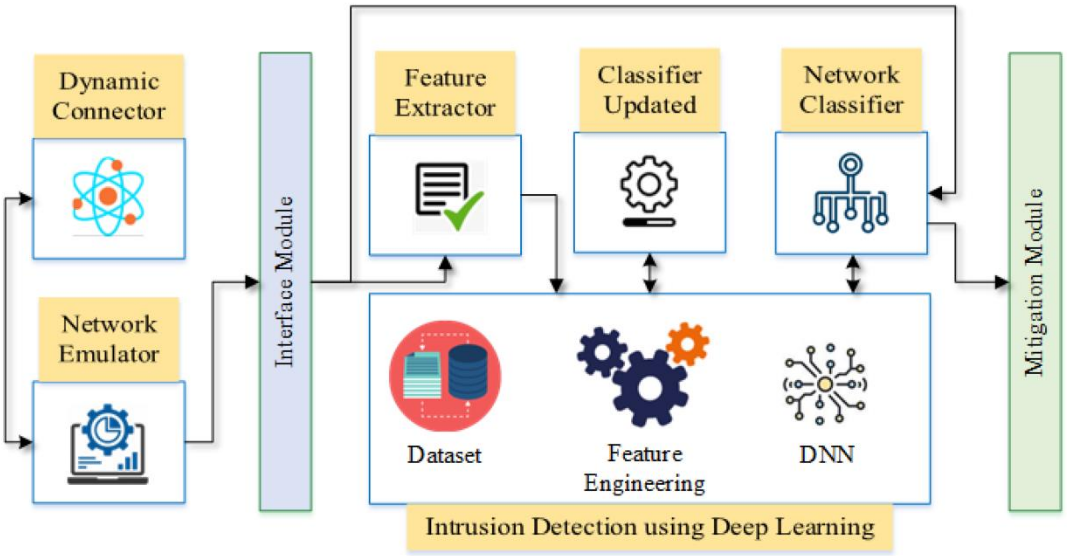

Figure 8:- Scalability for MQTT-based IoT networks. (Awajan, 2023)

Performance issues also arise due to the computational requirements of ML-based detection methods [Koroniotis et al., 2019]. Training and inference processes can be computationally intensive, especially for complex ML models. Striking a balance between detection accuracy and computational efficiency is crucial for practical deployment in resource-constrained IoT devices.

Additionally, the energy consumption of detection methods is a concern, particularly for battery-powered IoT devices. ML models and algorithms that consume excessive energy can drain the device's battery quickly. Developing energy-efficient detection techniques that optimize power consumption without compromising detection accuracy is a research challenge.

6.4 Interpretability and Explainability of ML Models

The interpretability and explainability of ML models used for detecting communication attacks in MQTT-based IoT networks are important factors [Zhang et al., 2020]. Understanding the decision-making process of ML models is crucial for gaining insights into the reasons behind their classifications and identifying potential vulnerabilities or biases.

However, many ML models, such as deep learning models, are often considered black boxes, meaning their internal workings and decision-making processes are not easily interpretable or explainable. This lack of interpretability can be problematic in the context of detecting communication attacks in MQTT-based IoT networks, as it becomes challenging to understand why a certain decision was made or to identify potential false positives or false negatives [Zhang et al., 2020].

Explainability and interpretability are particularly important in security-critical applications, where trust and accountability depend on explaining and justifying decisions made. In the case of ML-based detection methods, being able to explain why a certain MQTT communication was flagged as an attack or not can help security analysts in investigating and responding to potential threats.

Addressing the interpretability and explainability challenge requires developing techniques that can shed light on the inner workings of ML models. This can involve using methods such as model visualization, feature importance analysis, or generating explanations for individual predictions [Puiutta et al., 2020]. By providing insights into the factors influencing the detection decision, these techniques can help validate the reliability of ML models and improve their trustworthiness.

Furthermore, the explainability of ML models can also aid in identifying vulnerabilities and potential biases. ML models trained on biased or incomplete datasets can inadvertently discriminate against certain classes or exhibit biased behaviour. By understanding the decision-making process, it becomes possible to detect and mitigate such biases, ensuring fair and unbiased detection of communication attacks.

A new generation of machine learning models specifically designed for detecting communication attacks on MQTT-based IoT networks is being developed by researchers. These efforts aim to strike a balance between the complexity of ML models and the need for transparency and accountability. By addressing interpretability and explainability challenges, ML-based detection methods can become more trustworthy and reliable [Puiutta et al., 2020].

6.5 Addressing the Issue of False Positives and False Negatives

MQTT-based IoT networks face the challenge of false positives and false negatives when detecting communication attacks. A false positive is generated when legitimate MQTT communications are flagged incorrectly as attacks, while a false negative occurs when the actual attack is undetected.

False positives can be disruptive and burdensome for network administrators, as they can lead to unnecessary investigations and resource allocation [Zarpelão et al., 2017]. On the other hand, false negatives can pose serious security risks, allowing attacks to go unnoticed and potentially causing substantial damage.

Addressing the issue of false positives and false negatives requires finding a balance between detection accuracy and minimizing errors [Zarpelão et al., 2017]. ML-based detection methods can be fine-tuned to optimize their performance and reduce false positives or false negatives.

One approach to mitigating false positives and false negatives is through feature engineering and selection. By carefully choosing relevant features and designing effective feature extraction techniques, ML models can focus on the most discriminative aspects of MQTT communications, reducing the likelihood of false detections.

Moreover, the choice of ML algorithms and their hyper parameters can also influence the detection performance. Different algorithms have varying sensitivities and specificities, and finding the right combination for the given application is essential. Additionally, parameter tuning and optimization techniques can further refine the models' performance and strike a balance between false positives and false negatives.

Continuous monitoring and feedback loops are crucial for improving the detection accuracy over time. By collecting feedback from network administrators and security analysts, ML models can adapt and learn from misclassifications, thereby reducing false positives and false negatives in subsequent detections.

Furthermore, incorporating ensemble techniques, such as combining multiple ML models or employing hybrid approaches that leverage rule-based systems alongside ML models, can help improve the overall detection accuracy and mitigate the issue of false positives and false negatives.

However, it is important to note that completely eliminating false positives and false negatives is challenging, as it requires striking a delicate balance and considering the trade-offs between different detection objectives [U.Farooq et al., 2015]. Detection methods should be designed with a comprehensive understanding of the specific MQTT-based IoT network, its characteristics, and the acceptable levels of false positives and false negatives.

To address the issue of false positives and false negatives, it is essential to adopt a multi-faceted approach. The first step in minimizing false positives and false negatives is to improve the quality and diversity of the training dataset. This involves collecting and labelling data that adequately represents both normal MQTT communications and various attack scenarios. By ensuring a comprehensive dataset, ML models can learn to differentiate between legitimate and malicious traffic more accurately.

Additionally, on-going monitoring and feedback loops are crucial for refining the detection system's performance. Network administrators and security analysts can provide valuable insights and feedback on flagged communications [U.Farooq et al., 2015], helping to identify false positives and false negatives. This feedback can be used to update and retrain ML models, enhancing their ability to distinguish between benign and malicious MQTT communications.

Furthermore, IoT networks and the threat landscape are continuously evolving, making it important to take these factors into account. Regular updates and adaptations to the ML models and detection mechanisms are necessary to address new attack vectors and techniques. Continuous research and development efforts are required to stay ahead of emerging threats and to maintain a high level of detection accuracy.

Collaboration and information sharing among different stakeholders, such as IoT device manufacturers, network operators, and security researchers, can also contribute to reducing false positives and false negatives. Sharing insights, best practices, and threat intelligence can help identify common patterns and improve the overall effectiveness of detection methods.

Furthermore, implementing a feedback loop that involves human experts can provide an added layer of scrutiny and decision-making. By combining the capabilities of ML models with human expertise, it is possible to achieve a more reliable and robust detection system. Human analysts can review flagged communications, investigate suspicious activities, and make informed decisions based on their domain knowledge and experience.

In conclusion, detecting communication attacks in IoT networks using MQTT requires a comprehensive approach to avoid false positives and false negatives. This involves fine-tuning ML models, optimizing detection algorithms, continuously monitoring and updating the system, incorporating feedback loops, and leveraging human expertise. By striving for a balance between detection accuracy and minimizing errors, the reliability and effectiveness of ML-based detection methods can be improved, enhancing the security of MQTT-based IoT networks.

7. Future Directions

7.1 Enhanced Feature Engineering and Data Preprocessing

There is a need for enhanced feature engineering and data pre-processing techniques as ML-based detection methods for communication attacks in MQTT-based IoT networks continue to evolve [Frustaci et al., 2018]. Feature engineering plays a critical role in identifying relevant and discriminative features from the MQTT communication data. By extracting meaningful features, ML models can better capture the characteristics of normal and malicious traffic.

Future research should focus on developing advanced feature engineering techniques that can handle the complexity and diversity of MQTT-based IoT networks [Frustaci et al., 2018]. This may involve exploring new ways to extract temporal, spatial, and semantic features from MQTT messages. Additionally, incorporating domain knowledge and expert insights can further enhance feature engineering, ensuring that the extracted features are both relevant and informative.

Data pre-processing is another area that requires attention. Pre-processing techniques such as data normalization, outlier detection, and missing value handling can significantly impact the performance of ML models. It is recommended that future research explores innovative methods to preprocess MQTT communication data in order to improve the detection system's performance and reliability.

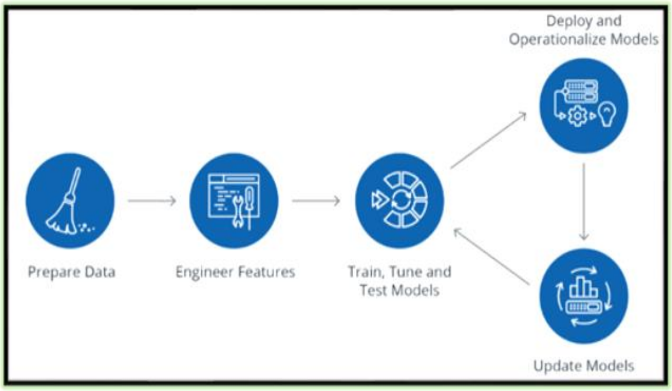

Figure 9:- Feature Improvement [Ali et al., 2023]

Furthermore, leveraging advanced data augmentation techniques, such as generative models, can help address the challenge of limited labelled datasets [Zamora-Izquierdo et al., 2019]. Data augmentation can artificially expand the training dataset by generating synthetic samples, enabling ML models to learn from a broader range of scenarios and improve their generalization capabilities.

7.2 Integration of Multiple Security Mechanisms

It is crucial that multiple security mechanisms are incorporated into MQTT-based IoT networks to enhance their overall security. ML-based detection methods can be strengthened by combining them with other security measures, such as anomaly detection systems, intrusion detection systems, and secure communication protocols.

Anomaly detection systems can complement ML models by identifying abnormal behaviour and deviations from normal communication patterns [Perera et al., 2012]. By leveraging anomaly detection techniques alongside ML-based detection methods, a comprehensive defense mechanism can be established to detect both known and unknown attacks.

Intrusion detection systems (IDS) can also be integrated to provide additional layers of protection. IDS can analyze network traffic, identify potential threats, and trigger alerts or take proactive measures to prevent attacks. By combining ML-based detection methods with IDS, the network's security posture can be further enhanced.

TLS (Transport Layer Security) protocols can also protect against eavesdropping and message tampering with an additional layer of security. Integrating ML-based detection methods with secure communication protocols ensures end-to-end security and enhances the overall robustness of MQTT-based IoT networks [Perera et al., 2012].

7.3 Explainable and Interpretable ML Models

The demand for explainable and interpretable ML models is growing rapidly, especially in security-critical applications such as detecting communication attacks in MQTT-based IoT networks [Azodi et al., 2020]. Explainability and interpretability allow security analysts to understand and trust the decisions made by ML models, increasing transparency and accountability.

Future research should focus on developing ML models that are inherently explainable and interpretable. This involves exploring model architectures and algorithms that generate human-understandable explanations for their decisions. Techniques such as rule extraction, attention mechanisms, and model visualization can aid in understanding the key factors influencing the ML models' classifications [Azodi et al., 2020].

Additionally, developing methods to quantify the uncertainty and confidence of ML models can contribute to their interpretability. Uncertainty estimation techniques, such as Bayesian approaches or ensemble methods, can provide insights into the models' confidence levels and identify cases where the models' decisions may be less reliable.

7.4 Real-Time Detection and Response

Real-time detection and response are crucial in MQTT-based IoT networks to mitigate the potential impact of communication attacks. ML-based detection methods should be designed to operate in real-time, providing timely alerts and responses to detected threats.

To achieve real-time detection, research efforts should focus on optimizing the computational efficiency of ML algorithms [Thangavel et al., 2014]. This involves developing lightweight ML models and designing efficient algorithms that can operate with minimal latency. Additionally, leveraging distributed computing and parallel processing techniques can help improve the scalability of ML-based detection systems, allowing them to handle the increasing volume of MQTT traffic in real-time.

Furthermore, integrating automated response mechanisms into the detection system can enable immediate actions to be taken upon detecting communication attacks. This can involve triggering predefined countermeasures, isolating affected devices, or dynamically adjusting network configurations to mitigate the impact of the attacks [Verma et al., 2019]. The development of intelligent response algorithms and decision-making frameworks will be essential for effective real-time detection and response.

7.5 Scalable and Resource-Efficient ML Algorithms

It is becoming increasingly important for ML algorithms to be scalable and resource-efficient as MQTT-based IoT networks expand in scope and complexity. Devices with limited memory and computational power often make complex ML models challenging to deploy. Therefore, developing lightweight ML algorithms that can operate efficiently on IoT devices without compromising detection accuracy is crucial [Guindon et al., 2010].

Research efforts should focus on designing novel ML architectures and algorithms that are specifically tailored for resource-constrained IoT environments. Techniques such as model compression, parameter sharing, and efficient model deployment can help reduce the computational and memory requirements of ML-based detection methods. Additionally, exploring edge computing approaches, where the ML models are deployed directly on IoT devices or gateways, can further improve the scalability and resource efficiency of the detection system.

Moreover, leveraging distributed ML techniques, such as federated learning or edge-to-cloud collaboration, can enable collaborative model training and inference across multiple IoT devices [Hussain et al., 2020]. MQTT-based IoT networks can take advantage of this distributed approach to distribute computational load and enhance scalability.

8. Conclusion

8.1 Summary of Key Findings

In summary, ML-based detection methods show promise in detecting communication attacks in MQTT-based IoT networks. However, several challenges and research directions need to be addressed to further improve their effectiveness and practical deployment.

The limitations of existing ML-based detection methods, including the reliance on labelled training datasets, vulnerability to adversarial attacks, and resource constraints of IoT devices, need to be overcome. Our focus is on enhancing feature engineering and data preprocessing techniques, integrating multiple security mechanisms, and developing ML models that can be explained and interpreted.

Real-time detection and response capabilities, along with scalable and resource-efficient ML algorithms, are essential to handle the growing volume of MQTT traffic and ensure timely protection of IoT networks.

8.2 Importance of ML-Based Detection Methods

ML-based detection methods have the potential to enhance the security of MQTT-based IoT networks by enabling proactive and intelligent detection of communication attacks. Detecting both known and unknown attacks, adjusting to changing threat landscapes, and providing real-time insight into incident response are key benefits offered by these solutions.

By leveraging the power of ML, IoT networks can benefit from automated and intelligent security mechanisms that can detect anomalies, identify malicious patterns, and protect the integrity and confidentiality of MQTT communications.

Table 3:- Table Highlighting The Importance Of Machine Learning (ML)-Based Detection Methods [Chen et al., 2020].

Importance of ML-Based Detection Methods	**Description**
Anomaly detection	ML algorithms can learn the normal behaviour patterns of MQTT-based IoT networks and detect anomalies or suspicious activities that deviate from the norm. This helps in identifying potential security breaches and attacks.
Intrusion detection	ML models can analyze MQTT network traffic and detect unauthorized access attempts or malicious activities. ML-based intrusion detection systems (IDS) can identify patterns indicative of known attacks and also adapt to new and emerging threats.
Malware detection	ML techniques can be used to develop models that identify malware or malicious code within MQTT messages. These models can analyze message payloads, extract features, and classify them as normal or malicious, enabling proactive detection and prevention of malware attacks.
Zero-day attack detection	ML algorithms can learn from historical MQTT network data to detect previously unseen attack patterns. By analyzing network behaviour, ML-based systems can identify zero-day attacks and take appropriate action to mitigate the risks.
DDoS attack detection	MQTT network traffic can be monitored with ML models, and distributed denial-of-service (DDoS) attacks can be detected with ML models. ML-based detection systems help prevent service disruptions by identifying legitimate traffic from abnormal traffic generated by botnets through analysis of network traffic patterns.
Adaptive security	ML-based detection methods can adapt to evolving security threats and changes in MQTT network behaviour. By continuously learning and updating their models, these systems can provide adaptive security measures, improving the overall resilience of the IoT network.
Improved threat intelligence	ML algorithms can analyze large volumes of MQTT network data to generate insights and improve threat intelligence. By detecting patterns, correlations, and anomalies, ML-based detection methods can provide valuable information for security analysts and aid in proactive threat mitigation.

8.3 Future Outlook and Recommendations

To advance ML-based detection methods for communication attacks in MQTT-based IoT networks, collaboration between researchers, industry experts, and stakeholders is crucial. Interdisciplinary efforts that combine expertise from machine learning, cyber security, IoT, and network protocols can lead to innovative solutions that address the unique challenges of this domain.

Furthermore, the development of standardized datasets, benchmarks, and evaluation metrics specific to MQTT-based IoT networks can facilitate fair comparisons and objective assessments of different ML-based detection methods. This will enable the research community to identify best practices and foster the development of robust and reliable detection systems.

Additionally, close collaboration with industry partners and IoT device manufacturers is necessary to ensure the practical applicability and scalability of ML-based detection methods. As a result of industry involvement, insights into real-world deployment challenges can be gained, data sources and datasets can be identified, and standard security protocols and practices can be developed for MQTT-based IoT networks [Abu Al-Haija, 2022].

MQTT-based IoT networks that rely on machine learning-based detection methods have a promising future in terms of ML-based detection methods. By addressing the identified research directions and leveraging collaborative efforts, we can overcome the current limitations and advance the field to create more scalable, efficient, and effective ML-based detection systems for communication attacks in MQTT-based IoT networks.

Improving the scalability of ML-based detection systems is crucial to handle the increasing volume of MQTT traffic in real-time. By developing lightweight ML algorithms specifically tailored for resource-constrained IoT environments, we can ensure efficient operation on IoT devices without compromising detection accuracy. Techniques such as model compression, parameter sharing, and efficient model deployment can help reduce computational and memory requirements. Additionally, exploring edge computing approaches, where ML models are deployed directly on IoT devices or gateways, can further enhance scalability and resource efficiency.

Distributed ML techniques, such as federated learning or edge-to-cloud collaboration, offer opportunities for collaborative model training and inference across multiple IoT devices. This distributed approach not only distributes the computational load but also enhances scalability by leveraging the collective knowledge of diverse IoT devices.

IoT networks based on MQTT can be strengthened through the use of ML-based detection methods. Our goal is to ensure practical deployment of these systems by addressing the challenges of scalability and resource efficiency. Collaborative efforts between researchers, industry experts, and stakeholders are crucial to advance the field and develop standardized protocols, datasets, and evaluation metrics. With continued research and development, ML-based detection methods can play a vital role in protecting MQTT-based IoT networks from communication attacks, contributing to the security and reliability of IoT deployments in the future.

References

[1] Abu Al-Haija, Q. (2022). Top-Down Machine Learning-Based Architecture for Cyberattacks Identification and Classification in IoT Communication Networks. *Frontiers in Big Data*, *4*. https://doi.org/10.3389/fdata.2021.782902

[2] Aitzhan, N. Z., & Svetinovic, D. (2018). Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Transactions on Dependable and Secure Computing*, *15*(5), 840–852. https://doi.org/10.1109/tdsc.2016.2616861

[3] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2019). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376. https://doi.org/10.1109/comst.2015.2444095

[4] Al-Fuqaha, A., Khreishah, A., Guizani, M., Rayes, A., & Mohammadi, M. (2015). Toward better horizontal integration among IoT services. *IEEE Communications Magazine*, *53*(9), 72–79.

https://doi.org/10.1109/mcom.2015.7263375

[5] Ali, T. E., Chong, Y.-W., & Manickam, S. (2023). Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. *Applied Sciences*, *13*(5), 3183. https://doi.org/10.3390/app13053183

[6] Álvaro Michelena Grandío, Aveleira-Mata, J., Jove, E., Martín Bayón-Gutiérrez, Paulo Novais, Fontenla-Romero, O., José Luis Calvo-Rolle, & Héctor Alaiz-Moretón. (2023). *A novel intelligent approach for man-in-the-middle attacks detection over internet of things environments based on message queuing telemetry transport*. https://doi.org/10.1111/exsy.13263

[7] Awajan, A. (2023). A Novel Deep Learning-Based Intrusion Detection System for IoT Networks. *Computers*, *12*(2), 34. https://doi.org/10.3390/computers12020034

[8] Azodi, C. B., Tang, J., & Shiu, S.-H. (2020). Opening the Black Box: Interpretable Machine Learning for Geneticists. *Trends in Genetics*, *36*(6), 442–455. https://doi.org/10.1016/j.tig.2020.03.005

[9] Celebi, M. E., & Aydin, K. (Eds.). (2016). *Unsupervised Learning Algorithms*. Springer International Publishing. https://doi.org/10.1007/978-3-319-24211-8

[10] Chen, F., Huo, Y., Zhu, J., & Fan, D. (2020, November 1). *A Review on the Study on MQTT Security Challenge*. IEEE Xplore. https://doi.org/10.1109/SmartCloud49737.2020.00032

[11] Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. *BMC Genomics*, *21*(1). https://doi.org/10.1186/s12864-019-6413-7

[12] *Detection of Eavesdropping Attack Network Projects*. (n.d.). Network Simulation Tools. https://networksimulationtools.com/eavesdropping-attack-network-projects/

[13] erlikaya, O. Y., & Gokhan Dalkiltc. (2018). *Authentication and Authorization Mechanism on Message Queue Telemetry Transport Protocol*. https://doi.org/10.1109/ubmk.2018.8566599

[14] Firdous, S. N., Baig, Z., Valli, C., & Ibrahim, A. (2017, June 1). *Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol*. IEEE Xplore. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.115

[15] Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet of Things Journal*, *5*(4), 2483–2495. https://doi.org/10.1109/jiot.2017.2767291

[16] Guindon, S., Dufayard, J.-F., Lefort, V., Anisimova, M., Hordijk, W., & Gascuel, O. (2010). New Algorithms and Methods to Estimate Maximum-Likelihood Phylogenies: Assessing the Performance of PhyML 3.0. *Systematic Biology*, *59*(3), 307–321. https://doi.org/10.1093/sysbio/syq010

[17] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access*, *7*, 82721–82743. https://doi.org/10.1109/access.2019.2924045

[18] Hernández Ramos, S., Villalba, M. T., & Lacuesta, R. (2018). MQTT Security: A Novel Fuzzing Approach. *Wireless Communications and Mobile Computing*, *2018*, 1–11. https://doi.org/10.1155/2018/8261746

[19] Hesamian, M. H., Jia, W., He, X., & Kennedy, P. (2019). Deep Learning Techniques for Medical Image Segmentation: Achievements and Challenges. *Journal of Digital Imaging*, *32*(4), 582–596. https://doi.org/10.1007/s10278-019-00227-x

[20] Hindy, H., Bayne, E., Bures, M., Atkinson, R., Tachtatzis, C., & Bellekens, X. (2021). Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset). *Selected Papers from the 12th International Networking Conference*, 73–84. https://doi.org/10.1007/978-3-030-64758-2_6

[21] Hoang, T. M., Nguyen, N. M., & Duong, T. Q. (2020). Detection of Eavesdropping Attack in UAV-Aided Wireless Systems: Unsupervised Learning With One-Class SVM and K-Means Clustering. *IEEE Wireless*

Communications Letters, *9*(2), 139–142. https://doi.org/10.1109/lwc.2019.2945022

[22] Hosseini, S., & Azizi, M. (2019). The hybrid technique for DDoS detection with supervised learning algorithms. *Computer Networks*, *158*, 35–45. https://doi.org/10.1016/j.comnet.2019.04.027

[23] Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys Tutorials*, *22*(3), 1686–1721. https://doi.org/10.1109/COMST.2020.2986444

[24] Hussein, N., & Nhlabatsi, A. (2022). Living in the Dark: MQTT-Based Exploitation of IoT Security Vulnerabilities in ZigBee Networks for Smart Lighting Control. *IoT*, *3*(4), 450–472. https://doi.org/10.3390/iot3040024

[25] Hussein, N., & Nhlabatsi, A. (2022). Living in the Dark: MQTT-Based Exploitation of IoT Security Vulnerabilities in ZigBee Networks for Smart Lighting Control. *IoT*, *3*(4), 450–472. https://doi.org/10.3390/iot3040024

[26] Javeed, D., Gao, T., Khan, M. T., & Ahmad, I. (2021). A Hybrid Deep Learning-Driven SDN Enabled Mechanism for Secure Communication in Internet of Things (IoT). *Sensors*, *21*(14), 4884. https://doi.org/10.3390/s21144884

[27] Kadari, P. (2021, February 21). *Introduction to Reinforcement Learning for Beginners*. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2021/02/introduction-to-reinforcement-learning-for-beginners/

[28] Kang, J. J., Fahd, K., Venkatraman, S., Trujillo-Rasua, R., & Haskell-Dowland, P. (2019). Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks. *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*. https://doi.org/10.1109/itnac46935.2019.9077977

[29] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

[30] Khan, M. A., Khan, M. A., Jan, S. U., Ahmad, J., Jamal, S. S., Shah, A. A., Pitropakis, N., & Buchanan, W. J. (2021). A Deep Learning-Based Intrusion Detection System for MQTT Enabled IoT. *Sensors*, *21*(21), 7016. https://doi.org/10.3390/s21217016

[31] Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. *Future Generation Computer Systems*, *100*, 779–796. https://doi.org/10.1016/j.future.2019.05.041

[32] Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. *Future Generation Computer Systems*, *100*, 779–796. https://doi.org/10.1016/j.future.2019.05.041

[33] Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., & Guizani, S. (2017). Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. *IEEE Communications Magazine*, *55*(9), 16–24. https://doi.org/10.1109/mcom.2017.1600514

[34] Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2016). A gap analysis of Internet-of-Things platforms. *Computer Communications*, *89-90*, 5–16. https://doi.org/10.1016/j.comcom.2016.03.015

[35] Mohamad Noor, M. binti, & Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, *148*, 283–294. https://doi.org/10.1016/j.comnet.2018.11.025

[36] Møller, M. F. (1993). A scaled conjugate gradient algorithm for fast supervised learning. *Neural Networks*, *6*(4), 525–533. https://doi.org/10.1016/s0893-6080(05)80056-5

[37] P., H., & K., K. (2019). Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. *EURASIP Journal on Wireless Communications and Networking*, *2019*(1). https://doi.org/10.1186/s13638-019-1402-8

[38] Perera, L. P., Oliveira, P., & Guedes Soares, C. (2012). Maritime Traffic Monitoring Based on Vessel

Detection, Tracking, State Estimation, and Trajectory Prediction. *IEEE Transactions on Intelligent Transportation Systems*, *13*(3), 1188–1200. https://doi.org/10.1109/tits.2012.2187282

[39] Puiutta, E., & Veith, E. M. S. P. (2020). Explainable Reinforcement Learning: A Survey. *Lecture Notes in Computer Science*, 77–95. https://doi.org/10.1007/978-3-030-57321-8_5

[40] Rahman, A., Roy, S., Kaiser, M. S., & Islam, Md. S. (2018, December 1). *A Lightweight Multi-tier S-MQTT Framework to Secure Communication between low-end IoT Nodes*. IEEE Xplore. https://doi.org/10.1109/NSysS.2018.8631379

[41] ResearchGate. (2015). *ResearchGate | Share and discover research*. ResearchGate; ResearchGate. https://www.researchgate.net

[42] Rizvi, S., Kurtz, A., Pfeffer, J., & Rizvi, M. (2018). Securing the Internet of Things (IoT): A Security Taxonomy for IoT. *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*. https://doi.org/10.1109/trustcom/bigdatase.2018.00034

[43] Sanjuan, E. B., Cardiel, I. A., Cerrada, J. A., & Cerrada, C. (2020). Message Queuing Telemetry Transport (MQTT) Security: A Cryptographic Smart Card Approach. *IEEE Access*, *8*, 115051–115062. https://doi.org/10.1109/ACCESS.2020.3003998

[44] Sathya, R., & Abraham, A. (2013). Comparison of Supervised and Unsupervised Learning Algorithms for Pattern Classification. *International Journal of Advanced Research in Artificial Intelligence*, *2*(2). https://doi.org/10.14569/ijarai.2013.020206

[45] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

[46] Singh, M., Rajan, M., V. Shivraj, & P. Balamuralidhar. (2015). *Secure MQTT for Internet of Things (IoT)*. 2015 Fifth International Conference on Communication Systems and Network Technologies. https://www.semanticscholar.org/paper/Secure-MQTT-for-Internet-of-Things-(IoT)-Singh-Rajan/96cf91f36ea3711277ae72426820a0b25f409d61/figure/0

[47] Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

[48] Tesauro, G., Jong, N. K., Das, R., & Bennani, M. (2006). A Hybrid Reinforcement Learning Approach to Autonomic Resource Allocation. *International Conference on Autonomic Computing*. https://doi.org/10.1109/icac.2006.1662383

[49] Thangavel, D., Ma, X., Valera, A., Tan, H.-X., & Tan, C. K.-Y. (2014, April 1). *Performance evaluation of MQTT and CoAP via a common middleware*. IEEE Xplore. https://doi.org/10.1109/ISSNIP.2014.6827678

[50] Tran, M.-Q., Elsisi, M., Liu, M.-K., Vu, V. Q., Mahmoud, K., Darwish, M. M. F., Abdelaziz, A. Y., & Lehtonen, M. (2022). Reliable Deep Learning and IoT-Based Monitoring System for Secure Computer Numerical Control Machines Against Cyber-Attacks With Experimental Verification. *IEEE Access*, *10*, 23186–23197. https://doi.org/10.1109/ACCESS.2022.3153471.

[51] U.Farooq, M., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A Review on Internet of Things (IoT). *International Journal of Computer Applications*, *113*(1), 1–7. https://doi.org/10.5120/19787-1571

[52] Wang, D., Chen, D., Song, B., Guizani, N., Yu, X., & Du, X. (2018). From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies. *IEEE Communications Magazine*, *56*(10), 114–120. https://doi.org/10.1109/mcom.2018.1701310

[53] Wortmann, F., & Flüchter, K. (2015). Internet of Things. *Business & Information Systems Engineering*, *57*(3), 221–224. https://doi.org/10.1007/s12599-015-0383-3

[54] Yassein, M. B., Shatnawi, M. Q., Aljwarneh, S., & Al-Hatmi, R. (2017). Internet of Things: Survey and open issues of MQTT protocol. *2017 International Conference on Engineering & MIS (ICEMIS)*. https://doi.org/10.1109/icemis.2017.8273112

[55] Zahra Jafargholi, & Wichs, D. (2015). *Tamper Detection and Continuous Non-malleable Codes*. 451–480. https://doi.org/10.1007/978-3-662-46494-6_19

[56] Zamora-Izquierdo, M. A., Santa, J., Martínez, J. A., Martínez, V., & Skarmeta, A. F. (2019). Smart farming IoT platform based on edge and cloud computing. *Biosystems Engineering*, *177*, 4–17. https://doi.org/10.1016/j.biosystemseng.2018.10.014

[57] Zantalis, F., Koulouras, G., Karabetsos, S., & Kandris, D. (2019). A Review of Machine Learning and IoT in Smart Transportation. *Future Internet*, *11*(4), 94. https://doi.org/10.3390/fi11040094

[58] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009

[59] Zekri, M., Kafhali, S. E., Aboutabit, N., & Saadi, Y. (2017, October 1). *DDoS attack detection using machine learning techniques in cloud computing environments*. IEEE Xplore. https://doi.org/10.1109/CloudTech.2017.8284731

[60] Zhang, Y., & Chen, X. (2020). Explainable Recommendation: A Survey and New Perspectives. *Foundations and Trends® in Information Retrieval*, *14*(1), 1–101. https://doi.org/10.1561/1500000066.