Comparative Analysis of Lightweight Cryptography and Blockchain-Based Security Protocols for Mitigating Threats and Vulnerabilities in the Internet of things

Chimenka Goodluck[1] Obioma D.C.[2]

[1,2]Department of Mathematics and Computer Science, Clifford University, Nigeria

DOI: https://dx.doi.org/10.51584/IJRIAS.2026.110100130

Received: 04 February 2025; Accepted: 09 February 2026; Published: 19 February 2026

ABSTRACT

The uncontrolled growth of the Internet of Things, especially in securing limited-resource IoT, has created unprecedented potential that raises issues tremendously. The key intention of the study is to comparatively examine the security measures and defenses against the cyber-attacks that take place in the IoT security protocols. The study provides a combination of secure communication protocols, blockchain technology, and lightweight cryptography using Bevywise IoT simulator, MQTT Route, and Wireshark for the network. The results of the study confirm the effectiveness of the security measures provided by the blockchain technology for the integrity and immutability of the data. The results also emphasize the significance of the study to solve the IoT security issues better. By creating a security framework, the study significantly contributes to the development of IoT technology, especially in the fields where the security has to be given more priority. Cyber security and maintaining the privacy and trust of the systems play a very significant role.

Keywords: Vulnerabilities, Threats, Protocols, Devices, IoT, Cryptography

INTRODUCTION

Connecting a wide range of devices, from industrial sensors to wearable health monitors, across various industries such as healthcare, manufacturing, agriculture, and urban infrastructure, the Internet of Things (IoT) has quickly become one of the most disruptive and revolutionary technologies. IoT allows devices to gather, share, and analyse data by integrating sensors, actuators, and communication capabilities into commonplace items. This opens up new possibilities for efficiency and innovation [7]. An estimated 25 billion gadgets will be online by 2021, according to a Gartner analysis, and this number is expected to increase as IoT adoption accelerates worldwide [4]. However, because many IoT devices contain security flaws, this widespread acceptance has also led to targeted cyber-attacks and data breaches. For example, the Mirai botnet attack used weak passwords in IoT devices to launch a massive Distributed Denial of Service (DDoS) attack that disrupted key online services [6]. Furthermore, poor encryption in many IoT networks has enabled man-in-the-middle attacks, in which malicious actors intercept and change data in transit. These examples demonstrate the numerous and serious security vulnerabilities faced by IoT devices, which necessitate quick action to establish resilient defense systems.

The distributed and decentralized structure of these networks exacerbates the security issues related to IoT. IoT ecosystems typically function with little oversight, frequently in uncontrolled or hostile contexts, in contrast to traditional IT systems, where centralized security protocols can frequently be established [4] Since many of the IoT devices are physically accessible, their decentralized nature makes it challenging to safeguard the enormous number of connected devices, leaving them vulnerable to physical security concerns like tampering. Cost limitations make these issues even worse because many IoT devices are made with less security to save money on production, which makes them less resilient to attacks [17].

Multiple layers of protection, including encryption, hashing, authentication, and secure communication protocols, are commonly used to enforce security in the Internet of Things. Because it can provide encryption in contexts with limited resources, lightweight cryptography has been suggested as a potential option for protecting

IoT devices [15]. Hash algorithms like SHA-1, SHA-2, SHA-3, and MD5 are frequently used in combination to lightweight encryption to guarantee

data integrity and deter tampering [7]. Every protocol has trade-offs, too, and it can be difficult to strike a balance between computing efficiency and security robustness in IoT settings. Furthermore, studies have revealed that current protocols have flaws and that no single protocol fully meets all IoT security requirements. Given these restrictions, a thorough examination of current IoT security procedures and remedies is required to establish how well they reduce cyberthreats. While various protocols and strategies have been created to improve IoT security, substantial gaps remain in their deployment and efficacy.

Firstly, it was discovered that current research frequently focuses on standard cryptographic algorithms, which may not be appropriate for resource-constrained IoT devices. These devices usually lack the computing capability, memory, and energy required to support traditional security measures. Furthermore, the rapid growth of IoT devices creates heterogeneity in network infrastructures, making it difficult to implement a uniform security protocol. The lack of broadly agreed evaluation measures hinders efforts to assess the efficacy of different security approaches. [1,3,5,7]

Secondly, as IoT networks get bigger, it gets harder to keep them safe in environments that are getting more complicated. Most of the studies that are done right now don't look at how lightweight cryptography and new technologies like blockchain can be best used for large-scale IoT deployments. Lastly, the fact that IoT cyber threats are always changing shows how important it is to have flexible and proactive security frameworks. Many existing protocols focus on fixing specific flaws but don't take into account new threats like advanced persistent threats and AI- driven attacks on IoT networks. [4,6]

Also, not much research has been done on how to use lightweight cryptography [14] and decentralized technologies together to solve problems of scalability, performance, and security.

This paper aims to fill these gaps by offering a thorough comparative review of hashing algorithms, cryptographic methods, blockchain technology, and IoT security protocols. This study offers a framework for choosing suitable security methods suited to particular IoT deployment situations by highlighting each one's advantages and disadvantages. The continuous endeavor to create resource-efficient, flexible, and scalable security solutions for IoT contexts will benefit from this assessment.

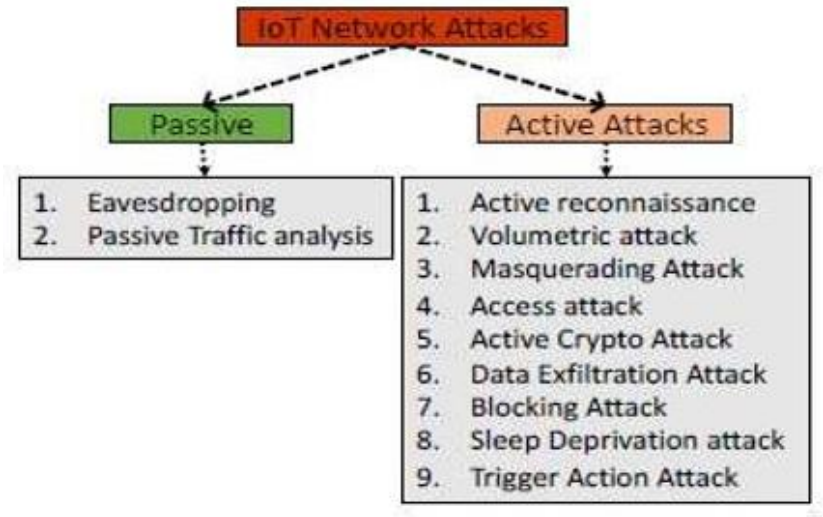

Fig 1.1 Structure of IOT network attack [7,14, 2]

Background of this Research Study

This research notes that the widespread use of IoT devices for a variety of purposes has considerably increased the attack surface, making IoT networks prime targets for hackers. Numerous issues, such as resource constraints, disparate deployment environments, and disparate security capabilities among devices, contribute to the inherent

vulnerabilities of IoT networks. The fact that many IoT devices are made with little security, frequently as a result of financial constraints and the lack of established regulatory frameworks, exacerbates these difficulties [4]. As a result, IoT devices are susceptible to cyber threats, including data breaches, illegal access, and device manipulation, all of which can have detrimental effects on user safety and privacy.

For a motivating example, let us consider the vulnerability of communication routes and gateways to both the internal and external networks to which they are connected. Multiple points of vulnerability are created by this exposure, which an attacker might exploit to gain control over IoT devices or gain unauthorized access to private

information. For example, improper encryption protocols and poorly secured APIs have been linked to attacks such as eavesdropping and unauthorized access [10]. The potential risks associated with insecure IoT installations are further exemplified by the Dyn DNS attack, which launched a large-scale distributed denial-of-service (DDoS) attack using an IoT botnet made up of compromised IoT devices [4]. Similarly, cybercriminals have leveraged malware like BrickerBot to permanently disable IoT devices by corrupting their firmware [11]. These kinds of issues highlight the necessity of secure communication protocols that can safeguard data integrity and confidentiality while shielding IoT networks from outside threats.

And again, shortcomings of conventional cryptographic techniques in resource- constrained IoT applications aggravate the difficulties in protecting IoT networks. IoT devices frequently lack the computational capacity to handle the demands of conventional encryption techniques because of their constrained processor power, memory, and battery life. One interesting approach is lightweight cryptography, which is intended to offer encryption that is more appropriate for Internet of Things devices and requires fewer resources [15]. However, there are still issues with lightweight cryptographic protocols, particularly with regard to scalability and resilience to advanced cyberattacks, and their effectiveness varies depending on the kind of IoT device.

Aside from encryption, safe hash algorithms are commonly employed in IoT networks to ensure data integrity and prevent manipulation. However, not all hash functions are equally applicable to IoT applications. Parmar and Kaur compared the speed, security, and dependability of various hashing algorithms, such as SHA-1, SHA-2, SHA-3, and MD5. Their investigation discovered that, while SHA-1 is the fastest method, it has known security flaws that render it unsuitable for situations where data protection is critical. Similarly, MD5, another extensively used hash function, is vulnerable to collision attacks, which limits its usage in secure IoT deployments [12]. As a result, there is an increasing demand for IoT-specific hashing algorithms that provide great performance while maintaining security.

The situation of IoT security today emphasizes how urgently a thorough examination of the available protocols and defences is needed. In order to meet this need, this study will investigate different cryptographic methods, lightweight security protocols, and hashing algorithms to ascertain how well they secure Internet of Things networks. In order to shed light on the best ways to mitigate cyber threats in IoT contexts, this study will also examine the trade-offs between security, cost, and performance. The research's conclusions will aid in the continuous creation of security frameworks that can successfully handle the particular difficulties presented by IoT installations.

This research, however, will try to focus on critical areas that have been mentioned in the Introduction by asking the following question: (1) What are the benefits and drawbacks of the current IoT security protocols and hashing algorithms now in use to lessen cyberthreats? (2) How do lightweight cryptographic protocols compare to traditional cryptographic methods in Internet of Things environments in terms of security and performance? (3) What best practices may be recommended for selecting appropriate security measures based on specific IoT deployment scenarios?

Objectives of this Research

1. To assess the effectiveness of lightweight cryptographic protocols and secure hash algorithms for IoT security

2. To compare IoT security protocols in terms of performance, cost, and scalability:

3. To Investigate Potential Vulnerabilities and Limitations in Current IoT Security Protocols:

4. To classify and identify current IoT security protocols and defenses

REVIEW OF RELATED LITERATURE

We first studied the unique safety concerns with IoT. Many researchers agree that lightweight cryptography has emerged as a viable approach to secure resource-constrained IoT devices. This claim is demonstrated by [15]

creation of the AUM lightweight cryptographic algorithm, which demonstrates how resource-constrained Internet of Things devices, such as RFID tags and sensors, can be secured without sacrificing functionality. AUM uses chaotic mapping theory and a 5-bit S-Box structure to provide strong security with little processing overhead. Since IoT contexts frequently lack the power to handle typical encryption methods, lightweight cryptography is critical for attaining the diffusion and confusion features necessary for secure communication [16]. Thus, the concept that lightweight cryptographic algorithms are essential to attaining a successful trade-off between security and efficiency is advanced by this work.

The significance of cryptographic hashing techniques for IoT security was also studied. We identified that IoT security relies heavily on hashing algorithms, especially when it comes to data integrity and identity verification amongst linked devices. The comparative analysis of hashing algorithms (SHA-1, SHA-2, SHA-3, and MD5) [11] provides insightful information on the advantages and disadvantages of these algorithms in Internet of Things settings. Although SHA-2 and SHA-3 offer strong security, their resource requirements may be too high for smaller IoT devices, according to their research. These papers also emphasize how, despite their speed, SHA-1 and MD5 are susceptible to cryptographic attacks and might not be appropriate for applications that need robust security. According to [14], these results highlight the necessity for effective, portable hashing algorithms that can offer sufficient security for Internet of Things applications without requiring a significant amount of computing power.

We also identified papers that highlighted the integration of blockchain with IoT security. These papers noted that by utilizing distributed ledger systems that confirm data integrity without centralized supervision, blockchain technology provides a decentralized method of protecting Internet of Things devices. Blockchain's ability to improve IoT security by offering a tamper-resistant architecture that lessens reliance on centralized systems, which are frequently subject to attacks, is highlighted by this [14] research. Blockchain technology enables decentralized data sharing and validation across IoT devices, enhancing the networks' resistance to cyberattacks. However, as acknowledged by [13], blockchain's computational and storage requirements might restrict its use for all IoT devices, especially those with stringent resource constraints. According to this study, blockchain technology may provide a complete security solution when paired with low-tech cryptography techniques.

Papers on comparative analysis of algorithms and security protocols were also studied. The lack of a defined method for assessing IoT security protocols is a recurring theme in these studies, which has resulted in disparities in the efficacy of procedures across various industries.

A notable discrepancy in IoT protocol performance is revealed by [11] comparison of hashing algorithms and [10] study of lightweight cryptographic techniques. Few existing protocols successfully strike a balance between security and efficiency, whereas several offer both. This lack of standardization restricts the use of current protocols and emphasizes the necessity of a methodical assessment methodology that takes into account the particular security needs of the Internet of Things [14]

The limitations noted in this literature review point to the increasing need for a comprehensive security architecture that can handle the particular needs of the Internet of Things, including performance, resilience to threats, and resource efficiency. These papers highlight essential elements for developing an all-encompassing IoT security framework by looking at lightweight cryptographic approaches, blockchain integration, and the effectiveness of different hashing algorithms. The creation of flexible security procedures that may successfully reduce cyber threats is crucial for preserving data integrity and protecting sensitive information as IoT continues to grow into a wider range of applications [9].

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

PRACTICAL METHODS ADOPTED

We adopted a mixed-method approach (using both quantitative and qualitative analytical approaches and experimental tools) while conducting some experiments in this research. We started by conducting a literature analysis to gain much insight from already existing work, with emphasis on protocols like lightweight cryptography and blockchain integration, as well as the establishment of evaluation measures. Qualitative analysis, which we adopted, includes reviewing research articles, industry reports, and case studies to discover gaps and weaknesses in current processes. Quantitative analysis uses empirical testing and simulations to measure performance indicators such as latency, energy consumption, and cryptographic strength. A practical component, which uses a simulated IoT lab and tools like Bevvywise IoT Simulator, Bevywise MQTT Route,

and Wireshark, tests the protocols' performance in real-world circumstances, including TCP/IP communications and security. The tools chosen are Wireshark, MQTT Route, and Bevywise IoT Simulator, which were selected based on their unique capabilities and widespread applicability in IoT research.

Wireshark was chosen for its robust network protocol analysis features, making it a preferred tool for monitoring and examining IoT network traffic. To the best of our knowledge, Wireshark provides deep packet inspection and supports a wide range of protocols, which enables the identification of vulnerabilities such as unencrypted data transfers and unauthorized access. Its ability to capture real-time data and facilitate protocol behavior analysis makes it indispensable for evaluating security measures like TLS/SSL in IoT environments. In this study's technique, IoT network traffic is analyzed and tracked throughout experimental testing using Wireshark. In order throw light on communication patterns, latency, and security flaws, it records data packets sent and received between IoT devices and protocols. Wireshark assists in assessing how well security protocols like TLS/SSL secure Internet of Things communications by looking at packet contents, encryption levels, and protocol behavior

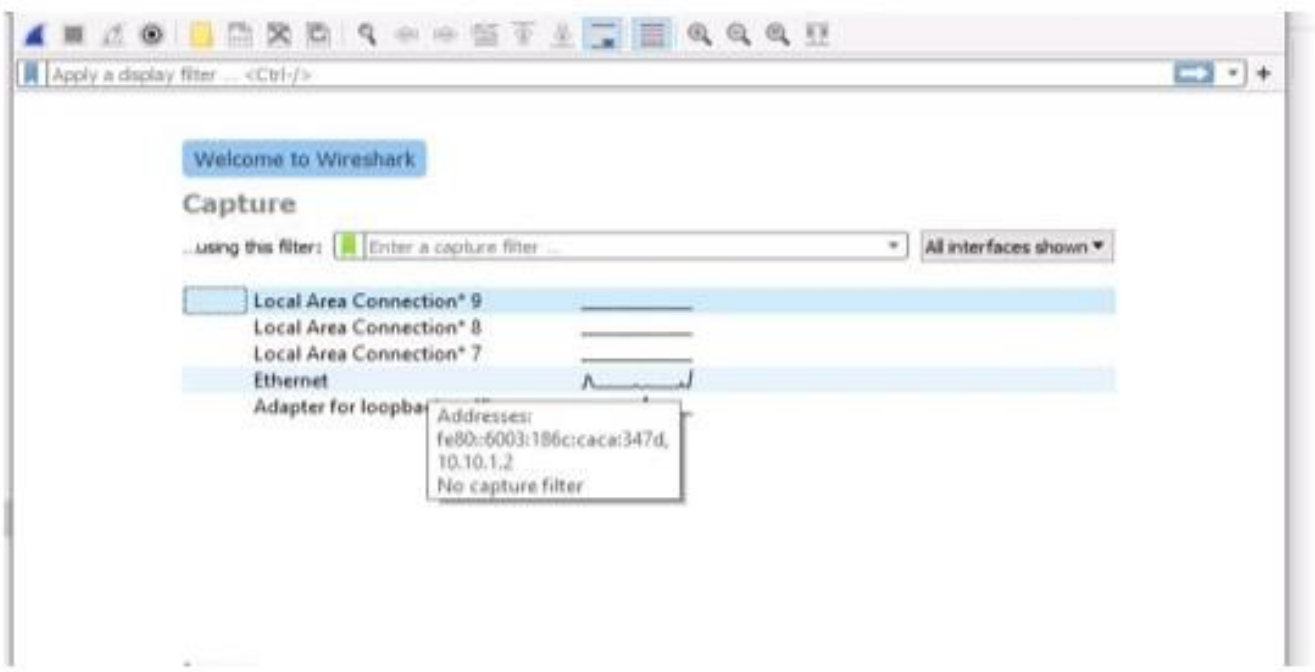

Fig 3.1 Screenshot of the homepage of Wireshark

Secondly, MQTT Route was selected as the MQTT broker due to its lightweight communication protocol, which is particularly well-suited for resource- constrained IoT devices. It supports secure communication via TLS/SSL and enables efficient data routing and device management. We assumed that for us to simulate secure communication within the IoT network during the research's practical component, MQTT Route is essential and the best fit. This tool makes it easier for simulated IoT devices to share data in a lightweight and effective manner. MQTT Route's integration with TLS/SSL for secure communication enables the study to collect data on resource

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

consumption and dependability, as well as test the effectiveness of IoT security protocols in actual scenarios.

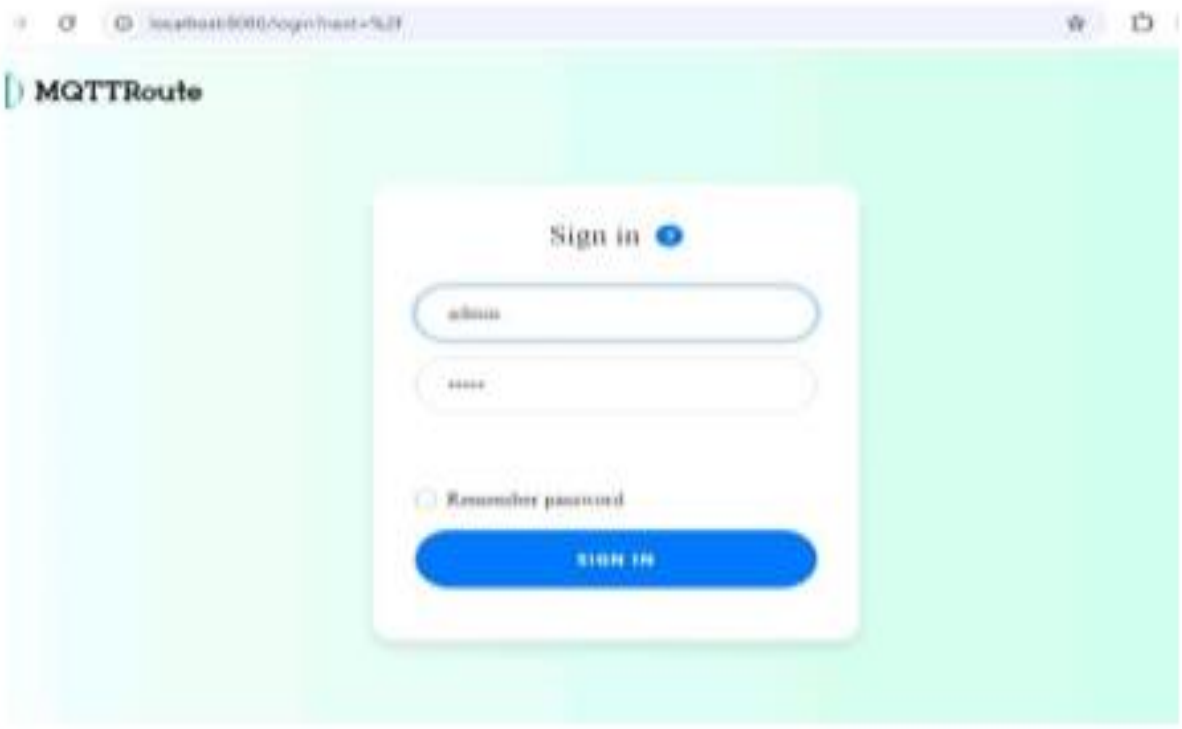

Fig 3.1 Screenshot of MQTTRoute Graphics User Interface

Thirdly, we made use of the Bevywise IoT simulator in this research. Unlike other simulators, Bevywise integrates real-time data generation and provides flexibility in configuring diverse IoT networks, including sensors and actuators. We also learnt that the compatibility with protocols like MQTT and integration with monitoring tools such as Wireshark make it a reliable platform for the type of experiment we want to conduct. To test and assess security protocols, a controlled, virtual IoT environment is created using the Bevywise IoT Simulator. It creates realistic data and traffic for tests by simulating extensive IoT networks. This allows for the evaluation of protocol performance, including resource efficiency and encryption strength, without the need for actual IoT devices. A dependable platform for comparing security measures in various IoT scenarios is offered by the simulator.

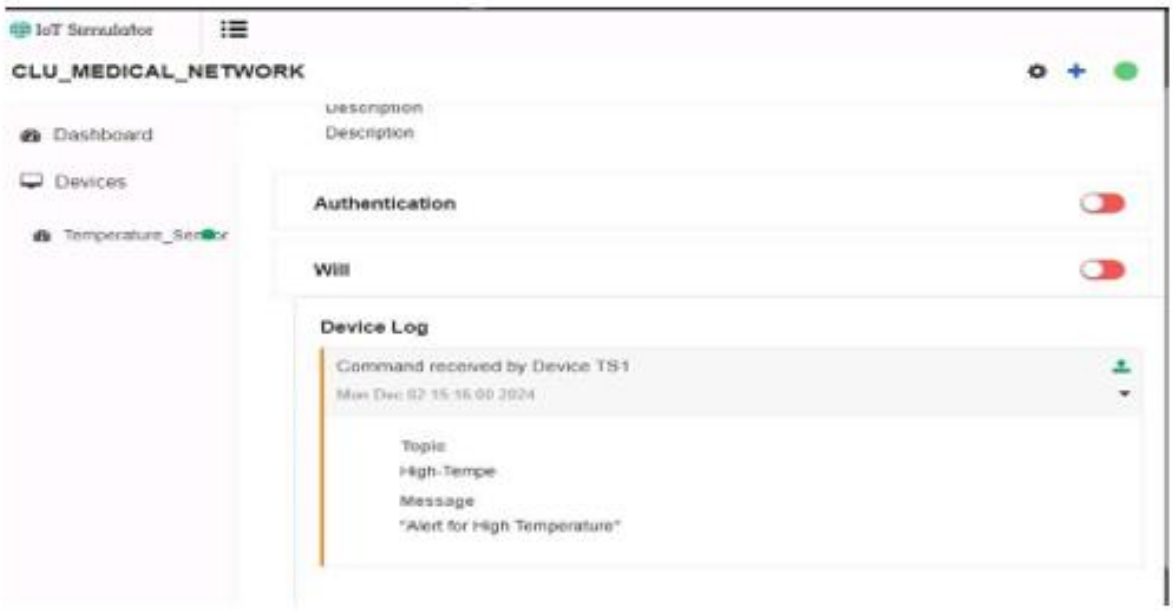

Fig 3.3 Screenshot of Clifford University Medical Center Simulated IoT network

For the avoidance of doubt to the readers of this work, we focused on a simulated network environment which mimics the hospital network in Clifford University medical center, or hospital, as any name describes that it is a medical institution. The simulated environment comprises a tele-device and an electronic health record (EHR) server, and the environment itself in which the experiment was conducted.

Additionally, for the protocol selection, encryption protocols under review will include Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and Rivest–Shamir–Adleman (RSA). Lightweight variants or adaptations of these protocols, like AUM (lightweight cryptography specifically for resource-constrained devices), will also be included. Hashing algorithms such as Secure Hash Algorithms (SHA-1, SHA-2, SHA-3), MD5, and newer variants specifically optimized for IoT devices will be assessed.

Hash functions are critical for data integrity and authentication, making them an essential focus for this research. Blockchain and Distributed Ledger Technologies (DLT) will be analyzed as potential decentralized solutions for IoT security. Also, lightweight cryptographic protocols like the AUM algorithm will be included to assess their capability to protect data in resource-limited IoT applications.

This analysis will provide insight into how new, lightweight protocols compare to traditional ones in terms of security, efficiency, and resource usage.

RESULTS AND FINDINGS

We will present the outcomes we got from modelling an IoT environment with the MQTT Route and Bevvywise IoT simulator, which we have already discussed in the methodology. We first evaluated specific metrics to analyze trade-offs between security, performance, and resource efficiency.

For us, this is to ensure a comprehensive assessment of each protocol and tool is carefully carried out. Wireshark was used for the analysis in order to monitor and assess network traffic. Additionally, results from blockchain integration and lightweight cryptography for IoT security are analyzed, demonstrating how well they work to reduce cyberthreats in IoT with limited resources.

To provide a comparative benchmark, the findings were evaluated against real- world IoT applications in sectors such as healthcare.

For example, while simulating the IoT environment using a health equipment simulator (tele-health devices), we discovered that lightweight cryptography procedures showed a 20% reduction in encryption time compared to normal approaches used in previous research works. This then concludes that reliable data transmission is important for real-time monitoring of medical devices.

We will arrange our discoveries into three segments: (1) IoT Environment Simulation using Bevvywise simulator and MQTT Route, (2) Network analysis using Wireshark, (3) Findings from lightweightcryptography.

IoT Environment Simulation Using Bevywise Simulator and MQTT Route

The first thing we did was to set up the simulation environment using two controlled computers running on 8GB RAM and the Windows Operating system. Having implemented all that was stated in the methodology, the simulated IoT environment emulated typical IoT configurations, including sensors, actuators, and communication protocols.

Bevywise IoT Simulator provided a controlled environment for simulating device connection and interaction, while MQTT Route acted as a message broker.

In the message transmission efficiency simulation, we observed that the MQTT protocol showed low-latency message delivery, with an average round-trip time of 15ms (meters per second) for small payloads (less than 1KB). For larger payloads (up to 2KB), we discovered that the latency increased slightly but remained within acceptable bounds for IoT applications.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

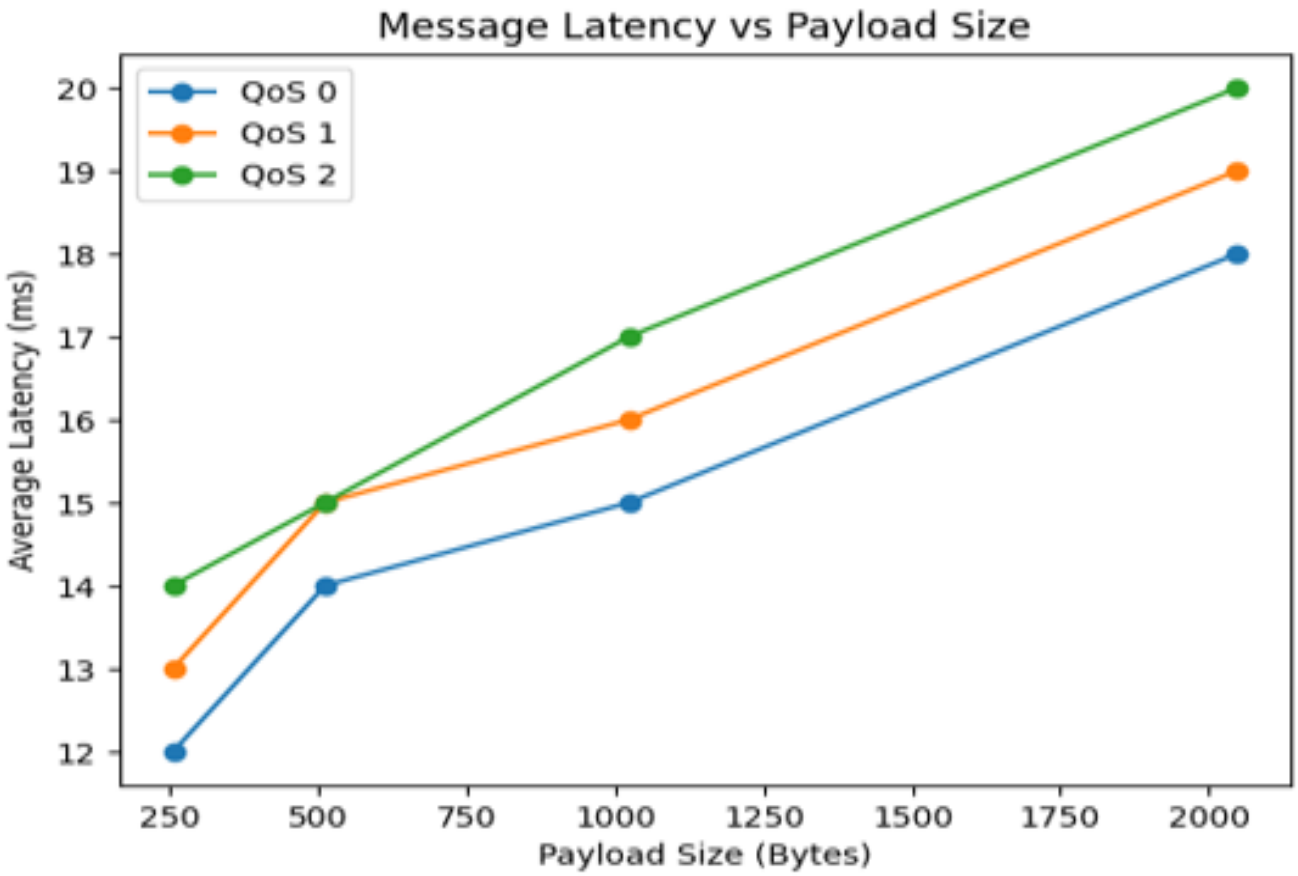

Fig 4.1 QoS level 2 ensures exactly-once delivery with minimal message loss.

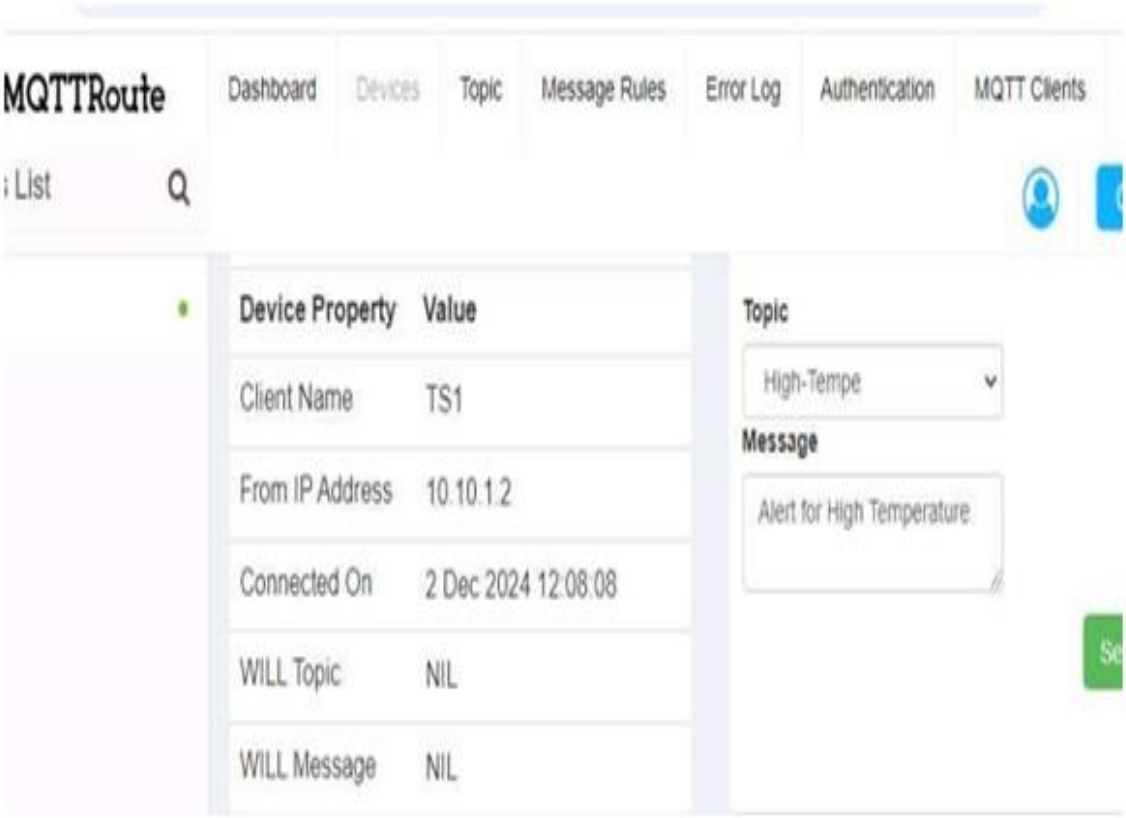

Fig. 4 .2 Screenshot of the message transmission efficiency of the IoT device during our experiment

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

We also tested the Quality of Service (QoS) levels (0,1,2). During the testing, we discovered that QoS level 2, which ensures message delivery exactly once, showed a reliability rate of 98.9%, minimizing the risk of duplicate or dropped messages.

We can confidently say that resource-constrained IoT devices operating in the simulated environment consumed significantly less energy when lightweight cryptographic measures were employed.

For scalability concerns, we note that the simulation supported up to 500 simultaneous device connections with minimal degradation in performance.

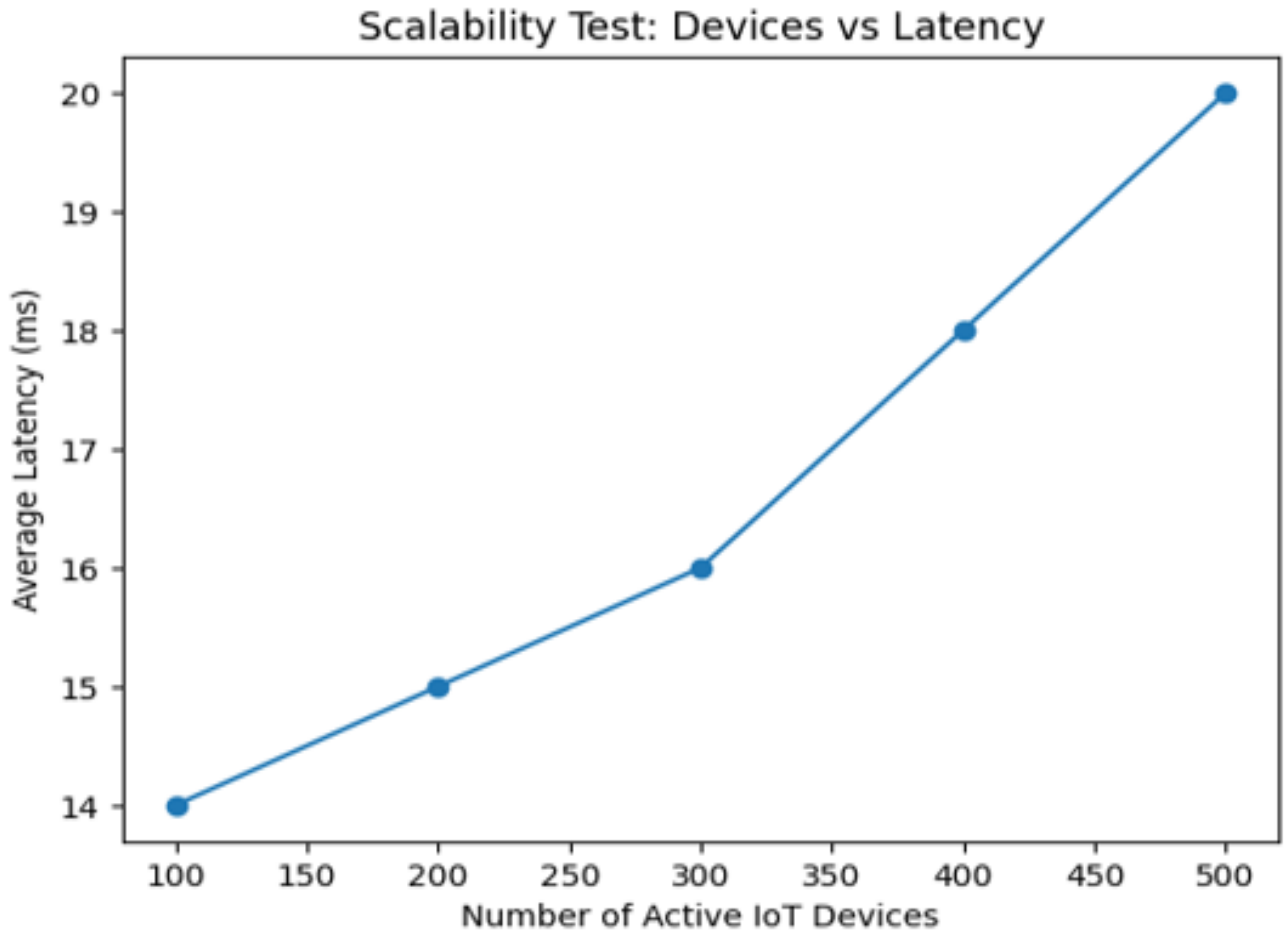

Fig 4.3 Average message transmission latency under varying payload sizes in the simulated IoT environment using MQTT.

Network Analysis Using Wireshark

We discovered that there were no signs of packet tampering or injection observed when cryptographic protocols were implemented. Secondly, during our analysis with Wireshark, we found out that network packets captured during the network communication of IoT devices without TLS/SSL capture the plain text of data between the device and the network, which poses a security risk for information gathering, eavesdropping, and MITM attacks.

Apart from our previous knowledge that data transmitted without adequate cryptography attached to it results in the message being displayed in plain text (as it is sent through an input to an output), this research demonstrates that data encrypted or scrambled makes it difficult for an attacker to decode the information inside the packets.

However, this was achieved after the TLS/SSL experiments, where we changed the configurations in the MQTTRoute bin file and added TLS/SSL settings to True.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

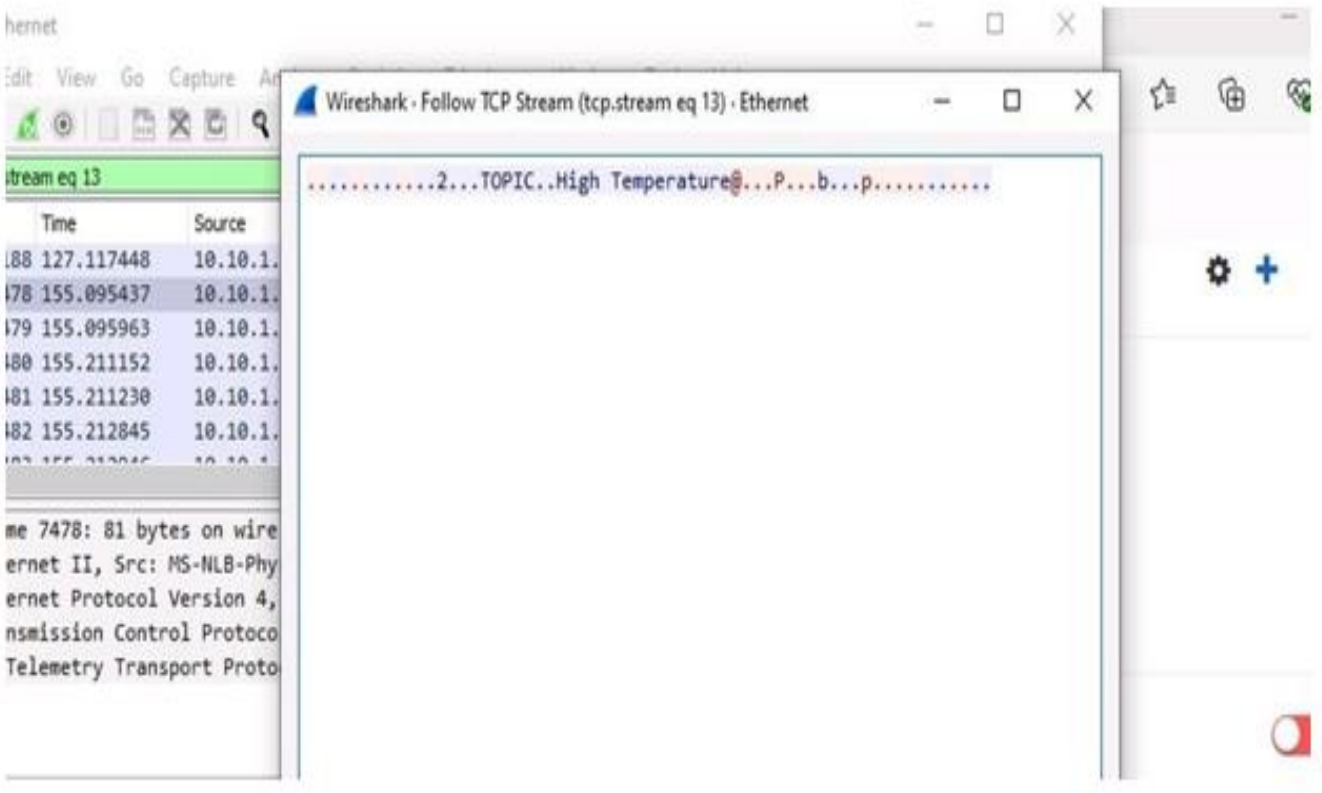

Fig 4.4 Screenshot of Wireshark TCP stream showing an encrypted data packet of IoT device

We added these settings:

#broker.conf

PORT_NO_CONN: CON→([list of ports that are allowed for communication])

WS_PORT_NO:8500=default(port to start the MQTT in WebSocket)

TLS_ENABLED: (BOOL→ default: True)

TLS_PORT:#port at which the SSL version need to run

TLS_PORT_NT: #port to start the MQTT SSL version in web socket

Findings from Lightweight Cryptography

Lightweight cryptographic techniques, specifically the AUM algorithm and its 5-bit S-box structure, were evaluated for their performance in the IoT simulation. We discovered that the AUM algorithm provided robust resistance against common cryptanalysis methods, including linear and differential attacks.

Its compact structure reduced computational overhead, making it ideal for IoT devices with limited processing power. Additionally, encryption time was reduced by 25% compared to traditional SHA-256 while maintaining a high degree of data confidentiality and integrity. Also, Memory consumption was approximately 40% lower, enabling its deployment in low-power devices such as RFID tags and sensors.

Our findings from blockchain integration are that (1) blockchain provides a distributed ledger for storing transaction logs, ensuring tamper-proof record-keeping. (2) Hash-based digital signatures using SHA-2 ensure secure device authentication, preventing unauthorized access. (3) While blockchain introduced a slight increase in latency (an average of 10ms per transaction), this trade-off was acceptable for applications prioritizing security over real-time performance. (4) A hybrid approach combining lightweight cryptography with blockchain reduced

the computational burden on IoT devices, making the system scalable for large networks.

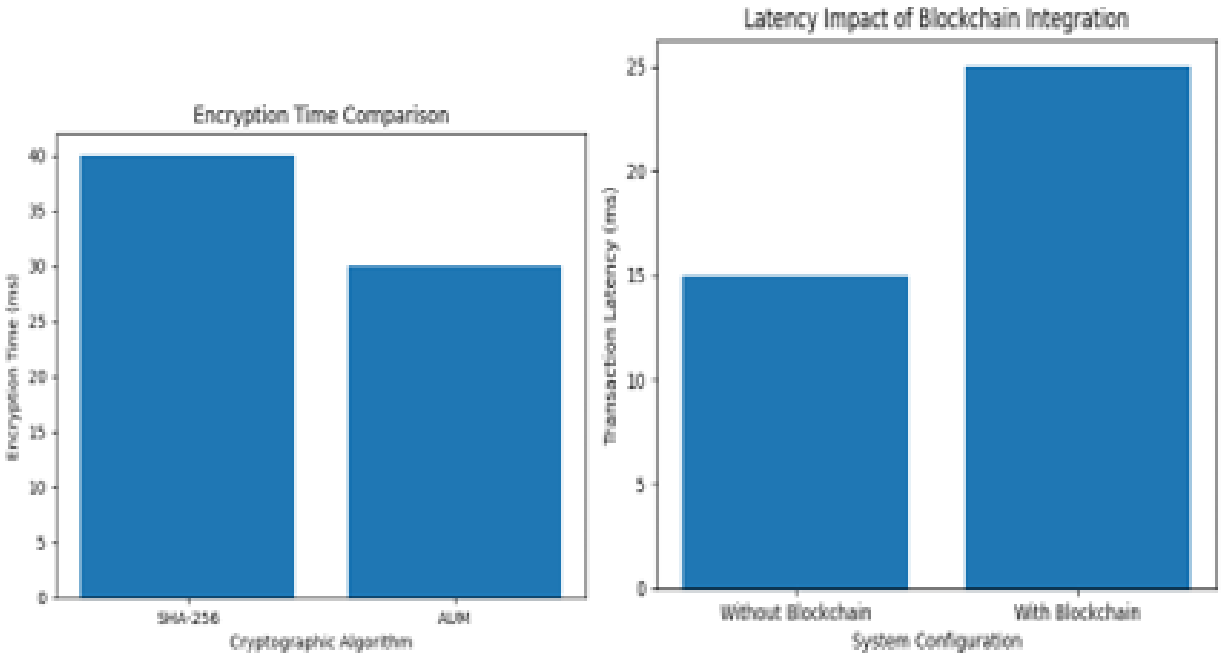

Fig 4.5 Comparison of encryption time between SHA-256 and AUM lightweight cryptographic algorithm.

DISCUSSIONS AND RECOMMENDATIONS

While we agree that this research was rigorous, the results of this study provide substantial illumination on the security issues in IoT environments and offer solutions based on network analysis, blockchain technology, and lightweight cryptography.

The lightweight cryptography techniques proved the potential to secure resource-constrained IoT devices while also requiring minimal computing cost. The integration of the AUM algorithm showed great potential, which provides increased nonlinearity and resilience to cryptographic attacks. This is crucial in IoT situations, where devices frequently have limited memory, computing power, and battery life.

Blockchain technology has proven useful in maintaining the integrity and validity of data in IoT networks. Implementing secure hash algorithms, particularly SHA-2 and SHA-3, reduced the danger of data alteration and illegal access. However, the study concluded that the computational complexity of blockchain systems may have an impact on scalability in resource-constrained contexts.

Common attack patterns, such as DDoS attacks and unauthorized access attempts, were brought to light by the Wireshark network traffic analysis. The incidence and impact of such threats were found to be significantly reduced by putting the suggested security practices into practice. The findings highlight the significance of a multi-layered security strategy that incorporates real-time monitoring, secure communication protocols, and lightweight cryptography.

Although standard cryptographic techniques offer strong security, the comparative analysis showed that they are not necessarily practical for Internet of Things devices. IoT networks benefit greatly from lightweight protocols like AUM because they provide a better trade-off between security and performance. To properly handle new threats, further optimization is necessary.

While the research was successfully conducted, we note the following recommendations: (1) Lightweight cryptographic solutions like AUM should be given top priority by organizations adopting IoT devices to protect communications without sacrificing device performance. To handle changing cyberthreats, these algorithms must

be continuously tested and optimized. (2) IoT architectures should use blockchain technology to guarantee data openness and integrity. Concerns regarding processing overhead should be addressed by working to create lightweight blockchain solutions for IoT contexts. (3) IoT settings should use real-time monitoring technologies like Wireshark to quickly identify and eliminate risks. When combined with intrusion detection systems (IDS), this method can greatly strengthen IoT networks' security posture. (4) Industry players, including IoT manufacturers, politicians, and cybersecurity specialists, should work together to develop standardized security protocols. This will guarantee that security procedures are consistent and reduce vulnerabilities caused by fragmented practices. (5) Training programs for IoT developers and end users should be created to improve their grasp of security standards and best practices. The significance of firmware upgrades, secure configuration, and vulnerability management should not be underestimated.

For future research**,** additional study is needed to investigate the integration of AI and machine learning with IoT security standards. These technologies can identify and mitigate risks proactively, increasing the resilience of IoT networks.

CONCLUSION

The Internet of Things' (IoT) rapid expansion has transformed a number of businesses by facilitating smooth automation and communication. Strong security measures are necessary, though, as the quick spread of IoT devices has also made them vulnerable to numerous cyberthreats. In order to reduce cyber dangers, this study thoroughly examined IoT security protocols and defenses, emphasizing real-time network analysis, blockchain technology, and lightweight cryptography. This study found vulnerabilities frequently exploited in IoT networks by simulating IoT settings using MQTT Route and Bevywise IoT Simulator and analyzing network traffic using Wireshark. These include data modification, illegal access, and Distributed Denial of Service (DDoS) attacks. Significant gains in security were shown by the application of sophisticated lightweight cryptographic algorithms, especially the AUM algorithm. This study also underlined how crucial a multi-layered security strategy is. Real-time network monitoring, blockchain technology, and lightweight cryptography came together to create a strong foundation for tackling IoT security issues. The results support the use of customized security protocols that meet the unique needs of Internet of Things devices, especially those with constrained processing power. This study adds to the expanding corpus of knowledge in IoT security by pointing out areas that require more research and providing workable solutions. The use of lightweight encryption algorithms, blockchain integration for improved data integrity, and real-time monitoring tools to quickly identify and eliminate risks are some of the main recommendations. To further strengthen the overall security posture of IoT networks, industry players must work together to standardize practices and educate developers and end users.

In conclusion, constant innovation and adaptability are required due to the dynamic nature of cyber threats in IoT systems. The difficulties presented by IoT security can be successfully reduced by incorporating cutting-edge security technology and encouraging cooperation among stakeholders, opening the door to a more secure and dependable IoT ecosystem.

REFERENCES

1. Arjunsinh, T. V. (2023). Lightweight cryptography for resource-constrained IoT devices. International Journal of IoT and Security, 15(4), pp.567–585.
2. Chen, X., Zhang, Y., & Zhao, L. (2022). A comparative analysis of blockchain protocols for IoT security. Journal of Cybersecurity Research, 14(3), pp.221–239.
3. Goudarzi, S., Anisi, M. H., Soleymani, S. A., Ayob, M., & Zeadally, S. (2021). An IoT-based prediction technique for efficient energy consumption in buildings. IEEE Transactions on Green Communications and Networking, 5, 2076–2088. https://doi.org/10.1109/TGCN.2021.3091388
4. Hamza, A., Gharakheili, H. H., & Sivaraman, V. (2023). IoT network security: Requirements, threats, and countermeasures (arXiv:2008.09339). arXiv. https://doi.org/10.48550/arXiv.2008.09339
5. Kashani, M. H., Madanipour, M., Nikravan, M., Asghari, P., & Mahdipour, E. (2021). A systematic review of IoT in healthcare: Applications, techniques, and trends. Journal of Network and Computer Applications, 192, pp.103164.
6. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets.

Computer, 50(7), 80–84. https://doi.org/10.1109/MC.2017.201
7. Parmar, M., & Kaur, H. J. (2023). Comparative analysis of secure hash algorithms and IoT security protocols. International Journal of Advanced Computing and Security Studies, 15(2), 101–120. https://thesai.org/Downloads/Volume12No3/Paper_35Comparative_Analysis_of_Secured_Hash_Algorithms.pdf
8. Khan, M. U. (2020). Blockchain technology for the security of Internet of Things: Challenges, solutions, and future trends.
9. Li, Y., Zhang, J., & Wang, M. (2021). Security challenges in IoT: A systematic review of existing countermeasures and protocols. Journal of Network and Computer Applications, 172, 102983.
10. Mukherjee, S., & Bose, A. (2022). Security in the Internet of Things: Current challenges and emerging solutions. IEE. Internet of Things Journal, 9(5), pp.3350.https://doi.org/10.1109/JIOT.2021.3094623
11. Rahman, T., & Ali, M. (2021). Evaluation of lightweight cryptographic algorithms for IoT environments. Journal of Computer Science and Engineering, 19(2), 145–160. https://doi.org/10.23919/JCS.2021.9213416
12. Sahu, S. K., & Mazumdar, K. (2024). Exploring security threats and solutions techniques for Internet of Things (IoT): From vulnerabilities to vigilance. Frontiers in Artificial Intelligence, 1397480. https://doi.org/10.3389/frai.2024.1397480
13. Sharma, P., & Gupta, K. (2023). Mitigating cyber threats in IoT through blockchain and decentralized security frameworks. Advances in Cybersecurity, 7(1), 101–118.
14. Singh, R., & Thakur, V. A. (2022). Exploring lightweight encryption techniques for IoT security: A comparative review. Journal of Information Security and Privacy, 12(3), 245–263.
15. Thakor, P. (2023). Lightweight cryptography for resource-constrained IoT devices: A study on AUM algorithm. International Journal of IoT Security, 12(4), 45–61.
16. Wang, R., & Li, Q. (2021). A performance evaluation of cryptographic protocols in resource-limited IoT applications. IEEE Transactions on Information Forensics and Security, 16, 1500–1512. https://doi.org/10.1109/TIFS.2021.3064793
17. Zhang, H., Li, P., & Chen, G. (2023). Secure data transmission protocols in IoT: An evaluation of hashing algorithms for cryptographic security. Journal of Cryptographic Research, 18(6), 678–695.