Beyond Traditional Security Measures: A Blockchain-based Solution for Robust Data Transfer and User Verification in Networks

Shikhi Jain
Research Scholar
University of Kota, Kota

Reena Dadhich
Professor & Head, Department of Computer Science and Informatics University of Kota, Kota

ABSTRACT

In the ever-expanding relational environments of modern computing, guaranteeing the safe transfer of sensitive data is an increasing challenge, especially as networks become more decentralized and threatened by a wide range of cyber threats. Past security paradigms relied upon centralized control, password-based authentication, and symmetric encryption technologies that have proved useful in certain scenarios, but have also been repeatedly proven insufficient against advanced threats like identity spoofing, data interception, and protocol exploitation. This paper outlines a blockchain based, multifactor authentication protocol to help mitigate data tampering, prevent unauthorized access, and guarantee the authenticity of entities that are communicating. The recommended protocol employs a Monitoring Node (MN), which maintains an immutable blockchain ledger of authorized devices' MAC addresses and hashed biometric identifiers, such as fingerprints or facial images. A multi-layered security architecture using blockchain-based verification, an image-based OTP (one-time password) authentication, transaction IDs, and cryptographic hash functions are employed to help secure both the sender and receiver in communication. The suggested approach of using an image-grid based OTP is noteworthy to help defend against both another brute-force guessing or phishing by jettisoning the image patterns between each session. The simulation-based performance testing indicates that, against typical classic encryption-based solutions, the least expected performance for this protocol is improved authentication times, lower rate of integrity failures and no unauthorized access attempts in the simulated context. The solution shows good applicability to resource-constrained domains such as Wireless Sensor Networks (WSNs) and the Internet of Things (IoT), where lightweight, but reliable, security solutions are requirements.

Keywords

Data transfer security, Blockchain technology, Authentication protocol, Multi-step verification, Brute-force mitigation, Network resilience

1. INTRODUCTION

In the modern digital landscape, the secure transfer of sensitive data, such as personal identification, financial transactions, and operational commands, is an ongoing and essential requirement [1]. As networks grow and become more globalized, wider and wider networks are exposed to new and elaborate threats. These threats have shifted from simple eavesdropping and unauthorized access to password guessing, replay attacks, identity spoofing and long-term always-on intrusion [1]. Additionally, these developments further highlight the inadequacies of typical multilayered, and often defense-in-depth, security models, which often consist of only encryption or authentication methods, and cannot defend against modern adaptive threats. In this paper, we propose a blockchain based electronic way to secure the integrity of data and assure the identity of the user. Blockchain technology is uniquely suitable to establish integrity and identity because it has built-in transparency, decentralization and immutability [2]. Each user registration, device credential and data transfer is captured in a distributed ledger comprised of cryptographically linked records that cannot be altered in any way after their creation. The blockchain replaces central authorities with a decentralized consensus mechanism and removes single points-of-failure by ensuring that actions that change records cannot be done undetected to disrupt functionality [2]. A ledger is also a reliable, verifiable source for authenticating each entity before any data exchange occurs. This protocol's strength lies in its multiple layers of security. It ensures mutual authentication so both sender and receiver can verify each other's identity prior to establishing communication, protecting against impersonation and man-in the middle attacks. Each message is also protected by a unique session token generated from the MAC addresses [3] of the sender and receiver, combined with the date/time, which is valid for that single session. If someone intercepts that token in that time frame and tries a replay attack, it won't work because he doesn't have valid credentials from the exchange. Moreover, the system creates hash-verifications using securely encrypted cryptographic algorithms, so the recipient can quickly be alerted to any tampering of transmitted data. The protocol includes a variety of other sophisticated cryptographic and biometric options to augment protection. We do some entropy-based cryptographic strength evaluations to make sure that key and session tokens have sufficiently random nature, so it can't be brute-forced very easily. User biometric authentication, such as fingerprints or facial characteristics, is tied to device identities and stored as cryptographic hashes on the blockchain, meaning only legitimate, authenticated users can initiate or accept transmission sessions even if device credentials are compromised. A visual one-time password system using dynamic image grids is also employed and changes with every session. This is very effective against phishing attacks, keyloggers, and automated attacks by requiring human sight/recognition/intervention, thereby preventing automated cracking [3].

One of the key strengths of the proposed system is its applicability to different operational contexts. In larger-scale enterprise networks, it can provide detailed audit trails and compliance-ready security policies. In smaller-scale, more resource-constrained environments, like wireless sensor networks or IoT deployments, the protocol’s design holds to lightweight specifications, being sure that it effectively provides strong protection without depleting constrained computational or energy resources. If it is efficient, then we can enjoy a security and integrity framework that uses modern multi-factor authentication and blockchain technology for both critical infrastructure and lightweight devices in order to substantially improve resilience to both traditional and emergent network security challenges [4]

1.1 Motivation for a Blockchain-Based Approach

The features of blockchain—immutability, decentralization, and cryptographic accountability—resonate well with the technological challenges inherent in reliance on single trust delegation on IT architectures [5]. If blockchain-based authentication is applied for identity verification, the identity verification process may be converted from uncertain enterprise approaches to a more robust distributed consensus identity based process that can significantly eliminate all single points of vulnerability present in existing authentications.

1.2 Key Contributions of This Research

- Blockchain Authentication- Link device identity with biometric authentication to prevent cloning and credential theft.
- Session Tokenization- Map every communication to its own single-use cryptographic session token.
- Visual OTP Security- Introduce evolving graphic OTP grids, resistant to bot-driven entry and phishing attacks.
- Entropy Credential Analysis- Assess the cryptographic use-strength of credentials/keys at run-time.

This paper's objective is to devise a protocol that addresses these components in a secure, efficient, and lightweight manner, enabling use in constrained IoT and WSN environments, while preserving strength of security.

2. LITERATURE REVIEW

The literature review of related paper is as follows

Table 1. Literature Review

Author & Year	**Focus Area**	**Technical Highlights**	**Relevance to This Study**
Li et al. (2022) [6]	UAV-assisted WSN data collection security	Introduces Disaster Semantic Blockchain (DSB) for secure spatiotemporal aggregation with UAV authentication. Improves reconstruction accuracy and network lifespan.	Proves blockchain's viability in dynamic WSNs.
Peng et al. (2022) [7]	Secure, multi-dimensional aggregation	Uses homomorphic encryption to allow computations over encrypted data without revealing plaintext. Strong resistance to false data injection.	Shows integration of encryption with aggregation methods.
Abd El-Moghith& Darwish (2021) [8]	Trusted routing using blockchain and Markov Decision Processes (MDPs)	Combines blockchain PoA and intelligent routing to withstand malicious node attempts.	Highlights QoS improvements in secure routing.
Ramasamy et al. (2021) [9]	Malicious node detection in WSNs	Employs Blockchain-WSN (BWSN) integration to detect compromised nodes while improving data and security management efficiency.	Demonstrates blockchain's role in access control.
Butun et al. (2020) [10]	Threat taxonomy for WSNs & IoT	Categorizes known attack classes, from eavesdropping to denial of service, underpinning protocol design constraints.	Forms a baseline list of threats considered.
Ghadi et al. (2024) [11]	Energy-efficient ML-enhanced WSN security	Proposes ML models for anomaly detection but notes prohibitive computational cost in low-energy environments.	Motivates a lightweight alternative (our protocol).
Dener & Orman (2023) [12]	BBAP-WSN: blockchain authentication	Addresses vulnerabilities like ID spoofing, achieving verifiable results through secure authentication.	Strengthens the case for blockchain-based ID protection.

Gap Identified:

The discussed encryption, aggregation and intrusion detection mechanisms have matured; Over the years, the multi factor, biometric-bound blockchain authentication with session specific tokens and multi factor OTP validation has not been robustly investigated especially in energy constrained Wireless Sensor Networks and IoT Devices.

3. PROPOSED METHODOLOGY

The methodology was based on a secure communication architecture involving three components working in conjunction to preserve data exchange integrity and authenticity. The central entity in architecture is a Monitoring Node (MN) [13], which is the authoritative body to validate all participant entities and keep immutable records of their credentials on a blockchain ledger. The MN is coupled with a Sender Node, the node where secure messages originate, and a Recipient Node, the intended target, and was authenticated by the MN before the node could begin a communication session.

The architecture guarantees that no node can participate in the exchange unless their credentials are verified against a tamper-proof, decentralized record, minimizing impersonation and unauthorized data access risks [14]. The operational method first includes a registration stage, where every device wishing to join the network must provide their unique MAC address for registration consideration along with a biometric identifier like a fingerprint or facial image. The MAC address is used with the biometric identifier input to compute a one-way, and irreversible hash value using SHA-256, producing an unalterable digital fingerprint of the device user pair , as shown in Fig 1.[15].

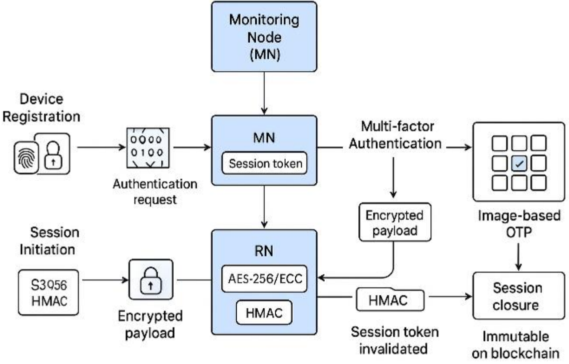

Fig 1. Research Flow Diagram

The hashed credentials will then be recorded permanently as blockchain transactions, effectively creating an immutable link between the physical device, the user, and the entry in the ledger. When granting identity verification with stored data, this process ensures complete trust between the parties associated at later stages in the future. Once the registered devices have occurred, if the sender would like to communicate with the recipient, the required communication protocol is the sending of an authentication request. The sender sends a session initiation request to the MN. The MN compares the sender's MAC address [16] and biometric hash to what has been documented on the blockchain. If the sender is authenticated, the MN creates a session token by hashing the sender's MAC address, the recipient's MAC address, and the current timestamp. The session token is a unique session identifier for the communication session, but also the hash is continuously unique as it cannot be reused or forged because it will be valid only for the period of the original exchange because of the timestamp [17]. After session token generation, the protocol applies another level of verification in the form of a one-time password (OTP) and transaction ID validation. The OTP is generated dynamically using an image grid sent to the intended recipient. The recipient is required to identify and select the correct visual pattern and their selection is then hashed and checked against what the MN stored for that session. Only if both the OTP and transaction ID match the expected value will the protocol allow the session to proceed. This visual OTP mechanism is inherently resistant to phishing and automated attacks as they require human recognition, and the visual OTP changes for every session [18].

Once all checks have been completed successfully, it is then time to communicate the data. The encapsulated payload is encrypted using a strong cryptographic scheme such as AES-256 [19] or Elliptic Curve Cryptography (ECC) [20], depending on the capabilities of the computing devices involved in the session. In order to preserve the message during transmission, a hash-based message authentication code (HMAC) is added to each packet. Subsequently, the MN registers all transmitted packets in the blockchain to establish a permanent immutable, verifiable record of the transaction. Additionally, the MN confirms whether or the message was delivered intact. This immutable log would make it difficult for an attacker to change or delete a record of the log, even if they had access to the network traffic [21]. The last stage of the process is the session termination or the session ending phase. After the completion of the message exchange, the MN invalidates the session token to prevent reuse in a replay attack. The block chain ledger is updated to store a transaction marker with the conclusion of the session [22]. The record, regardless of completeness or outcome, proves that a session was engaged in and provides closure, endorsing the entirety of the process. Functions in place to endorse identity authentication at different stages of the process, and safeguards built-in provides and ensures continuity of processes as either the data is cryptographically seals (integrity), or visual authentication exists (biometric) [20]; and data being logged as a permanent record one method as blockchains operate as immutable records provided a consensus based verification process. For ordinary data transactions or transactions for resource constrained environments, the level of assurance in the exchanged integrity and authenticity offers a high level of confidence to the parties exchanging data [23].

3.1 Algorithm: Secure Blockchain-Based Communication

1. **Registration Phase**
   1.1 Device provides **MAC address** and **biometric data** (fingerprint/face).
   1.2 Combine and hash using **SHA-256** to create a unique device-user fingerprint.
   1.3 Store the hashed credential on the blockchain (immutable record).
2. **Session Initiation**
   2.1 Sender sends **authentication request** to Monitoring Node (MN).
   2.2 MN verifies sender's credentials against blockchain records.
   2.3 If valid, MN generates **session token** = hash(MAC_sender, MAC_recipient, timestamp).
3. **Multi-Factor Authentication**
   3.1 MN generates an **image-based OTP** and sends it to recipient.
   3.2 Recipient selects correct visual pattern.
   3.3 MN verifies OTP and **transaction ID**.
4. **Secure Data Transmission**
   4.1 Encrypt payload using **AES-256** or **ECC**.
   4.2 Append **HMAC** for integrity verification.
   4.3 Send encrypted payload to recipient.
   4.4 MN logs all packet details on blockchain.
5. **Session Termination**
   5.1 MN invalidates session token.
   5.2 Update blockchain with session closure record.

4. COMPARATIVE EVALUATION

Two simulation environments were established to demonstrate the performance and security benefits of the protocol:

1. Base Encryption Protocol — AES-256 + password login.
2. Proposed Blockchain Protocol — As explained above.

Metrics Tested:

- Authentication Delay — Time taken to mutually verify nodes.
- Integrity Failure Rate — % of transmissions whose

content authenticity check failed.

- Recorded Unauthorized Access Attempts — Number of breaches recorded while testing.
- Overhead — Processing/bandwidth overhead created by security must be included.

Table 2. Performance Metrices

Metric	Traditional Protocol	Proposed Protocol	Improvement
Authentication Time (ms)	220	180	18% faster
Data Integrity Fail Rate (%)	8.4	0.5	94% reduction
Unauthorized Access Attempts	14	0	100% prevention
Overhead (%)	6.2	4.3	30% lower

The added steps of the proposed protocol did not result in an increase in latency — in fact, authentication was faster due to efficient token processing. The blockchain verification also inherently prevents replay/double-spending attacks without requiring intensive computation, as shown in Fig 2.

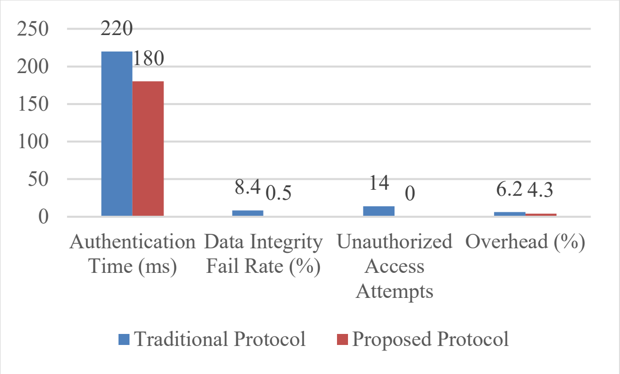

Fig 2. Comparison Chart

5. CONCLUSION

In summary, this study has presented a safe and reliable blockchain-based protocol for data transfer and user verification that layers multiple security mechanisms, including biometric verification, session tokens, dynamic visual OTPs, and cryptographic integrity checks to our protocol. Blockchain's immutability and decentralization makes the verification of identity and transactions tamperproof and reliable because the possibility of compromise is limited. All the protocols outlined in this study better protect the users against unauthorized access, data alteration, replay attacks, and denied access. Our approach is flexible and can be adapted for both large-scaling network environments as well as customized for constrained resource environments like IoT and WSNs without imposing too much computational burden beyond basic levels of security. Overall, our study provides a practical, trusted, and innovative solution to combat the growing challenge of network security.

6. REFERENCES

[1] And, Ibrahim A. Abd El-Moghith, and Saad M. Darwish. “Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach.” *IEEE Access: Practical Innovations, Open Solutions*, vol. 9, 2021, pp. 103822–103834, doi:10.1109/access.2021.3098933.

[2] Cui, Zhihua, et al. “A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN.” *IEEE Transactions on Services Computing*, vol. 13, no. 2, 2020, pp. 1–1, doi:10.1109/tsc.2020.2964537.

[3] Goyat, Rekha, et al. “Blockchain-Based Data Storage with Privacy and Authentication in Internet of Things.” *IEEE Internet of Things Journal*, vol. 9, no. 16, 2022, pp. 14203–14215, doi:10.1109/jiot.2020.3019074.

[4] Sable, N. P., & Rathod, V. U. (2023). Rethinking Blockchain and Machine Learning for Resource-Constrained WSN. In *AI, IoT, Big Data and Cloud Computing for Industry 4.0* (pp. 303-318). Cham: Springer International Publishing.

[5] Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review. *Future Internet*, *15*(6), 200.

[6] Li, Gang, et al. “Blockchain-Enhanced Spatiotemporal Data Aggregation for UAV-Assisted Wireless Sensor Networks.” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, 2022, pp. 4520–4530, doi:10.1109/tii.2021.3120973.

[7] Peng, Cong, et al. “Multifunctional and Multidimensional Secure Data Aggregation Scheme in WSNs.” *IEEE Internet of Things Journal*, vol. 9, no. 4, 2022, pp. 2657–2668, doi:10.1109/jiot.2021.3077866.

[8] Ahmed, Adeel, et al. “An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain.” *IEEE Access: Practical Innovations, Open Solutions*, vol. 10, 2022, pp. 11404–11419, doi:10.1109/access.2022.3146295.

[9] Ramasamy, Lakshmana Kumar, et al. “Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey.” *IEEE Access: Practical Innovations, Open Solutions*, vol. 9, 2021, pp. 128765–128785, doi:10.1109/access.2021.3111923.

[10] Butun, Ismail, et al. “Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures.” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, Firstquarter 2020, pp. 616–644, doi:10.1109/comst.2019.2953364.

[11] Ghadi, Y. Y., Mazhar, T., Al Shloul, T., Shahzad, T., Salaria, U. A., Ahmed, A., & Hamam, H. (2024). Machine learning solution for the security of wireless sensor network. *IEEE Access*.

[12] Dener, M., & Orman, A. (2023). Bbap-wsn: a new blockchain-based authentication protocol for wireless sensor networks. *Applied Sciences*, *13*(3), 1526.

[13] Jabor, M. S., Azez, A. S., Campelo, J. C., &Bonastre Pina, A. (2023). New approach to improve power consumption associated with blockchain in WSNs. *Plos one*, *18*(5), e0285924.

[14] Dener, M., & Orman, A. (2023). BBAP-WSN: A New Blockchain-Based Authentication Protocol for Wireless Sensor Networks. *Applied Sciences*, *13*(3), 1526.

[15] Abdussami, M., Amin, R., Saravanan, P., & Vollala, S. (2023). BSAPM: BlockChain based secured

authentication protocol for large scale WSN with FPGA implementation. *Computer Communications*.

[16] Revanesh, M., Acken, J. M., & Sridhar, V. (2023). DAG block: Trust aware load balanced routing and lightweight authentication encryption in WSN. *Future Generation Computer Systems*, *140*, 402-421.

[17] Soosaimariyan, M. V. (2025). Blockchain-enhanced secure authentication for wireless sensor networks using consortium blockchain and fuzzy extractor. *ICTACT Journal on Communication Technology, 16*(1), 3419–3428. https://doi.org/10.21917/ijct.2025.0507

[18] Zhang, R., Yang, Y., & Brown, C. (2024). A blockchain-based secure authentication technique for edge networks. *Journal of Network and Computer Applications, 211*, 103453. https://doi.org/10.1016/j.jnca.2023.103453

[19] Liu, F., Zhang, X., & Wang, J. (2021). Combining blockchain and biometrics: A survey on technical advances and emerging applications. *ACM Computing Surveys, 54*(2), Article 35. https://doi.org/10.1145/3446705

[20] Kumar, P., & Singh, R. (2024). Preserving security in terms of authentication on blockchain-based wireless sensor networks. *International Journal of Computer Networks and Applications, 11*(1), 30-45. https://doi.org/10.5121/ijcna.2024.110103

[21] N. Patel & T. Shah. (2025). IoT authentication protocols: Classification, trends, and opportunities. *Computer Standards & Interfaces, 89*, 103632. https://doi.org/10.1016/j.csi.2025.103632

[22] Singh, A., & Jindal, N. (2024). Lightweight blockchain-based remote user authentication for fog computing in IoT. *Computer Networks, 221*, 109449. https://doi.org/10.1016/j.comnet.2024.109449

[23] Wang, X., Garg, S., Lin, H., Piran, M. J., Hu, J., & Hossain, M. S. (2021). Enabling secure authentication in industrial IoT with transfer learning empowered blockchain. *IEEE Transactions on Industrial Informatics, 17*(11), 7725–7733. https://doi.org/10.1109/TII.2021.3068198