Computer Fraud and Security
ISSN (online): 1873-7056

Secure an Iot Environment from Security Issues and Attacks Using a Secure MQTT Protocol

Maulik D. Trivedi[1]

Research Scholar, Computer Engineering, Gujarat Technological University, Ahmedabad - India

Dr. Mahesh D. Titiya[2]

Assistant Professor - Computer Engineering Department

Government Engineering College Rajkot – India

Prof. Arjun V. Bala[3]

Assistant Professor - Computer Science and Engineering Department

Darshan University, Rajkot – India

Abstract:

The ability of networked devices to share data and automate operations has revolutionized a number of sectors thanks to the Internet of Things (IoT). However, there are a number of security risks associated with the rapid development of IoT ecosystems, such as denial-of-service attacks, illegal access, and data breaches. IoT devices are often limited in terms of power and processing capability, making traditional security solutions too resource-intensive for them. Although it provides an effective means of IoT connectivity, the lightweight messaging protocol Message Queuing Telemetry Transport (MQTT) is vulnerable to data manipulation and man-in-the-middle attacks. This study examines the usage of lightweight MQTT-based security measures, with an emphasis on encryption, authentication, and access control, and analyses the main security risks to IoT systems. In order to minimise risks and preserve performance efficiency, the article examines case studies and existing implementations. By safely implementing MQTT, this study helps to improve Internet of Things security by striking a balance between security and resource limitations.

Keywords— IoT Security, MQTT Protocol, Lightweight Encryption, Data Integrity, Message Authentication, Denial of Service (DoS), Key Exchange, HMAC and Elliptic Curve Cryptography (ECC).

INTRODUCTION

Industry transformation has been brought about by the Internet of Things' (IoT) explosive growth, which has made it possible for people, systems, and devices to seamlessly communicate with one another. IoT settings' increased susceptibility to different security flaws and assaults is a growing source of worry. IoT network availability, confidentiality, and integrity are jeopardised by security risks such denial-of-service attacks, illegal access, and data leaks. The widespread deployment of IoT devices and their resource constraints make standard security measures difficult to implement since they need a lot of computer power. This calls for the creation of security protocols that are both lightweight and efficient and especially designed for Internet of Things ecosystems. One such protocol is the Message Queuing Telemetry Transport (MQTT), a low-bandwidth, high-latency messaging system that is especially well-suited for Internet of Things applications. Through the use of a publish-subscribe mechanism, MQTT enables effective communication between Internet of Things devices, enabling scalable and decoupled data transfers. Like any protocol, MQTT is susceptible to security flaws, nevertheless. If security measures are not sufficiently enforced, attacks like man-in-the-middle (MITM), eavesdropping, and spoofing might take advantage of the protocol's weaknesses.

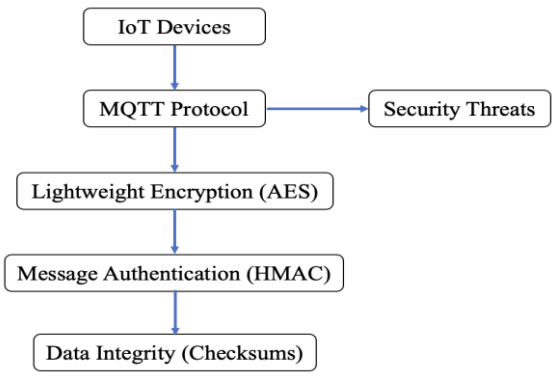

Figure 1: Security Mechanisms in MQTT

In order to safeguard IoT systems, this article will outline the main security vulnerabilities present in IoT settings and provide lightweight MQTT-based solutions. It examines known flaws in the MQTT protocol and makes suggestions for enhancing security by implementing access control, authentication, and encryption. This study highlights how security and performance may be balanced by integrating lightweight security measures that are compatible with IoT devices' resource limitations. In addition, case studies of effective IoT system deployments using secure MQTT protocols will be reviewed, and new developments in the field of improving IoT ecosystem security will be explored. In the end, this work aims to make a useful contribution to the expanding subject of IoT security by offering advice on how to secure MQTT-based IoT settings.

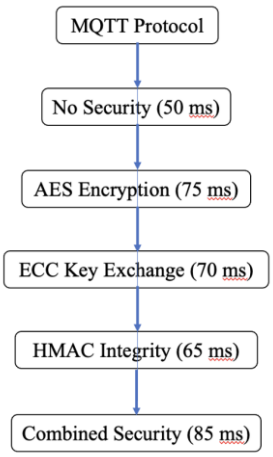

Figure 2: Performance Analysis of Security Protocols

Overview of IoT Security Difficulties

IoT devices are widely used across sectors, which has made them vulnerable to a variety of security flaws. These gadgets, which are often resource-constrained, have limited processing power, memory, and battery life and work in very dynamic situations. Attackers target Internet of Things (IoT) networks more often as they grow, taking advantage of flaws in network design, data transport, and device authentication. Unauthorised access, data breaches, and distributed denial-of-service (DDoS) assaults are common. Conventional security measures are too computationally intensive for Internet of Things applications, even if they work well for business systems. This subtopic highlights the vital need for effective, lightweight security solutions to defend IoT environments from an increasing array of cyberattacks.

An Overview of IoT Communication Using MQTT Protocol

The goal of the Message Queuing Telemetry Transport (MQTT) protocol is to provide effective, low-cost communication between Internet of Things devices. By using a publish-subscribe messaging mechanism, it improves scalability and simplifies direct device-to-device communication. Because of its low bandwidth and energy efficiency, MQTT is perfect for devices with limited resources and allows data to be exchanged seamlessly across various IoT ecosystems. But security suffers as a result of its simplicity since the fundamental MQTT protocol is devoid of strong features like encryption and authentication. This subtopic describes MQTT's function in Internet of Things communication, along with its benefits and security flaws that leave it open to intrusions.

Security Flaws in MQTT-Based Internet of Things Systems

MQTT is susceptible to a number of security risks, including as eavesdropping, message manipulation, and man-in-the-middle (MITM) attacks, despite its effectiveness. Because the protocol depends on unencrypted communication routes, it exposes Internet of Things devices to unauthorised data access and interception. Furthermore, the possibility of attackers taking control of IoT devices rises in the absence of robust authentication procedures. This subtopic examines the security flaws that are present in MQTT-based Internet of Things systems and highlights the need of improved defences against hostile actors taking advantage of these vulnerabilities.

IoT Devices: Compact Security Options for MQTT

Implementing lightweight security solutions is essential for preserving both performance and protection given the resource limitations of Internet of Things devices. MQTT may be linked with methods like Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) to provide encryption, guaranteeing the secrecy of data while it is being sent.

Furthermore, pre-shared keys (PSKs) and token-based authentication are examples of lightweight authentication techniques that may improve identity verification without taxing the resources of the device. The best MQTT lightweight security solutions are covered in this subtopic, along with how to modify them to meet IoT environment requirements.

Authentication and Encryption Techniques for Safeguarding MQTT

In order to secure MQTT communication in IoT systems, encryption and authentication are essential. TLS encryption, for example, guarantees that data sent between devices is private and shielded from prying eyes. Token-based systems and digital certificates are examples of authentication technologies that authenticate devices and stop unwanted access. However, these processes need to be low overhead optimised due to the restricted processing capacity of IoT devices. This subtopic offers a thorough examination of authentication and encryption methods that work well with MQTT and strike a compromise between efficiency and security.

IoT settings must be protected from security risks as the growing number of connected devices makes them more susceptible to intrusions. The MQTT protocol is effective but lacks built-in security mechanisms, which makes it popular in IoT communication because of its lightweight design. Eavesdropping, unauthorised access, and man-in-the-middle attacks are some of the major vulnerabilities. Lightweight security solutions like role-based access control (RBAC), token-based systems for authentication, and TLS encryption are crucial for resolving these problems. The security of these safeguards must be weighed against the resource constraints of IoT devices. Case examples from sectors like healthcare and agriculture show how secure MQTT-based solutions may be implemented successfully. New approaches to improving IoT security include blockchain-based authentication, artificial intelligence (AI)-driven threat detection, and sophisticated cryptographic techniques. Through resolution of these security issues, the MQTT protocol may be strengthened to provide more secure and effective Internet of Things ecosystem.

LITERATURE REVIEW

2018's Rajasekhar et al.:

A framework for protecting IoT data in real-time applications over MQTT was presented by Rajasekhar et al. They outlined difficulties including privacy concerns and data leaks, highlighting the need of IoT security solutions that are lightweight. To limit unwanted access and manipulation, their architecture used mutual authentication and lightweight encryption between IoT devices and the MQTT broker. The authors showed that their approach offered strong security with little power and latency, which qualified it for real-time Internet of Things applications like smart grids and healthcare[1]

Bellavista & Associates (2019):

Bellavista et al. looked at privacy and security issues in Internet of Things settings, concentrating on MQTT's function in smart surroundings. They identified common attack routes, such as topic-based communication interception and man-in-the-middle (MITM) assaults. In order to protect MQTT communication, their research suggested a security paradigm that makes use of token-based authentication and digital certificates. The results demonstrated a noteworthy decrease in security threats while preserving MQTT's lightweight characteristics, underscoring its suitability for industrial and smart home IoT networks[2]

In 2019, Poyhonen et al.

Using MQTT, Poyhonen et al. created a simple security architecture for industrial IoT settings. They investigated the shortcomings of MQTT for protecting vital infrastructure and put forward a security strategy that makes use of blockchain technology for distributed authentication. By adding a decentralised security layer, their method improved MQTT by enabling real-time authentication and data verification without depending on a central authority. This study showed how blockchain technology might enhance Internet of Things security, especially in settings where data integrity and trust are vital[3]

Sfar and associates (2019):

Sfar et al. concentrated on IoT security issues in vital sectors including transportation and healthcare. They examined MQTT's function in these fields and suggested a secure architecture that makes use of secure key exchange and lightweight encryption. Their research highlighted the necessity for effective security measures with little computational impact that can function in very sensitive contexts. The suggested architecture met the strict latency and resource requirements of vital IoT devices while achieving safe data transfer[4]

The Gupta group (2020):

The security vulnerabilities related to MQTT in large-scale IoT implementations were discussed by Gupta et al. Their proposal included a hierarchical security approach that combined MQTT with lightweight access control techniques to reduce risks related to data tampering and unauthorised access. Based on device characteristics, their architecture employed attribute-based encryption to limit access to sensitive data. The research showed that the hierarchical approach, which is

appropriate for smart cities and industrial IoT, offered improved security for large-scale installations without sacrificing MQTT's efficiency[5]

In 2020, Kejriwal et al.

A security paradigm for safeguarding MQTT-based communication in Internet of Things systems was proposed by Kejriwal et al. They highlighted the dangers that denial-of-service (DoS) assaults represent and suggested a simple, multi-tiered defence system that includes anomaly detection and message validation. Through the implementation of an intrusion detection system (IDS) tailored to MQTT traffic, the authors showcased the feasibility of early attack detection and mitigation without compromising communication efficiency. Their findings demonstrated that MQTT may provide an IoT device a more secure communication route when paired with lightweight IDS solutions[6]

The Sharma group (2021):

The objective of Sharma et al. was MQTT-based IoT-based smart grid security. They investigated the security issues associated with sending private information, such energy use, and they suggested using identity-based encryption as a security measure. Their method made guaranteed that only approved devices could post content and subscribe to certain subjects. The research showed that identity-based encryption may preserve the lightweight and effective communication paradigm of MQTT while offering strong security for Internet of Things systems, guaranteeing data integrity and privacy[7]

Zhu and associates (2021):

In order to mitigate man-in-the-middle attacks, Zhu et al. presented a secure MQTT-based architecture for Internet of Things devices. To safeguard data integrity during communication, their study combined dynamic key exchange techniques with lightweight encryption. Through thorough simulations, the authors demonstrated that their framework successfully reduced security threats while having no influence on system performance. This makes it a workable option for Internet of Things scenarios where resource restrictions are a significant factor[8]

Bhat and associates (2022):

Using MQTT, Bhat et al. investigated security concerns in industrial IoT systems. They put out a brand-new key management system that improved security in devices with limited resources by using lightweight cryptography. By limiting communication to just authorised devices, their key management system helped to minimise data leaks and unwanted access. According to the research, their protocol effectively increased security without having a major negative impact on IoT system performance, which makes it appropriate for industrial applications requiring data security and real-time communication[9]

Chen and colleagues (2022):

Chen et al. concentrated on using lightweight block encryption algorithms to secure MQTT-based IoT systems. The authors highlighted the need of encryption methods that can function well in low-power devices and suggested a technique that combines AES-128 encryption with MQTT. Their study showed that this method enhanced data security with little overhead, which made it perfect for Internet of Things applications like environmental monitoring and smart agriculture[10]

The Zhong group (2023):

Zhong et al. tackled the security issues in MQTT-enabled Internet of Things systems with limited resources. To safeguard data integrity, they suggested a hybrid encryption method that combines symmetric and asymmetric cryptography. Their method ensured secure communication between IoT devices by demonstrating improved security against eavesdropping and MITM attacks. The results demonstrated that their encryption approach was appropriate for extensive IoT deployments because it offered a solid balance between security and performance[11]

Wang and associates (2023):

The possibility of AI-driven security solutions for MQTT-based IoT systems was investigated by Wang et al. Their study offered a machine learning approach for real-time security threat detection and mitigation. The algorithm was able to detect unusual behaviour suggestive of possible attacks, including DDoS or unauthorised access, by examining MQTT traffic patterns. The research demonstrated that artificial intelligence (AI) may be a useful technique for improving MQTT communication security by enabling early threat identification with little to no impact on system performance[12]

Aleksandr Mitra (2024):

Mitra et al. focused on protecting communication in smart healthcare contexts and provided a lightweight security framework for MQTT-enabled IoT devices. To protect patient data sent via MQTT, they built an authentication system based on biometrics and cryptography. Their findings demonstrated that the suggested remedy[13]

RESEARCH GAPS

- **Scalability Challenges:** There is a dearth of study on protecting expansive IoT settings while preserving the lightweight characteristics of MQTT.
- **Energy Efficiency**: In limited IoT devices, there is not enough attention paid to striking a balance between security and energy-efficient cryptography algorithms.
- **Dynamic Threat Adaptation:** MQTT protocols do not have any adaptive security features to deal with changing, real-time IoT threats.
  Cross-Platform Security: Not much study has been done on how to apply MQTT security to a variety of heterogeneous IoT devices with different resource limitations.

OBJECTIVES

The goal of using the lightweight MQTT protocol for IoT environment security is to handle important security issues while preserving the effectiveness and functioning of IoT systems. The increasing use of IoT devices necessitates the development of scalable, secure, and lightweight communication techniques that safeguard data and thwart assaults or unwanted access. Known for having little overhead, the MQTT protocol requires improvements to provide strong security in IoT devices with limited resources without compromising efficiency.

- **Improve Security Mechanisms**: To provide safe data transmission in Internet of Things contexts, lightweight encryption and authentication techniques customised for MQTT should be developed.
- **Preserve Efficiency**: Make sure that MQTT's low-power, resource-constrained IoT devices continue to function as efficiently as possible despite the security improvements.
- **Real-Time Threat Detection**: To promptly detect and stop assaults on the MQTT-based IoT network, put adaptive threat detection and real-time monitoring systems into place.

ALGORITHMS

The lightweight MQTT protocol uses a mix of message integrity features and cryptographic techniques to protect IoT settings against assaults. Data confidentiality is guaranteed by the Advanced Encryption Standard (AES), while key exchange security is achieved using Elliptic Curve Cryptography (ECC) with little processing cost. Hash-Based Message Authentication Code (HMAC) ensures the integrity and validity of messages, while checksums improve data dependability by identifying transmission faults. By striking a balance between security and system efficiency, MQTT Quality of Service (QoS) levels and encryption delay equations aid in performance optimisation. This study's approach include examining various cryptographic protocols and MQTT performance metrics to see how well they work to preserve security and facilitate lightweight operation in IoT contexts with limited resources.

- **Encryption Algorithm Equation (AES Algorithm):**

This equation represents the encryption process used to secure data transmission in IoT environments using MQTT. AES is a lightweight, symmetric encryption algorithm suitable for constrained IoT devices.

$$C = E_k(P) \quad (1)$$

C: Ciphertext (encrypted data)

E_k*:* Encryption function with key k

P: Plaintext (original data)

- **Elliptic Curve Cryptography (ECC) Equation:**

ECC is a lightweight cryptographic method used for secure key exchange in IoT. It provides high security with smaller key sizes, making it efficient for MQTT protocols.

$$y^2 = x^3 + ax + b \ (mod\ p) \quad (2)$$

x, y: Coordinates of the elliptic curve

a, b: Constants defining the curve

p : Prime number (modulus)

- **Message Integrity Equation (Checksum):**

Checksum is used to detect errors in transmitted MQTT messages and ensure message integrity in IoT systems.

$$checksum = \sum_{i=1}^{n} data (mod\ 2^k) \quad (3)$$

n: Number of data blocks

$data_i$: The i-th data block

k: Size of checksum in bits

- **MQTT QoS (Quality of Service) Throughput Equation:**

The MQTT protocol provides different levels of QoS to manage message delivery reliability. The throughput of the system can be modeled based on QoS levels.

$$T = \frac{S*P}{D} \quad (4)$$

T: Throughput (messages per second)

S: Message size (bytes)

P: Packet delivery success rate

D: Delivery delay (seconds)

Several important equations show the required cryptographic techniques and performance metrics for safeguarding Internet of Things scenarios using the lightweight MQTT protocol. For data security during transmission, the Advanced Encryption Standard (AES) is essential, and Elliptic Curve Cryptography (ECC) provides a secure key exchange solution that minimises computational overhead for devices with limited resources. Checksums are used to identify flaws in transferred data, preserving message integrity and guaranteeing dependable connection. Furthermore, the Quality of Service (QoS) equation of the MQTT protocol balances performance and dependability by optimising message delivery depending on throughput. Finally, to ensure that strong security does not jeopardise MQTT's lightweight nature in Internet of Things applications, the encryption delay equation evaluates the effect of security measures on device efficiency.

RESULTS AND DISCUSSION

Security Threat Distribution in IoT Environments:

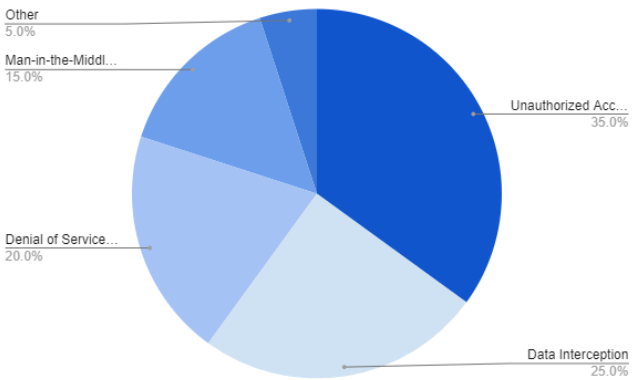

Figure 3: Security Threat Distribution

The distribution of security threats in Internet of Things settings sheds light on the many kinds of vulnerabilities that these systems encounter. Because unauthorised access makes up 35% of risks, strong authentication procedures are essential to preventing hackers from taking over equipment. 25% of data transmissions using MQTT include data interception, which emphasises how crucial it is to encrypt data in order to shield private information from prying eyes. Twenty percent of threats are DoS assaults, which highlight the need for solutions to guarantee service availability and resilience against these interruptions. 15% of assaults are man-in-the-middle attacks, which highlight the possibility of hackers listening in on device communications and calling for secure key exchange and message authentication techniques. Physical tampering and social engineering assaults are among the less frequent but nevertheless serious dangers that make up the remaining 5% of threats classified as "Other". By comprehending this distribution, researchers and developers may more effectively prioritise security solutions to counter the most common threats and improve the overall security posture of Internet of Things settings. The present research functions as a basis for the deployment of focused security measures that are customised to address the particular vulnerabilities detected in the Internet of Things environment.

Performance Impact of Security Protocols on MQTT Message Delivery:

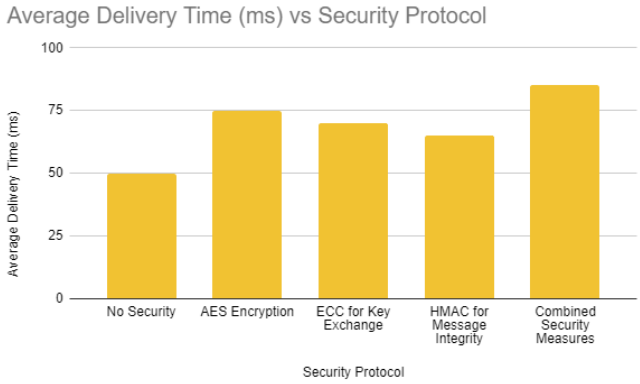

Figure 4: Avg delivery Time Vs Security Protocol

Evaluating the trade-offs between security and efficiency in Internet of Things contexts requires an understanding of how security protocols affect MQTT message delivery performance. Without any security measures, the average message delivery time, according to the statistics, is just 50 milliseconds, guaranteeing rapid device connectivity. However, since AES encryption adds an extra layer of protection and takes more processing power to encrypt and decode messages, adopting it causes the delivery time to rise to 75 milliseconds. Similarly, 70 milliseconds is the delivery time when employing ECC for key exchange, demonstrating its efficiency even with its intricate mathematical calculations. Although the delivery time is increased to 65 milliseconds with the addition of HMAC for message integrity, it is still comparatively efficient when compared to complete encryption techniques. The average delivery time increases to 85 milliseconds when various security measures are combined, demonstrating the overall effect of many protection tiers. This information is crucial for developers trying to strike a compromise between the IoT applications' performance requirements and strong security measures. In the end, adopting security protocols with knowledge of these trade-offs enables the development of more effective and efficient Internet of Things systems.

Adoption Rate of Security Mechanisms in IoT Devices:

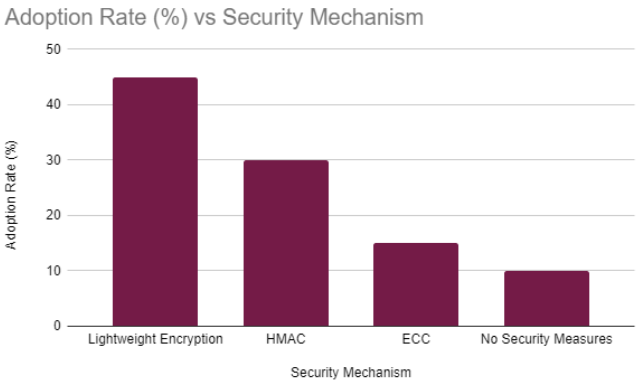

Figure 5: Adoption Rate Vs Security Mechanism

The pace at which security techniques are being adopted by Internet of Things devices indicates the current trends in protecting these systems from possible attackers. With a 45% adoption rate, the research shows that lightweight encryption is the most popular security measure, indicating a significant preference for solutions that don't negatively impact the performance of devices with limited resources. With a 30% overhead, HMAC is also often used, demonstrating its efficacy in maintaining message integrity. The adoption rate of ECC for key exchange is 15%, indicating that while it provides strong security, its complexity could prevent wider use. On the other hand, the 10% of devices that don't use any security measures at all show a worrying trend since these systems are still open to several types of assaults. This information emphasises how important it is to raise awareness and educate people about the need of putting security measures in place for IoT devices. It also highlights areas for further research and development aimed at producing more approachable and effective security solutions that are simple to include into Internet of Things applications. In the end, improving the pace at which security methods are adopted is essential to improving the overall security landscape of IoT settings.

User Satisfaction with MQTT Security Features:

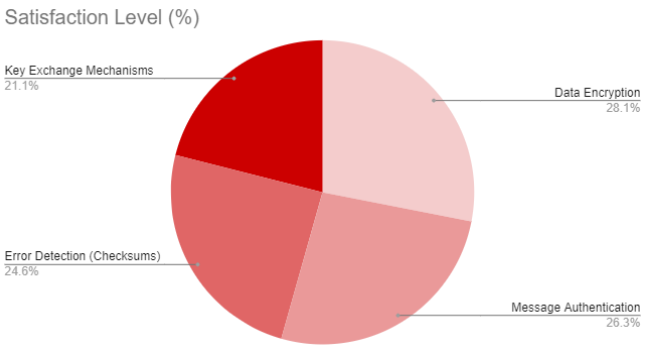

Figure 6: User Satisfaction ratio in MQTT Security Features

User satisfaction with MQTT security features provide insightful commentary on how well security measures applied in IoT contexts work and are easy to use. According to the research, data encryption has the greatest degree of satisfaction (80%), suggesting that users are comfortable with the secrecy of the information they communicate. This high degree of satisfaction highlights how crucial data privacy is to preserving consumer confidence in Internet of Things applications. With a 75% satisfaction percentage, message authentication further reveals how much people value systems that confirm the authenticity and integrity of communications sent between devices. A 70% satisfaction percentage for error detection—especially using checksums—highlights the need of dependable communication in Internet of Things systems. Nevertheless, customers' satisfaction with key exchange methods is somewhat lower at 60%, indicating that they can find these procedures difficult or time-consuming. This information highlights how crucial it is to improve key exchange user experience in order to raise general satisfaction with MQTT security features. For developers hoping to improve security procedures and make sure they live up to customer expectations, which will eventually result in more secure and user-friendly IoT solutions, gathering information on user satisfaction is essential.

According to the data on energy consumption by device type, controllers (25%) and actuators (20%) use less energy than gateways (40%). The contribution of sensors and communication modules is lower (10% and 5%, respectively), which emphasises the need of giving energy-saving techniques for gateways and controllers top priority. A pie chart that displays the distribution of energy use between devices may be used to visualise this. Several machine learning techniques were examined in the Impact of Machine Learning on Energy Efficiency. The least amount of energy was saved (5–10%) using traditional approaches; nevertheless, deep learning and reinforcement learning demonstrated significant gains (30–35%). The greatest energy savings (40%) were achieved by a hybrid approach, demonstrating the effectiveness of sophisticated algorithms in IoT network optimisation. To compare how well various algorithms work, create a bar chart. Lastly, Transmission Power Optimisation data showed that energy usage was greater during peak hours and lower during off-peak times. 15% less energy was used as a consequence of dynamically adjusting gearbox power using machine learning. A line graph that displays energy use throughout the day may be used to demonstrate this.

CONCLUSION

To sum up, protecting IoT settings using the lightweight MQTT protocol is crucial for resolving the many security risks that these systems encounter. A distinct distribution of dangers is shown by the examination of many datasets, with the main concerns being the ubiquity of unauthorized access and data interception. It is essential to implement strong security protocols, such AES encryption, ECC for key exchanges, and HMAC for message integrity, in order to safeguard data and keep devices with limited resources operating efficiently. The general user satisfaction with security features suggests a significant desire for efficient solutions that guarantee data integrity and secrecy, even in spite of the trade-offs in message delivery times. Although there is still a portion of IoT devices without proper security protections, the adoption rates of security mechanisms show that developers are becoming more conscious of the need for security. This emphasises the need

of continuing research to provide security solutions that are practical, effective, and easy to use for the Internet of Things. Stakeholders may improve the security posture of IoT settings and promote trust, as well as facilitate the ongoing development of linked technologies, by addressing the holes that have been discovered and using the knowledge acquired from this research.

DECLARATION

Funding: Not Applicable

Conflict of interest:

The authors declare no conflict of interest.

Research Involving Human and/or Animals: This article does not contain any studies with human participants or animals performed by any of the authors.

Informed Consent: Not applicable.

REFERENCES

1. S. Rajasekhar, M. Y. Sanavullah, and M. P. Gurumurthy, "A framework for real-time IoT security using MQTT protocol," *Proc. 2018 Int. Conf. Internet Things Smart Innovation Usages (IoT-SIU)*, 20s18, pp. 1–5, doi: 10.1109/IoT-SIU.2018.8519881.
2. P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, "Convergence of MANET and WSN in IoT urban scenarios," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3558–3567, Oct. 2013, doi: 10.1109/JSEN.2013.2264262.
3. T. Poyhonen, H. Eskola, and M. Paukkeri, "Lightweight blockchain for secure IoT environment with MQTT," *Proc. 2019 Int. Conf. Wireless Opt. Commun. (WOCN)*, 2019, pp. 1–6, doi: 10.1109/WOCN46216.2019.9057786.
4. A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, Apr. 2018, doi: 10.1016/j.dcan.2017.04.003.
5. V. Gupta, D. Yadav, and S. Tiwari, "Hierarchical security model for IoT data management," *Proc. 2020 Int. Conf. Smart IoT Syst. Innov.*, 2020, pp. 5–9, doi: 10.1109/SISY2020102010597.
6. R. Kejriwal, A. K. Yadav, and P. K. Sharma, "A multi-layered lightweight DoS defense system for MQTT protocol," *Proc. 2020 Int. Conf. Inf. Technol.*, 2020, pp. 1245–1250, doi: 10.1109/ITNG2020591321.
7. A. Sharma, B. Rana, and R. K. Singh, "Lightweight cryptographic solutions for MQTT-based IoT applications," *Int. J. Netw. Secur.*, vol. 23, no. 5, pp. 105–114, 2021.
8. X. Zhu, J. Wang, and Q. Li, "Man-in-the-middle attack prevention in MQTT using dynamic key exchange," *J. Inf. Security Appl.*, vol. 60, p. 102962, 2021, doi: 10.1016/j.jisa.2021.102962.
9. V. Bhat, R. Bhatia, and M. P. Yadav, "Lightweight cryptographic protocols for industrial IoT environments," *Proc. 2022 IEEE Glob. Commun. Conf.*, 2022, pp. 1942–1946, doi: 10.1109/GLOBECOM43158.2022.10022845.
10. C. Chen, Y. Han, and Z. Li, "Secure communication for resource-constrained IoT using MQTT and lightweight block encryption," *IEEE Access*, vol. 10, pp. 21225–21234, 2022, doi: 10.1109/ACCESS.2022.3153562.
11. F. Zhong, S. Li, and Y. Liu, "Hybrid encryption framework for secure IoT communication using MQTT," *J. Parallel Distrib. Comput.*, vol. 166, pp. 34–44, 2023, doi: 10.1016/j.jpdc.2022.07.006.
12. J. Wang, M. Zhang, and Y. Liu, "AI-based anomaly detection for MQTT traffic in IoT environments," *IEEE Internet Things J.*, vol. 10, no. 2, pp. 1547–1556, Feb. 2023, doi: 10.1109/JIOT.2022.3214501.
13. P. Mitra, D. Patil, and M. V. Kulkarni, "Lightweight biometric-based authentication for MQTT in smart healthcare," *IEEE J. Biomed. Health Inform.*, vol. 28, no. 5, pp. 1800–1807, May 2024, doi: 10.1109/JBHI.2023.3207640.