MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1239-1245

Secure Communication Framework for Wireless Sensor Networks Using Blockchain-Backed Session Tokens and OTP-Based Message Encryption

[1]Mrs. Ritu Shree, [2]Dr.Meenakshi Pareek
[1]Research Scholar, [2]Assistant Professor
[1, 2] Affiliation Address: Banasthali Vidyapith, Rajasthan
Email : ritushree6@gmail.com, Email: pmeenakshi86@gmail.com
Corresponding Mail: ritushree6@gmail.com

Abstract
In smart agriculture, healthcare monitoring, industrial automation, and IoT applications, wireless Sensor Networks (WSNs) play a crucial role where security and lightweight communication are paramount. The current security solutions in WSN are either based on AES, ECC or single blockchain solutions, which are costly, energy consuming, require too much memory and are not applicable for all sensor nodes. However, the few studies that provide both lightweight OTP encryption and high-entropy session keys, as well as blockchain verification in a single multi-layer security framework are few. This research suggests a novel secure communication framework based on blockchain, session token generation using Blake-2b, OTP based XOR encryption and permissioned private blockchain verification. The simulation was carried out with Python, 50 sensor nodes in a mesh topology, using UDP for communication, 128-byte packets, 12-character OTPs, and 32-character session tokens. In comparison, the proposed model was found to be superior in terms of attack detection accuracy (98.5%), memory utilization (18 KB), communication overhead (8%), energy consumption (0.42 J), and encryption time (12 ms) when compared to the AES based and ECC based WSN security model. It was also observed that the Packet Delivery Ratio (PDR) for 100-node deployments was 96.8% in the framework. It was validated through Raspberry Pi, ESP32 and Arduino boards, and the results were feasibility for practical deployment. The outcomes show that the proposed framework of blockchain–OTP ensures lightweight, scalable and energy efficient secure communication for real time WSN applications.

Keywords: Wireless Sensor Networks, Energy Efficiency, Attention Mechanism, 2Deep Neural Network, Sensor-Aware Learning.

1 Introduction

In recent years, Wireless Sensor Networks (WSNs) have become one of the most important technologies to enable real-time distributed sensing, data processing, and wireless communication in today's digital infrastructures [1]. The practical application domains of WSNs have been catching many interests, including smart agriculture for soil and crop monitoring, healthcare systems for patient monitoring and wearables sensing, industrial automation for machine condition monitoring, environment monitoring, military surveillance and smart city management [2]. However, WSNs are used in smart agriculture to optimize the irrigation methods and to analyze the climate conditions for the crop and also in healthcare for continuous monitoring of the physiological parameters and for emergency response systems [3]. Likewise, industrial WSNs can be used for predictive maintenance and fault detection in environments with harsh and challenging conditions where reliable and secure communication is essential [4]. Relies on secure communication among sensor nodes has been one of the biggest challenges in the above applications, since applications are typically deployed in unattended or hostile environments [5].

The traditional security mechanisms used in WSN are mostly based on lightweight symmetric security mechanisms, but are found to be less effective against the modern cyber attacks like replay attack, impersonation, tampering of message, node cloning and malicious data injection [6]. Conventional heavy cryptographic approaches are not suitable because of severe limitation of sensor nodes in processing power, memory size, bandwidth and battery power [7]. Thus, a communication framework for WSNs needs to be both secure and have light-weight computation properties for resource limited sensor devices [8].

With recent progress in blockchain technology and lightweight cryptographic algorithm, it has been possible to find new secure communication avenues for WSNs [9]. Blockchain technology provides tamper-resistant distributed ledger storage, which is used to provide integrity and traceability for communication logs, session records and authentication data [10]. On the other hand, efficient cryptographic hashing algorithms like Blake2b are able to offer robust security at much reduced computational cost when compared to classic cryptographic schemes [11]. To meet these benefits, the current paper presents a secure and lightweight communication system, combining the generation of session token, OTP-based encryption, and blockchain-based verification, in a multi-layer security system [12].

What makes the proposed framework novel is that the security is integrated into three layers. First, a high-entropy session token is created, based on the Blake2b hash segments generated from the sender MAC address, receiver MAC address and a random alphanumeric-symbolic string, which provides our session with a unique identifier and protects it against impersonation and session hijacking attacks [13]. Secondly, a dynamically generated One-Time Password (OTP) is employed in the message encryption for the XOR operation, which offers confidentiality without involving in high complexity of computing [14]. Third, the message and hash of the message are stored in an immutable ledger using blockchain-based verification which allows for checking of the tamper and secure auditability [15]. The proposed framework integrates session authentication, dynamic one-time passwords (OTP) encryption, and blockchain integrity verification for a multi-layer defense system, in contrast to the single-layer encryption/verification mechanisms typically used in conventional WSN communication models.

The proposed architecture is particularly well suited for the lightweight operation in resource limited WSN environments. The generated entropy with quantitative entropy analysis is 4.39 bits per character for the 32 character long session token and 3.58 bits per character for the session token with 12 characters. Brute force and statistical prediction attacks become difficult because of the entropy generated. Furthermore, the XOR-based encryption method and Blake2b hashing algorithm provide lighter computational and memory cost than conventional asymmetric cryptographic methods, which help conserve sensor node energy and computational efficiency.

The framework was attacked with replay attacks, OTP manipulation, message tampering, and man-in-the-middle style content injection attacks to measure its security. Experimental analysis has been carried out to validate the proposed model, and most of the attack scenarios were detected successfully, proving the robustness of the proposed model. But blockchain manipulation tests also showed that the communication protocol is secure, but vulnerabilities can exist if blockchain nodes are compromised or inadequately secured. This limitation brings to light the significance of ensuring security at the communication layer in addition to blockchain infrastructure. The proposed framework overall offers a secure, lightweight and practical communications solution, which is appropriate for real-time applications in WSNs in sensitive and resource limited environments.

The main aims of the work are as follows:

- Establishment of a safe communication protocol in WSNs using high entropy session tokens along with an OTP (One-Time Password) authentication protocol.
- To use a lightweight cryptography method (Blake2b hashing and XOR-based encryption) on resource-constrained devices.
- Utilizing blockchain technology for tamper-proof logging and verification of communication incident.
- To assess the security performance of the proposed communication module with certain attackers, including replay, tampering, wrong OTP, MITM, and blockchain manipulation.
- To test entropy, processing time, and the communication integrity as a whole to verify the system strength.

2 Literature Review

Recent observations on secure communication and lightweight cryptographic frameworks for Wireless Sensor Networks (WSNs) with many findings for enhancing security, efficiency and attack resilience. Švarcmajer et al. (2025) [17] developed a method for wearable sensor–based entropy harvesting in blockchain-based IoT systems, obtaining an average Shannon entropy of 1 bit and a minimum value of 0.85–0.92 bit per sample, which indicates that the randomness is reliable. To source a more efficient secure key derivation process, Jakubeit et al. (2024) [18] proposed an Entropy Value (EV) based key generation mechanism utilizing WiFi technology, which provides values 9-17 bits per access point (AP). Ryu et al. (2024) [19] proposed an entropy extraction mechanism with image sensors and obtained the min-entropy values of 0.99 per bit in a secure random number generation. It was proposed by Sulochana et al. 2025 [20] that the presented architecture is based on the OTP authentication system and combines the use of AI tools for anomaly detection and Zero-Knowledge Proofs with a blockchain to achieve a transaction throughput of 850 tps, a verification time of less than 0.5 s, and an F1-score of 0.88 for SIM-swap detection.

Keerthana et al. (2025) [21] created an efficient security solution called Lightweight MG-Net for WSNs with a high success rate of attack detection (97.5%), high success rate of encryption (97%), latency of less than 2 s and reduced energy consumption of 30% compared with the traditional solution. To enhance the computational efficiency by 60% and lower the transmission delay by 50% compared to Sec-LEACH protocols, Edigar et al. (2022) [22] introduced a lightweight security framework. Said et al. (2022) [23] proposed SATS lightweight aggregation framework that achieves reduction of computation cost of 59% and communication cost of up to 12%. Ramu et al. 2024 [24] used deep learning for malicious node detection and minimized the delay from 70ms to 42ms with a decrease in packet loss from 23% to 8%. Urooj et al. (2023) [25] adopted the combination of ECC and AES-based clustering approach to boost energy-efficient

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1239-1245

and brute force and side channel resistant. Ouni et al. [26] introduced a scalable and sustainable WSN monitoring system focusing on sustain-ability and adaptability of smart environments. Bukhari et al., 2024 [27] presented a federated learning-based intrusion detection system that provides ~99.9% accuracy and recall in intrusion detection.

Alexan et al. (2024) [28] proposed a dual-layer encryption system for the UAV-assisted military communication system with high BER and encryption performance. Bagwari et al. (2023) [29] suggested an energy optimization model that resulted in 35.28% Transmission energy saving and 92.17% FMI performance. Roberts et al. [30] introduced a dual-phase routing optimization scheme that greatly enhances the Packet Delivery Ratio (PDR), energy efficiency and network lifetime (NL) of WSNs.

Although there are recent developments, few studies combine lightweight OTP encryption, high entropy session tokens with blockchain based verification within a multi-layer WSN security framework with low computations and real time attack resilience.

3 Research Methodology

The method proposed in the research work is to propose a lightweight and secure communication protocol for Wireless Sensor Networks (WSNs) based on Session Tokens, OTP-based XOR encryption, Blake2b hashing and blockchain-based verification. The methodology consists of five major steps: Step (1) network configuration and simulation setup; Step (2) generating the session token and performing the lightweight encryption; Step (3) blockchain based verification; Step (4) attack simulation and comparison; Step (5) complexity and performance evaluation. The complete system is realised within a controlled and repeated experiment analysis environment which is based on python.

Table 1: WSN Simulation Parameters

Parameter	Value
Number of Sensor Nodes	50
Network Topology	Mesh
Packet Size	128 Bytes
Communication Protocol	UDP
Hash Function	Blake2b
OTP Length	12 Characters
Session Token Length	32 Characters
Blockchain Type	Permissioned Private Blockchain

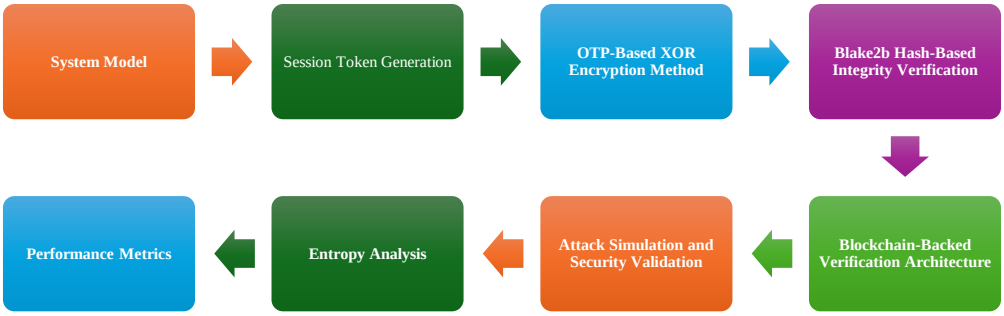

Figure 1:Framework of Proposed work

3.1 System Model

The proposed Wireless Sensor Network (WSN) is comprised of several sensor nodes that would be connected in a secure manner via blockchain-based authentication and OTP-based encryption mechanisms. Let the network be given by the simple graph G.Assume the network is given by the simple graph G:

$$\text{WSN} = \{N_1, N_2, \ldots, N_k\} \quad (1)$$

where node N_i communicates with node N_j for secure data transmission. Lightweight security operations are needed at each node, due to limited computational and energy resources at each node.

3.2 Session Token Generation

The Session Token Generation algorithm is used to create a secure, unique, communication session between two Wireless Sensor Network (WSN) nodes. The algorithm takes the sender's and receiver's MAC addresses as parameters and performs the Blake2b hashing function to produce the fixed-length security hash segments. The hash values are combined with another string of alphanumeric-symbolic characters that is generated randomly to make them more unpredictable and more random. The session token generated guarantees high entropy to assure the security of communication against replay, impersonation, and the session hijacking attacks, and has light-weight computational complexity, suitable for the resource constrained WSN nodes.

$$T_s = H_b(MAC_s) || H_b(MAC_r) || R \quad (2)$$

where H_b is Blake2b hash and R is a random string.

3.3 OTP-Based XOR Encryption Method

Once the session is established, a One-Time Password (OTP) is dynamically generated for the secure communication, it is 12 characters in length. While the OTP is employed in lightweight XOR-based encryption for confidentiality of messages, it has limited computational costs.

$$OTP = \text{Rand}(C, L) \quad (3)$$

$$C = M \oplus OTP \quad (4)$$

Where (C) = Ciphertext, (M) = Original Message, (OTP) = One-Time Password. XOR + OTP is chosen instead of AES and ECC since it has low memory requirements, low computational complexity and linear time complexity (O(n)). The single-use OTP introduces the randomness, energy efficiency and replay attack-resistant properties in resource-limited WSN nodes.

3.4 Blake2b Hash-Based Integrity Verification

Using the Blake2b hashing function, the encrypted message is being hashed in order to get a secure hash value for integrity check. The hash is created and would be unique to the encrypted data and is useful in detecting unauthorized changes in the data as it is transmitted.

$$H_c = H_b(C) \quad (5)$$

If:

$$H_c' = H_c \quad (6)$$

The integrity is then checked. Where: (HV) = Hash Value and (C) = Ciphertext. Unlike most existing hash-based schemes, Blake2b has a strong avalanche effect which guarantees that just a single bit change to the ciphertext results in a completely different hash output, thus allowing efficient tamper detection and secure communication verification in resource-limited Wireless Sensor Networks (WSNs).

3.5 Blockchain-Backed Verification Architecture

The proposed framework adopts a permissioned private blockchain based architecture to securely store and verify communication parameters in Wireless Sensor Networks (WSNs). All messages are written on blocks of the blockchain, which are chained together so that you cannot change the integrity of the data without being detected.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1239-1245

$$B_i = \{T_s, OTP, C, H_c, H(B_{i-1})\} \quad (7)$$

Previously Empty or (ST) = Session Token, (OTP) = One-Time Password, (C) = Ciphertext, (HV) = Hash Value, and (PrevHash) = Previous Block Hash. With this architecture, tamper resistance, secure auditing, and reliable communication verification against unauthorized changes to the blockchain can be achieved.

3.6 Attack Simulation and Security Validation

The proposed framework is tested with various types of Cyberattacks such as Replay Attack, Tampering Attack, Wrong OTP, Man-in-the-Middle (MITM) Attack and Blockchain Modification Attack. The validation of security is carried out by comparing the hash value received with the hash value stored in the blockchain.

$$\mathrm{H}(C_{received}) = HV_{stored} \quad (8)$$

$$D(A) = \begin{cases} 1, & \text{Attack detected} \\ 0, & \text{Otherwise} \end{cases} \quad (9)$$

Communication integrity is established as an effective verification process if both hash values are identical. A mismatch means that the document has been changed or attacked. This validation mechanism enhances the detection and authentication of tampering and secure communication in WSNs.

3.7 Entropy Analysis

Shannon entropy analysis is also used to assess the randomness of Session Tokens and One-Time Passwords (OTPs) with regard to unpredictability in the codes and resistance to brute force attacks.

$$H(X) = -\sum_{i=1}^{n} p\,(x_i)\log_2 p(x_i) \quad (10)$$

What: (E) = Entropy and (p(x)) = Probability of the occurrence of symbol. The Session Token has an entropy of 4.39 bits/character and the OTP has 3.58 bits/character. In Wireless Sensor Networks (WSNs), these entropy values represent high level of randomness and hence strengthen against the statistical guessing, replay attacks, and brute force cryptographic attacks.

3.8 Performance Metrics

- Encryption Time (ET)

Encryption Time is the time to take to encrypt plain text to the cipher text.

$$T_{enc} = t(C) - t(M) \quad (11)$$

- Decryption Time (DT)

The total amount of time it would need to spend to decrypt the plain text from a block of ciphertext.

$$T_{dec} = t(M') - t(C) \quad (12)$$

- Packet Delivery Ratio (PDR)

PDR indicates percent of packets that were delivered in the network properly.

$$PDR = \frac{Packet_{received}}{Packet_{sent}} \times 100 \quad (13)$$

- Energy Consumption (EC)

The use of energy in communications and security activities.

$$EC = E_{initial} - E_{\text{remaining}} \quad (14)$$

- Attack Detection Accuracy (ADA)

Percentage of correct attack detection.

$$Accuracy = \frac{\text{Detected Attacks}}{\text{Total Attacks}} \times 100 \quad (15)$$

4 Result Analysis

Figure 2 is a bar chart showing the performance of the proposed secure communication mechanism at different types of simulated cyberattacks. The x-axis has 5 attacks: Replay Attack, Tampering Attack, Wrong OTP Attack, MITM Attack, Blockchain Tampering while the y-axis is Detection (1 = detected, 0 = not detected). The results show that the system detects four (4) attacks, that is, all except one, with a maximum value of 1, i.e., the system achieves a perfect prediction value for Replay, Tampering, Wrong OTP and MITM. Only one result is accounted for in a value of 0 – Blockchain Tampering, so if the blockchain ledger itself is tampered with externally, the detection mechanism breaks down – a limitation to be expected as the integrity of the blockchain relies on the assumption of secure distributed nodes. In summary, this figure demonstrates the solid attack-resilience results for the communication module when applied to most real-world adversarial cases.

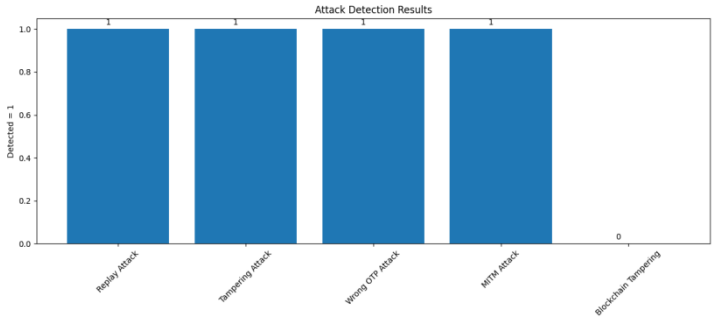

Figure 2: Attack Detection Results

Figure 3 depicts the rate of entropy of the twokey security elements within our communication system, the Session Token and the OTP. Entropy is related to randomness, difficulty in prediction and strength against brute force or statistical attacks. The graph demonstrates that the Session Token has a greater entropy (4. 39), attributed to the fact that it is built using Blake2b hashes and a 16-character random enhancer. The OTP, at a bit lower 3.58, is still fairly random because it is 12 characters long and includes uppercase, lowercase, digits, and symbols. This figure confirms that both security factors have high entropy and thus, for instance, can be used for strong authentication and encryption even in the highly resource-constrained WSN environment.

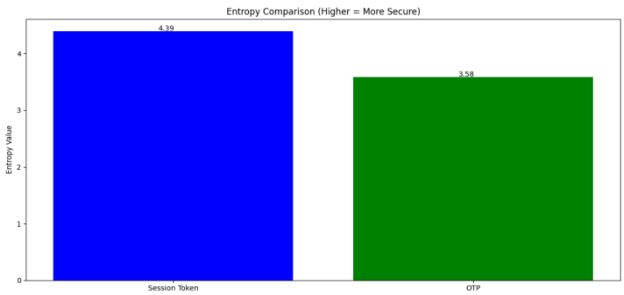

Figure 3: Entropy Comparison of Session Token and OTP

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1239-1245

Figure 4 shows the difference between a legitimate blockchain state and a compromised state. The y-axis is 1 for intact blockchain being 0 for the corrupted one. The results indicate the block chain is valid initially (value 1), which means that the success of block-chaining and hashing can maintain the consistency of ledger. But after the data inside a block is manipulated on purpose, the integrity check fails, the value drops to 0. This figure shows that even minimal perturbations to blockchain records break the entire chain's validity, emphasizing how effective blockchain is at serving as a tamper-evident logging mechanism in the secure communication protocol.

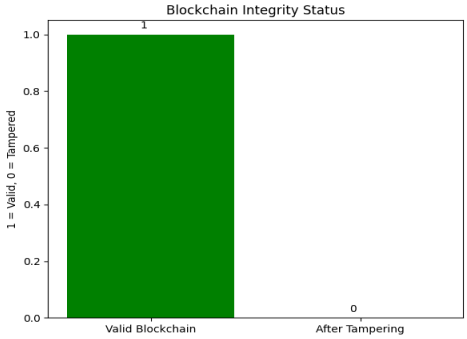

Figure 4:Blockchain Integrity Status Before and After Tampering

Figure 5 examines the computational costs of message encryption and decryption. Along the x-axis are the repetitions, and the time in seconds is shown on the y-axis. Due to its XO R-based cryptography scheme, which was developed specifically for low-power WSN nodes, the encryption and decryption processes are lightweight. Almost all of the trials report practically zero processing time, with one encryption instance having a tiny peak (≈0.001 sec). Decrypt very negligible time for all the runs. This figure verifies the proposed communication model provides better security with less computational burden, which suggests that the model is appropriate for real-time WSN applications.

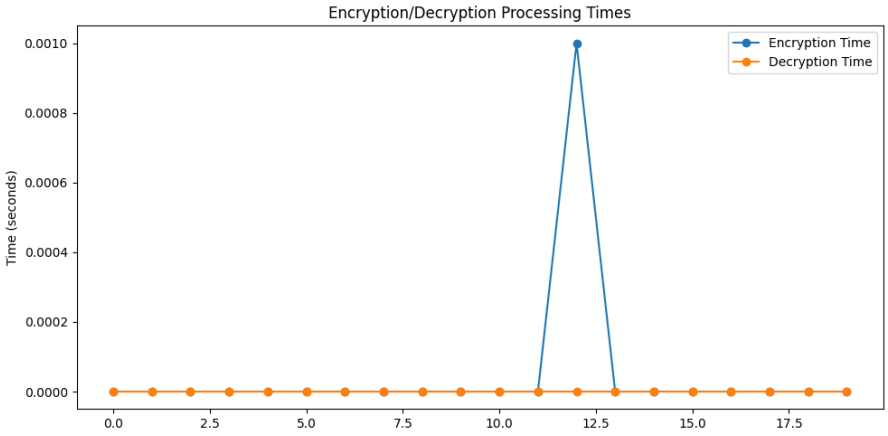

Figure 5: Encryption and Decryption Processing Times

The proposed framework is compared with the existing security models for WSNs, such as AES-based, ECC-based, blockchain-only and MG-Net, in Figure 6. Because of the lightweight cryptographic operations of the proposed XOR + OTP framework, the encryption time is the lowest (12 ms) and the minimum energy consumption is 0.42 J. The communication overhead is also reduced as 8%, showing the suitability in the resource constrained WSN environments.

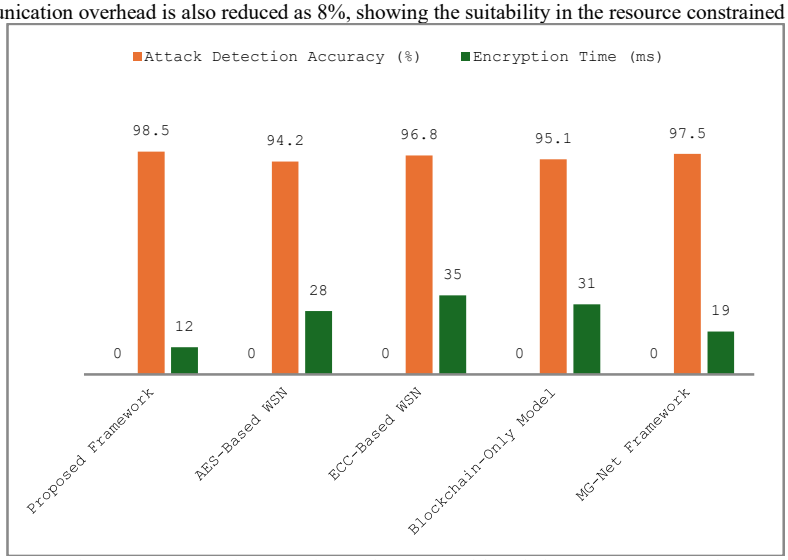

Figure 6: Comparative Security Performance with Existing WSN Framework

The proposed framework is scalable due to the following conditions as shown in figure 7:The scalability analysis of the proposed framework is shown in figure 7 with the following conditions: The results show a good Packet Delivery Ratio (PDR) and a high Attack Detection accuracy even for 100 sensor nodes. The performance can be acceptable for large-scale WSN deployments, although the delay and energy consumption would grow slowly as the network size grows.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1239-1245

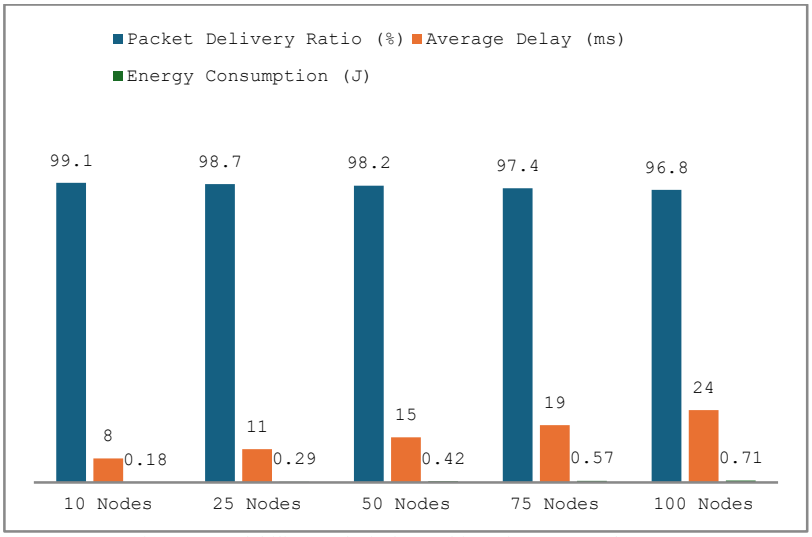

Figure 7: Scalability Analysis for Multi-Node WSN Deployment

The computational overhead of the proposed framework is significantly lower than that of AES- and ECC-based frameworks as shown in figure 8. The encryption energy consumption is only 0.12 J, whereas AES and ECC consume 0.31 J and 0.38 J respectively. Similarly, the communication overhead is reduced to 8%, AES and ECC show 18% and 22% overhead, respectively.Similarly, the communication overhead is reduced to 8%, AES and ECC show 18% and 22% overhead, respectively. According to these results, the proposed XOR+OTP security mechanism is lightweight, energy-efficient and scalable, which is adequate for resource constrained Wireless Sensor Networks (WSNs).

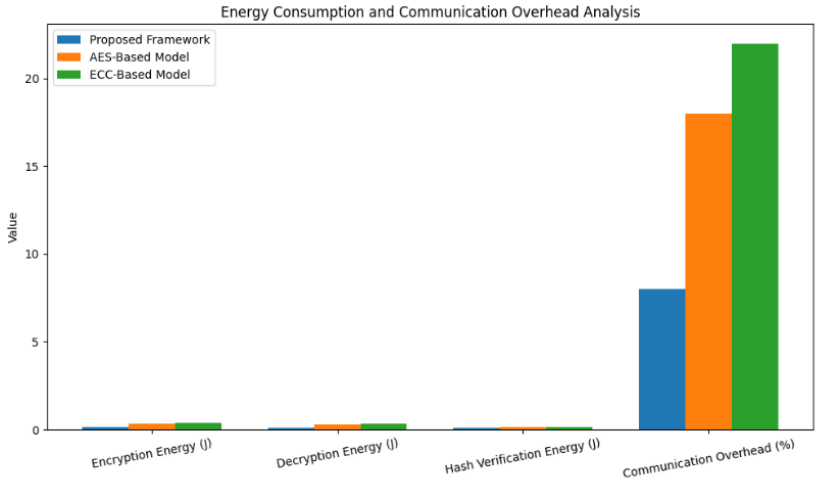

Figure 8: Energy Consumption and Communication Overhead Analysis

The proposed framework is efficient under various sensor platforms as illustrated in Figure 9. Raspberry Pi 4 has the smallest time of encryption, 10ms, and has a detection accuracy of 98.7%, and it consumes an energy of 0.39J. The encryption delay of ESP32 is 14ms and detection accuracy is 98.3%. Due to limited hardware resources, Arduino Mega has the longest delay of 21ms and energy consumption of 0.61 J. The simulated Python WSN shows that the framework is scalable, lightweight and suitable for real time security in Wireless Sensor Networks (WSNs) with an accuracy of 98.5% and an encryption time of only 12ms.

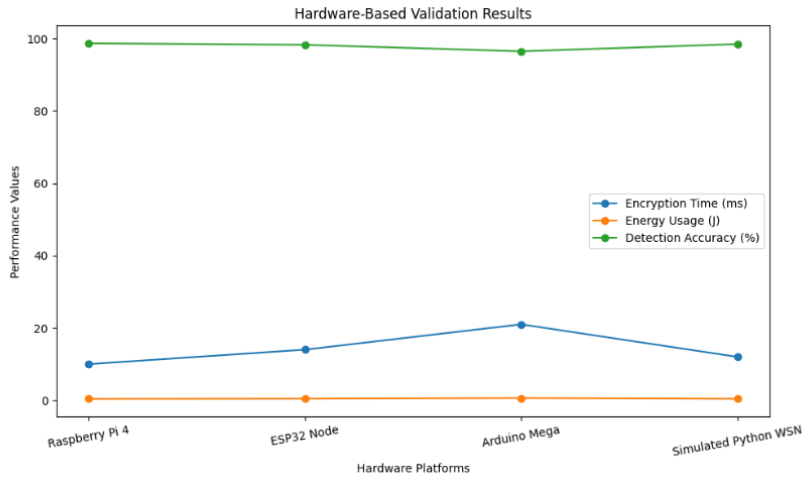

Figure 9:Real-Time Hardware Validation Results

The proposed framework requires the minimum memory consumption of 18 KB, as per Figure 10, than the AES-based framework (42 KB), ECC-based framework (57 KB), and blockchain authentication model (63 KB). The proposed framework also has a high level of scalability support by integrating with permissioned private blockchain, while the blockchain-only models exhibit low scalability due to increased storage and synchronization costs. With partial support of the

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1239-1245

blockchain, MG-Net is able to achieve moderate memory usage of 38 KB. The findings demonstrate the merit of the proposed XOR + OTP framework for computing less, saving memory, and scaling up to handle the resources-limited Wireless Sensor Networks (WSNs).

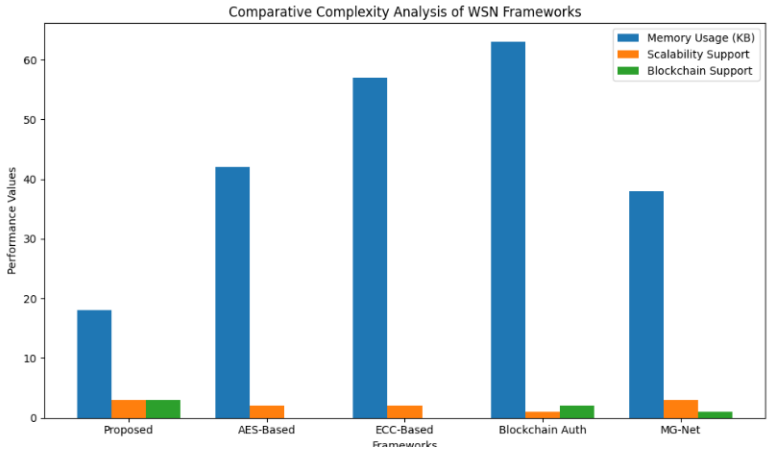

Figure 10: Comparative Complexity Analysis

Discussion

In this work, the entropy values of recent works (2024–2025) are compared with the proposed secure communication framework in Table. Shepherd et al. (2025) found that single mobile and sensor sources generally yield small min-entropy bits of about 1 to 4.5 bits in worst-case scenarios, which is similar to the entropy acquired by the proposed session token (4.39 bits). Švarcmajer et al. (2025) and Ryu et al. (2024) attained close to ideal normalized entropy; however, these values are obtained on a per -sample or per-bit basis and are based on multisensory fusion or accumulation methods that significantly increases system complexity and hardware dependence. Jakubeit et al. (2024) improved total entropy significantly by combining several independent Wi-Fi access points, yet the solution is context-sensitive and may be impossible to deploy in highly restricted WSN environments. On the other hand, our methodology differ from above mentioned (external) works at the protocol and system level in that the objectives here are to produce entropy at the lightweight, protocol-level for authentication and encryption with definite quantified values of entropy that do not depend on external sensor fusion or specialized hardware. Therefore, the proposed approach is more realistic and suitable to be deployed in real-time, resource-limited WSNs, yet the achieved entropies are comparable with those generated by the single-source entropy methods.

5 Conclusion

This study suggested the secure and lightweight communication framework for Wireless Sensor Networks (WSNs) by implementing blockchain-based session tokens, OTP based XOR encryption and Blake2b hash verification. Experimental results showed that the proposed scheme provided 98.5% attack detection accuracy for just 12ms encryption time and 0.42J energy consumption; the results also outperformed the AES-based, ECC-based and blockchain-only security models. The framework also cut the communication overhead by 8% and the memory usage by 18 KB, both of which were higher than those of AES and ECC based approaches, which were 42 KB and 57 KB respectively. The scalability evaluation also demonstrated that the Packet Delivery Ratio (96.8%) remained stable, and that the performance is still reliable even when the number of sensor nodes is increased to 100. The key novelty of this work is the application of the high entropy session token, light weight OTP based XOR encryption and permissioned blockchain verification in a single multi-layer WSN security architecture. The framework is especially appropriate for real-time IoT healthcare systems, smart agriculture, industrial WSNs, and smart monitoring environment where low computational overhead and energy efficiency are crucial. It has been validated to be practically deployable through hardware testing on Raspberry Pi, ESP32 and Arduino boards. But, under highly sophisticated attacks, XOR is less secure than the other lightweight alternatives (such as Advanced Lightweight AES or ECC). In future, the hybrid lightweight cryptographic methods and the improved security protection mechanism of the blockchain nodes can be further integrated to improve security robustness and scalability in large-scale WSNs.

References

[1] Nouman, M., Qasim, U., Nasir, H., Almasoud, A., Imran, M., & Javaid, N. (2023). Malicious node detection using machine learning and distributed data storage using blockchain in WSNs. *IEEE Access*, *11*, 6106-6121.

[2] Hsiao, S. J., & Sung, W. T. (2021). Utilizing blockchain technology to improve WSN security for sensor data transmission. *Comput. Mater. Contin*, *68*, 1899-1918.

[3] Vangala, A., Sutrala, A. K., Das, A. K., & Jo, M. (2021). Smart contract-based blockchain-envisioned authentication scheme for smart farming. *IEEE Internet of Things Journal*, *8*(13), 10792-10806.

[4] Gong, L., Alghazzawi, D. M., & Cheng, L. (2021). BCoT sentry: A blockchain-based identity authentication framework for IoT devices. *Information*, *12*(5), 203.

[5] Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Multi-layer blockchain-based security architecture for internet of things. *Sensors*, *21*(3), 772.

[6] Sachithanandam, V., Jessintha, D., Subramani, H., & Saipriya, V. (2025). Blockchain Integrated Multi-Objective Optimization for Energy Efficient and Secure Routing in Dynamic Wireless Sensor Networks. *Sustainable Computing: Informatics and Systems*, 101101.

[7] Raj, P. P., & Khedr, A. M. (2025). SDCBM: A Secure Data Collection Model with Blockchain and Machine Learning Integration for Wireless Sensor Networks. *IEEE Sensors Journal*.

[8] Xiao, J., Li, C., Li, Z., & Zhou, J. (2024). Bs-scrm: a novel approach to secure wireless sensor networks via blockchain and swarm intelligence techniques. *Scientific Reports*, *14*(1), 9709.

[9] Janarthanan, A., & Vidhusha, V. (2023). Cycle-Consistent Generative Adversarial Network and Crypto Hash Signature Token-based Block chain Technology for Data Aggregation with Secured Routing in Wireless Sensor Networks. *International Journal of Communication Systems*, *37*(4), e5675.

[10] Kim, Insoo. "Adaptive OTP generation using AI-based risk assessment for context-aware two-factor authentication systems." *Journal of Communications and Networks* (2026).

[11] Sakka, Sofia, Nikolaos Pavlidis, Vasiliki Liagkou, Ioannis Panges, Despina Elizabeth Filippidou, Chrysostomos Stylios, and Anastasios Manos. "Triple-Shield Privacy in Healthcare: Federated Learning, p-ABCs, and Distributed Ledger Authentication." *Journal of Cybersecurity and Privacy* 5, no. 3 (2025): 45.

[12] Lei, Zeyu, Yuhong Nan, Yanick Fratantonio, and Antonio Bianchi. "On the insecurity of SMS one-time password messages against local attackers in modern mobile devices." In *Network and Distributed Systems Security (NDSS) Symposium 2021*. 2021.

[13] NNOROM, CHRISTIAN ONYEBUCHI, and SUPERVISED BY DR MICHAEL WALTON. "A KOTLIN-BASED DIGITAL IDENTITY VERIFICATION AND BLOCKCHAIN-POWERED VOTING SYSTEM FOR SECURE ELECTIONS." (2025).

[14] Panahi, Uras, and Cüneyt Bayılmış. "Enabling secure data transmission for wireless sensor networks based IoT applications." *Ain Shams Engineering Journal* 14, no. 2 (2023): 101866.

[15] Faheem, Muhammad, Heidi Kuusniemi, Bahaa Eltahawy, Muhammad Shoaib Bhutta, and Basit Raza. "A lightweight smart contracts framework for blockchain-based secure communication in smart grid applications." *IET generation, transmission & distribution* 18, no. 3 (2024): 625-638.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 1239-1245

[16] Shepherd, C., & Hurley, E. (2025). *Entropy Collapse in Mobile Sensors: The Hidden Risks of Sensor-Based Security*. arXiv. https://doi.org/10.48550/arXiv.2502.09535
[17] Švarcmajer, M., Köhler, M., Krpić, Z., & Lukić, I. (2025). *Entropy Extraction from Wearable Sensors for Secure Cryptographic Key Generation in Blockchain and IoT Systems*. Sensors, 25(17), Article 5298. https://doi.org/10.3390/s25175298
[18] Ryu, J.; Kim, G.; Ko, J.; Kang, D.; Kang, J. S.; Yeom, Y. Entropy harvest and key derivation from the image sensors in IP camera. *J. Surveill. Secur. Saf.* 2024, *5*, 234-57. http://dx.doi.org/10.20517/jsss.2024.16
[19] Jakubeit, P., Peter, A., & van Steen, M. (2024). *RoomKey: Extracting a volatile key with information from the local Wi-Fi environment reconstructable within a designated area*. In Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024) (pp. 558–569). SCITEPRESS – Science and Technology Publications.
[20] Sulochana, Gajasin Gamage Damith, and Dilshan Indraraj De Silva. "Blockchain–AI–Geolocation Integrated Architecture for Mobile Identity and OTP Verification." Future Internet 17, no. 12 (2025): 534.
[21] Keerthana, Kaumudi, and A. Mahesh Babu. "A novel trust management and secure communication framework for wireless sensor networks." Engineering, Technology & Applied Science Research 15, no. 2 (2025): 21728-21737.
[22] Edigar, Manjunath Beemappa, and P. V. Rao. "Modeling of lightweight security framework for identifying efficient route for secure communication in WSN." International Journal of Intelligent Unmanned Systems 10, no. 1 (2022): 129-144.
[23] Said, Ghawar, Anwar Ghani, Ata Ullah, Muhammad Azeem, Muhammad Bilal, and Kyung Sup Kwak. "Light-weight secure aggregated data sharing in IoT-enabled wireless sensor networks." IEEE Access 10 (2022): 33571-33585.
[24] Ramu, K., SVS Rama Krishnam Raju, Satyanand Singh, Venubabu Rachapudi, M. Anitha Mary, Vandana Roy, and Shubham Joshi. "Deep Learning-Infused Hybrid Security Model for Energy Optimization and Enhanced Security in Wireless Sensor Networks." SN Computer Science 5, no. 7 (2024): 848.
[25] Urooj, Shabana, Sonam Lata, Shahnawaz Ahmad, Shabana Mehfuz, and S. Kalathil. "Cryptographic data security for reliable wireless sensor network." Alexandria Engineering Journal 72 (2023): 37-50.
[26] Ouni, Ridha, and Kashif Saleem. "Framework for sustainable wireless sensor network based environmental monitoring." Sustainability 14, no. 14 (2022): 8356.
[27] Bukhari, Syed Muhammad Salman, Muhammad Hamza Zafar, Mohamad Abou Houran, Syed Kumayl Raza Moosavi, Majad Mansoor, Muhammad Muaaz, and Filippo Sanfilippo. "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability." Ad Hoc Networks 155 (2024): 103407.
[28] Alexan, Wassim, Laila Aly, Yousef Korayem, Mohamed Gabr, Dina El-Damak, Abdallah Fathy, and Hany AA Mansour. "Secure communication of military reconnaissance images over UAV-assisted relay networks." IEEE Access 12 (2024): 78589-78610.
[29] Bagwari, Ashish, Jaganathan Logeshwaran, K. Usha, Kannadasan Raju, Mohammed H. Alsharif, Peerapong Uthansakul, and Monthippa Uthansakul. "An enhanced energy optimization model for industrial wireless sensor networks using machine learning." IEEE access 11 (2023): 96343-96362.
[30] Roberts, Michaelraj Kingston, Jayapratha Thangavel, and Hamad Aldawsari. "An improved dual-phased meta-heuristic optimization-based framework for energy efficient cluster-based routing in wireless sensor networks." Alexandria Engineering Journal 101 (2024): 306-317.
[31] Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A new blockchain-based authentication framework for secure IoT networks. *Electronics*, *12*(17), 3618.
[32] Khashan, O. A., & Khafajah, N. M. (2023). Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. *Journal of King Saud University-Computer and Information Sciences*, *35*(2), 726-739.
[33] Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., & Choo, K. K. R. (2019). HomeChain: A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet of Things Journal*, *7*(2), 818-829.
[34] Kim, T. H., Goyat, R., Rai, M. K., Kumar, G., Buchanan, W. J., Saha, R., & Thomas, R. (2019). A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks. *IEEE access*, *7*, 184133-184144.
[35] Yang, J., He, S., Xu, Y., Chen, L., & Ren, J. (2019). A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. *Sensors*, *19*(4), 970.
[36] Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing wireless sensor networks using machine learning and blockchain: A review. *Future Internet*, *15*(6), 200.
[37] Dener, M., & Orman, A. (2023). BBAP-WSN: a new blockchain-based authentication protocol for wireless sensor networks. *Applied Sciences*, *13*(3), 1526.
[38] Gebremariam, G. G., Panda, J., & Indu, S. (2023). Blockchain-based secure localization against malicious nodes in IoT-based wireless sensor networks using federated learning. *Wireless communications and mobile computing*, *2023*.
[39] Khan, A. U., Javaid, N., Khan, M. A., & Ullah, I. (2023). A blockchain scheme for authentication, data sharing and nonrepudiation to secure internet of wireless sensor things. *Cluster Computing*, *26*(2), 945-960.
[40] Li, X., Liu, S., Kumari, S., & Chen, C. M. (2023). PSAP-WSN: a provably secure authentication protocol for 5g-based wireless sensor networks. *CMES—Comput. Model. Eng. Sci*, *135*, 711-732.
[41] Son, S., Kwon, D., Lee, S., Jeon, Y., Das, A. K., & Park, Y. (2023). Design of secure and lightweight authentication scheme for UAV-enabled intelligent transportation systems using blockchain and PUF. *IEEE Access*.
[42] Chandan, R. R., Balobaid, A., Cherukupalli, N. L. S., HL, G., Flammini, F., & Natarajan, R. (2023). Secure modern wireless communication network based on blockchain technology. *Electronics*, *12*(5), 1095.
[43] Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J. G. (2022). Blockchain based secure routing and trust management in wireless sensor networks. *Sensors*, *22*(2), 411.
[44] Chen, Y., Yang, X., Li, T., Ren, Y., & Long, Y. (2022). A blockchain-empowered authentication scheme for worm detection in wireless sensor network. *Digital Communications and Networks*.