e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

SECURING MQTT-BASED COMMUNICATION FOR THE AUTOMOBILE AND MEDICAL INDUSTRIES AGAINST MAN-IN-THE-MIDDLE ATTACKS

Prof. Jyothis KP*1, Ramyashree RC*2, Divya S*3

*1,2,3Dayananda Sagar Academy Of Technology And Management, India.

DOI: https://www.doi.org/10.56726/IRJMETS67132

ABSTRACT

The increasing adoption of MQTT (Message Queuing Telemetry Transport) in IoT systems has revolutionized industries like healthcare and automotive by enabling efficient, real-time communication. However, MQTT's lackof native security mechanisms exposes critical applications to cyber threats, particularly Man-in-the-Middle (MITM)attacks. These attacks can compromise sensitive dataintegrity, disrupt communication, and pose severe safetyrisks.

This paper proposes a comprehensive framework that secures MQTT communication using lightweight cryptographic algorithms, mutual authentication, and dynamic key management. By addressing the constraints of resource- limited IoT devices, the framework ensures robust security without impacting device performance. Experiments validatethe framework's ability to defend against MITM attackswhile maintaining compliance with healthcare and automotive cybersecurity standards like HIPAA and ISO/SAE 21434.

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized traditional industries by enabling interconnectivity and real-time data exchange, fundamentally transforming sectors like healthcare and automotive. At the core of many IoT systems is the MQTT protocol, widely recognized for its lightweight, publish-subscribe architecture and capacity to operate in low-bandwidth environments.[1]

These qualities make MQTT indispensable for applications in healthcare (e.g., pacemakers, insulin pumps, and wearablehealth monitors) and automotive systems (e.g., vehicle-to- everything or V2X communication), where real-time, efficient data transmission is critical for safety and reliability [1]. Despite its advantages, MQTT lacks built-in encryption or authentication, leaving it highly vulnerable to cyberattacks such as Man-in-the-Middle (MITM) attacks.

These attacks allow adversaries to intercept, eavesdrop, and manipulate communication between devices, leading to potentially catastrophic outcomes. In healthcare, MITM attacks can compromise sensitive medical data, alter criticaldevice settings, and even disrupt essential operations, endangering patient lives [2]. Similarly, in automotive systems, compromised V2X communication can disrupt essentialsafety functions, such as braking or steering, potentiallyleading to traffic accidents or system malfunctions.

As IoT adoption grows, securing MQTT communication becomes paramount to ensuring the safety, reliability, and privacy of connected systems. This paper addresses these challenges by introducing a secure MQTT framework that leverages lightweightencryption, mutual authentication, and dynamic keymanagement.

The proposed solution ensures secure, reliable communication while preserving the performance and energy efficiency of resource-constrained IoT devices. Moreover, it complies with critical industry standards such as HIPAA (Health Insurance Portability and Accountability Act) for healthcare and ISO/SAE 21434for automotive cybersecurity, making it suitable fordeployment in real-world environments [2].

By safeguarding data integrity and authenticity, theproposed framework not only mitigates the risks associated with MITM attacks but also fosters trust in IoT systems across critical industries. This researchbridges the gap between security and performance, paving the way for the secure evolution of IoT technologies in healthcare, automotive, and beyond.

II. LITERATURE REVIEW

In a recent study, Security Analysis of MQTT and Its Application in IoT (Zhang et al., 2023), the authors provide a thorough investigation into the security vulnerabilities of MQTT in large-scale IoT environments. This research focuses on how the lightweight nature of MQTT, while beneficial for efficient data transmission, leaves systems exposed to substantial security risks, particularly in sensitive sectors such as healthcare [5].

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

The study suggests that implementing end-to-end encryption (E2EE) is a critical step to securing communication, as it ensures that even if attackers intercept data, they will be unable to read or modify it. The paper emphasizes the importance of combining E2EE with mutual TLS (mTLS) to authenticate both the client and the server, thus defending against Man-in-the-Middle (MITM) attacks [4]. Additionally, it highlights the need for secure key management protocols, particularly in large-scale deployments where the volume of real-time data streams can amplify the risk of data breaches and system failures.

In another significant paper, Securing Medical IoT Systems: A Survey on MQTT-Based Communication in Healthcare (Patel et al., 2023), the authors explore the security challenges faced by medical IoT systems, which rely on MQTT for transmitting vast amounts of sensitive health data between devices, healthcare providers, and cloud-based platforms. The study stresses that because MQTT is commonly used to monitor patient vitals, track medical devices, and transmit diagnostic data, the integrity and confidentiality of these communications are paramount. The authors advocate for mutual authentication and the use of advanced encryption techniques to protect this sensitive data [6]. Furthermore, the paper discusses the necessity of fine-grained access control, ensuring that only authorized devices and personnel can access patient information. A key concern addressed is the scalability of these security measures in large-scale medical IoT networks, where hundreds or thousands of devices might be involved. The authors suggest implementing role-based access control (RBAC) in combination with time-limited tokens, as these mechanisms could effectively limit unauthorized access and reduce the risks associated with tampering.

Similarly, A Secure Architecture for MQTT-Based Communication in Vehicular Networks (Zhao et al., 2022) provides insights into the security requirements for Vehicle-to-Everything (V2X) communication systems, which are crucial for vehicle diagnostics, navigation updates, and collision detection in real-time. This paper demonstrates that MQTT, although an efficient protocol, is prone to MITM attacks, particularly in environments where the integrity of data is essential for safety. To secure such systems, the authors propose a hybrid security architecture that integrates mutual TLS (mTLS) for authentication and blockchain technology for maintaining immutable logs of the data transmitted. By utilizing blockchain, the system can ensure that once data is transmitted, it cannot be altered, thus ensuring both security and auditability. The study also acknowledges the scalability challenges in vehicular networks, particularly with the increasing number of connected vehicles, and recommends the use of a distributed Public Key Infrastructure (PKI) to facilitate the secure management of authentication and encryption keys[6].

In the realm of large-scale IoT communications, the paper Anomaly Detection in MQTT Communication: A Machine Learning Approach (Wang et al., 2023) explores how machine learning can be leveraged to detect anomalies in MQTT traffic, which is crucial for identifying sophisticated MITM or Denial-of-Service (DoS) attacks. As IoT networks handle vast amounts of data, traditional security measures might fall short of identifying complex attack patterns [7]. The study proposes a machine learning-based framework that detects abnormal patterns in MQTT message flows, such as unusual message frequency or irregular authentication attempts. By training the model on historical data from both healthcare and automotive IoT systems, the system can identify deviations from normal communication patterns in real-time, enabling faster threat detection and response.

Finally, the integration of blockchain technology in securing MQTT-based communication is explored in the paper Blockchain-Enabled Secure IoT Communication: Application to MQTT in Healthcare (Bhagat et al., 2023). The authors suggest a decentralized blockchain system to verify the integrity of MQTT messages, particularly in healthcare settings where large volumes of sensitive data are transmitted between IoT devices, hospitals, and cloud-based services. Blockchain's immutable ledger ensures that any alterations to transmitted data can be easily detected [8]. Additionally, blockchain's decentralized nature makes it scalable, as it avoids placing excessive load on the central server or MQTT broker, ensuring both security and efficiency in large IoT systems. The paper also explores how combining blockchain with edge computing can reduce latency and improve real-time data processing for time-sensitive applications, such as remote surgery or patient monitoring.

III. IMPLEMENTATION

The implementation of the proposed framework integrates lightweight encryption, mutual authentication, and dynamic key management into an MQTT communication setup, tailored for healthcare and automotive IoT

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

systems. To address the vulnerabilities of MQTT communication, the proposed framework combines encryption, mutual authentication, and dynamic key management [3]. These components ensure secure data transmission while maintaining the efficiency required for IoT devices in healthcare and automotive applications.

Lightweight encryption is used to secure the data exchanged between devices. The Advanced Encryption Standard (AES-128) is implemented to encrypt message payloads, providing strong protection with minimal computational overhead. This makes it suitable for low- power IoT devices like pacemakers and vehicle sensors[3]. Additionally, Elliptic Curve Cryptography (ECC) is employed for key exchange, ensuring that encryption keys are securely shared between devices. ECC's smaller key sizes make it more efficient than traditional methods, such asRSA, without compromising security.

To prevent unauthorized devices from accessing the communication network, **mutual authentication** is enforced. Devices authenticate each other using X.509 certificates, which are issued by a trusted Certificate Authority (CA). During the handshake process, the broker and the client verify each other's identities, ensuring that only legitimate devices can communicate. A challenge-response mechanism adds another layer of protection by verifying each device's authenticity in real-time. This preventsimpersonation attacks and ensures that attackers cannot gainunauthorized access to sensitive data [2].

The framework also incorporates **dynamic key management** to enhance security over time. Encryption keys are rotated periodically to minimize the risk of compromise. A secure key distribution protocol ensures that keys areupdated dynamically without disrupting ongoing communication. Each session generates unique keys, which are valid only for the duration of that session. This prevents attackers from using stolen keys to decrypt past or future communications. In case of device compromise, the framework supports key revocation, where compromised keys are immediately invalidated and replaced with newones.

The MQTT broker plays a crucial role in ensuring security. It is configured to enforce encryption through Transport Layer Security (TLS) for added protection and restrict unauthorized access through role-based controls. The broker also validates message integrity by embedding cryptographic hashes in the payloads, ensuring that any tampering is immediately detected. Replay attacks are mitigated by using timestamps in each message, which prevents attackers from resendingpreviously intercepted data [1].

The framework is designed to be lightweight, ensuring minimal impact on device performance. Energy-efficient cryptographic operations are implemented to preserve battery life in devices like pacemakers and vehicle sensors. Experimental validation involved testing the framework in simulated environments, including healthcare (e.g., pacemaker monitoring systems) and automotive (e.g., vehicle-to-infrastructure communication) scenarios. Simulated MITM attacks were conducted to test the framework's resilience. The results demonstrated that the framework effectively prevented these attacks while maintaining low latency and high throughput. Performance metrics such as CPUusage and memory consumption confirmed the suitability of the framework for resource-constrained IoT devices [2].

Finally, the framework was tested for compliance with industry standards. In healthcare, it adhered to HIPAA requirements by ensuring data confidentiality and integrity. In automotive systems, it met ISO/SAE 21434 standards by addressing the cybersecurity needs of V2X communication. The implementation proved scalable, handling increasing device numbers and message sizes without compromising security or performance.

IV. RELATED WORK

In recent years, the security of MQTT-based communication in IoT environments has garnered significant attention due to its widespread use in sectors like automotive and healthcare. As these industries continue to adopt IoT solutions that rely on real-time data transmission and device interoperability, the need to secure MQTT communications against threats like Man-in-the-Middle (MITM) attacks has become more pressing. Several studies have explored various techniques to address these vulnerabilities.

A notable contribution in this area is Security Analysis of MQTT and Its Application in IoT (Zhang et al., 2023), which provides an in-depth security analysis of MQTT when applied to large-scale IoT systems. This study highlights the inherent vulnerabilities of MQTT, especially in environments dealing with sensitive data such as healthcare, where it can be susceptible to MITM attacks. The authors suggest implementing end-to-end encryption (E2EE) to protect data from being intercepted or tampered with during transmission. Additionally,

they propose combining E2EE with mutual TLS (mTLS) to ensure the authenticity of both the client and server, thereby reducing the risk of unauthorized access. This dual-layered encryption strategy provides an effective defense against MITM attacks, ensuring both confidentiality and integrity, even in large and complex IoT networks [5].

Similarly, in the field of healthcare IoT, the paper Securing Medical IoT Systems: A Survey on MQTT-Based Communication in Healthcare (Patel et al., 2023) explores the unique security challenges faced by medical IoT systems. The study emphasizes the use of MQTT to monitor patient vitals, track medical devices, and transmit critical diagnostic data, making it a prime target for MITM attacks. The authors advocate for implementing advanced encryption techniques and mutual authentication to safeguard patient data. They also stress the importance of fine-grained access control, where only authorized personnel or devices can access sensitive health information. The study highlights the scalability issues of securing large medical IoT networks and suggests role-based access control (RBAC), along with time-limited tokens, as effective solutions for managing large numbers of connected devices [6].

In the automotive sector, A Secure Architecture for MQTT-Based Communication in Vehicular Networks (Zhao et al., 2022) addresses the growing concerns related to the security of Vehicle-to-Everything (V2X) communications, where MQTT is used for real-time vehicle diagnostics, navigation updates, and safety-critical functions such as collision detection. The study demonstrates how MQTT can be vulnerable to MITM attacks in vehicular environments, particularly when the communication is crucial for safety. To mitigate these risks, the authors propose a hybrid security architecture that integrates mutual TLS (mTLS) for device authentication with blockchain technology for immutable data logging. This ensures that all transmitted messages are verifiable and cannot be altered, providing enhanced security and auditability. The paper also addresses the scalability challenges of automotive IoT systems and suggests utilizing a distributed Public Key Infrastructure (PKI) to manage authentication and encryption keys more efficiently [9].

V. CONCLUSION

This paper introduces a lightweight security framework designed to mitigate Man-in-the-Middle (MITM) attacks in MQTT-based communication, catering to the specific requirements of healthcare and automotive industries. MQTT, a widely used protocol for its simplicity and efficiency, lacks inherent security mechanisms, making IoT systems vulnerable to cyberattacks. The proposed framework integrates Advanced Encryption Standard (AES) for securingdata payloads, Elliptic Curve Cryptography (ECC) for efficient key exchange, mutual authentication for verifying device identities, and dynamic key management to periodically update cryptographic keys, ensuring continuousprotection.

Experimental results demonstrate the framework'seffectiveness in preventing MITM attacks while maintaining low latency and computational overhead, critical for resource-constrained IoT devices such as pacemakers and vehicle sensors. The solution aligns with industry standards like HIPAA for healthcare and ISO/SAE 21434 for automotive cybersecurity, ensuring compliance and reliability in real-world applications.

This research addresses current gaps in securing MQTT communication by providing a balanced approach to performance and security. The results highlight the framework's ability to enhance data integrity and confidentiality without compromising the operational efficiency of IoT devices.

VI. FUTURE ENHANCEMENT

Future work will focus on extending the framework’s scalability to support diverse IoT ecosystems, such as smart cities and industrial automation. Additionally, advanced cryptographic techniques and machine learning-based anomaly detection will be explored to further strengthen security measures. This research contributes to building trust in IoT technologies byensuring safe, secure, and reliable communication in critical environments.

One of the key improvements to secure MQTT communication is the adoption of end-to-end encryption (E2EE). While MQTT over SSL/TLS (MQTTS) ensures that data is encrypted during transmission, it only protects the channel, not the actual data payload. This means that an attacker could still potentially intercept and modify the message content in the application layer. By implementing E2EE, where the client encrypts the message before sending and only the intended recipient can decrypt it, communication remains secure even if an attacker manages to intercept the transmission. This is particularly important in the healthcare sector, where patient

data needs to remain confidential and cannot be tampered with during transmission.

Alongside encryption, mutual authentication adds another crucial layer of security. Traditional MQTT setups typically involve server-side authentication via SSL/TLS, but this only verifies the server, leaving the client's authenticity unchecked. By utilizing mutual TLS (mTLS), both the client and the server authenticate each other, ensuring that only authorized entities can communicate with each other. This is particularly important in the automotive industry, where connected devices in vehicles communicate with external servers or cloud-based services. Here, ensuring that both the vehicle (client) and the diagnostic server (broker) are authenticated is essential to protect against MITM attacks that could interfere with vehicle diagnostics or control systems.

Another important enhancement is the implementation of topic-based access control (ACLs). In MQTT, clients can subscribe to broad topics, but without proper management, this could expose sensitive data to unauthorized clients. Fine-grained ACLs can be used to grant clients access only to specific topics based on their credentials or permissions. In healthcare, this ensures that only authorized devices and personnel can access sensitive patient data, preventing unauthorized access or manipulation of medical records, which is critical for maintaining patient confidentiality and safety.

VII. REFERENCES

[1] Shalini, S., Sheela, S., Taj, S., & Bagalatti, M. R. (2024). Vulnerabilities in Internet of Things and Their Mitigation with SDN and Other Techniques. In CRC Press eBooks (pp. 279–288).

[2] S. S, S. S, A. S, B. P, G. C and R. K S, "An Effective Counterfeit Medicine Authentication System Using Blockchain and IoT," 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, 2023, pp. 1-5, doi: 10.1109/INCET57972.2023.10170622

[3] T. J. Lakshmi, Shalini S., Sheela S., Saakshi P.. WSN with IoT Using Raspberry Pi as a Tool for Communication. International Journal of VLSI Circuit Design & Technology. 2023;01(01):34-42.

[4] Nguyen, T., & Kim, S. (2022). Enhancing MQTT Communication Security Using TLS: Challenges and Considerations for IoT Devices. Journal of IoTSecurity,34(2),125–134.

[5] Zhang, W., & Chen, Y. (2023). LightweightCryptographic Solutions for Securing MQTTCommunication in Resource-Constrained IoTDevices. International Journal of EmbeddedSystems,42(3),210–222.

[6] Patel, A., & Gupta, N. (2021). Addressing Security Vulnerabilities in MQTT Communication for Healthcare IoT. International Journal of IoT Applications, 28(1), 45–59.

[7] Wang, X., & Liu, H. (2022). Secure Key Management and Encryption Techniques for MQTT in Automotive IoT Applications. Automotive Cybersecurity Journal, 19(5), 110– 123.

[8] EMQ Technologies. (2022). Ensure MQTT Security with TLS/SSL: A Practical Guide. EMQ Blog.

[9] Ali, K., & Farooq, M. (2022). Lightweight Encryption Techniques for Healthcare IoT Systems: A Case Study on MQTT Communication.Healthcare Technology Letters, 10(1), 15–23.

[10] Chen, L., & Zhang, S. (2022). Implementing Dynamic Key Management in MQTT Communication: A Secure Framework for IoT. International Journal of Secure IoT Systems, 36(2),89–101.

[11] Nguyen, H., & Tran, K. (2021). A Review of MQTT Security Features and Vulnerabilities inAutomotive IoT Networks. Cybersecurity and IoT Journal, 25(1), 55–67.