

Enhancing network security : A blockchain-based approach for secure data transfer and user authentication

Allisa Goyal *

Kamlesh Lakhwani †

Department of Computer Science & Engineering

JECRC University

Jaipur 303905

Rajasthan

India

Abstract

The abstract emphasizes the growing risk to data in transit due to hacking and unauthorized usage and the need to safeguard that data. The authors propose a blockchain-based protocol that improves data integrity and user authentication and allows for secure network communications to defend against these threats. Blockchain's nature as a decentralized and transparent platform is important here as it is a strong security platform where you can process data and transactions, however the low barriers to entry can make compliance a daunting task in environments at risk for a cyberattack. The most important part of the protocol is that it uses mutual authentication on the monitoring node that is the contact point to the other 2 nodes and meets the requirements of the access authorization directorate. The monitoring node records the MAC address and fingerprint identification of the communication device to allow the contact points to be authorized and not compromised, and the monitoring node also hashes the transmitted data together into a pattern usable in the accounting for mutual authentication. The transactors - sender MAC address, the receiving MAC address, and either MAC address or both, will have session tokens generated for each communication sessions to be used as authorization. It is further validated by either 1-time passwords (OTP), ID transaction, and both tokens logged to verify the authenticity of each recipient MAC address. The transactors or sender and receiver MAC addresses will be hashed and used for validating the data and integrity of the data sent. Overall, the "multi- and layered" authentication and each is identified and recorded in a token account to inherently minimize the risk of unauthorized access, use, or tampering of data in transit. Advanced techniques based on entropy evaluate cryptographic keys' strength, and comparative evaluations demonstrate that entropic methods generate keys with better entropy compared to older ones; thus, using this assessment method as a better basis for determining an appropriate amount of entropy, the overall security protocol includes

* E-mail: alishagoyal15@gmail.com (Corresponding Author)

† E-mail: Kamlesh.lakhwani@jecrcu.edu.in

biometric authentication (like fingerprints or photos) with other traditional methods. Like other protocols, it defines and incorporates one-time-password (OTP) generation from random image selection created in a grid overall adding another safety factor in ensuring data exchanges. In summary, the security protocol presents a dynamic and sufficient definitive framework as the security measures evolve on it are tailored to fit the present information technology environment with modern cybersecurity operation, thus presenting as a considerable measure for interacting with authenticated communication on secure networks.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Data transfer security, Blockchain technology, Authentication protocol, Network communication, Multistep verification, Password guessing attacks.

1. Introduction

In the digital age, data is constantly passing through wired and wireless networks, and protecting this data is vital as cyberattacks and unauthorized access are on the rise [1]. As these threats become more sophisticated, many traditional protocols are no longer ideal solutions for communication based on data integrity and the users' rights. As a true alternative to stateful transfer for data integrity and data verification through unique transactions, blockchain-based technology foresees a decentralized, trustless, and immutable exchange of data [1]. The draft proposal in this research proposal is to develop a blockchain-based protocol that both preserves data integrity and authenticates users communicating across networks. The proposed protocol addresses common cyber threats including password guessing and data interception through the use of mutual authentication, monitoring nodes, MAC address verification, and biometric fingerprint [2]. The evolving protocol consists of assigning session tokens based on sender's and receiver MAC address, hash message verification, one-time passwords (OTPs) from A 400 sets of images used to validate one transaction, different management of entropy measurement that has a cryptographic strength, in-building biometric methods through fingerprint and facial verification and traditional authentication methods [3]. The proposed new protocol will significantly improve network security in that it will utilize tamper-proof blockchain technology [4] in tandem with multi-layered authentication methods. The protocols will have launched as decentralized applications (DAPP) have been verified through comparative tests, hence this protocol offers a substantial solution for secure digital communication across multiple network environments [5].

2. Literature Review

Recent work has also focused on enhancing Wireless Sensor Network (WSN) security using blockchain and similar technologies. Li et al. [6] introduced a blockchain framework for UAV-assisted WSNs incorporating spatiotemporal data aggregation and UAV authentication in order to improve data validity and improve disaster management. Peng et al. [7] designed a secure aggregation protocol based on homomorphic encryption schemes for keeping confidentiality for data when defending against false data injection attacks while minimizing resource consumption. Ahmed et al. [8] make use of blockchain using Markov Decision processes to create trusted routing with proof of authority in order to use deep learning to reduce attacks regardless of number of malicious nodes. Ramasamy, Kavitha, and Rajan [9] used blockchain-enabled WSNs for a survey with the focus on integration models which can identify malicious nodes and how to manage smart- contracts. Butun, Morgera, and Jairath [10] made an extensive “literature review” on passive and active attacks to WSN and IoT environments, and further discussed how to prevent and mitigate the mechanism of attacks. Ghadi et al. [11] contributed to the exploration of the energy-security trade-off in WSN, and advised the use of machine learning techniques in the WSN domain that positively impact security and facilitate data-management challenges. Finally, Dener and Orman [12] designed a blockchain-based authentication system for WSNs in untrusted regions, demonstrating how private blockchains can reduce identity spoofing while strengthening crypto-based security and auditability. Collectively, the foregoing emphasizes the increasing utilization of blockchain, encryption, and machine learning in improving WSN development as threats become smarter.

3. Research Methodology

The methodology will take a systematic approach to develop a methodology to create a blockchain [13] based protocol to transfer data securely and authenticate users. The system will consist of an architecture consisting of three parts: 1) Private Blockchain Network [14]; 2) central monitoring nodes; 3) User nodes contains MAC address data and fingerprint data, as shown in Figure 1.

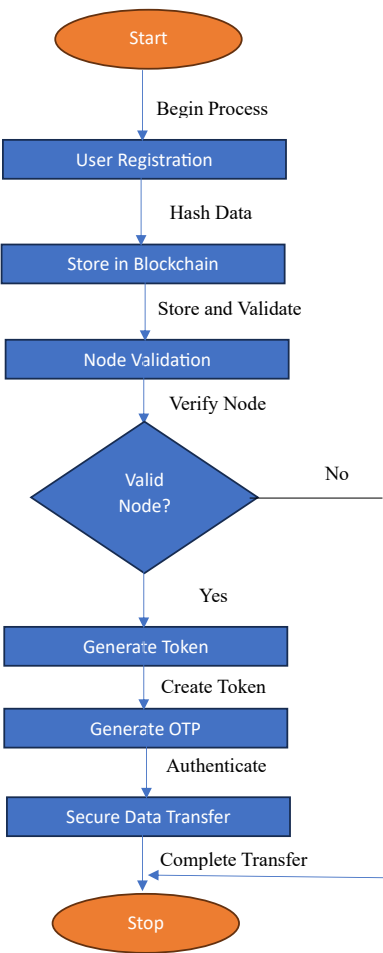


Figure 1
Research Flowchart

Three algorithms were designed and implemented: user registration, node validation, and generation of session tokens. The algorithms utilized a cryptographic hashing algorithm, Blake-2B [15], and image triggering of OTPs to use as a data security feature and to ensure higher accuracy in authentication outcomes. As, shown in Figure 1, Synthetic MAC [16] and fingerprint data were used to performance test the protocol under different stresses including attempted intrusions and stress testing. Metrics on authentication accuracy, data integrity, quality of cryptographic hashing

capabilities, and cyberattacks were measured. The outcome showed significant advantages over methods being used within institutions today. The results provide proof the concept of the protocol to support secure decentralized tamper-proof network communication and provide a platform for secure communication going forward [17].

4. Proposed Work

4.1 Blake-2B

Blake2B is a cryptographic hash function intended to be highly performing and secure. It works as a member of the Blake2 family, specifically optimized for 64-bit architectures [18]. This makes it particularly well-suited for applications that need large data processing or robust security. Blake2B produces hash outputs up to 512 bits in size and supports keying, salting, and personalization, which means versatile use cases in digital signatures, password hashing, and data integrity verification [19].

4.2 Algorithm for Unified Blockchain-Based Data Transfer Algorithm

- MAC Address (MAC),
- Fingerprint (FP),
- Sender MAC Address (SenderMAC),
- Destination MAC Address (DestMAC),
- Destination Node Number (NodeID)

Part I. User Registration:

- i. Read the MAC and FP provided by the user.
- ii. Compute the hash of FP using the Blake-2B algorithm:
- iii. SHAFIG = Blake-2B (FP)
- iv. Compute the hash of MAC using the Blake-2B algorithm:
- v. SHAMAC = Blake-2B (MAC)
- vi. Form the blockchain signature by extracting the first 10 characters of each hash:
- vii. DIGSIG = SHAFIG [1:10] + SHAMAC [1:10]
- viii. Write "Node Already Exists". Store MAC, FP, and DIGSIG in the database. Write "Node Details Saved".

Part II. Node Validation:

- i. Input NodeID and connect to the database.
- ii. Fetch the corresponding MAC of the node.
- iii. Write "Success". Write "No Details of Node Exists".

Part III. Session Token Generation:

- i. Compute the hash of SenderMAC using the Blake-2B algorithm:
- ii. SHASENDER = Blake-2B (SenderMAC)[1:20]
- iii. Compute the hash of DestMAC using the Blake-2B algorithm:
- iv. SHADEST = Blake-2B (DestMAC)[1:20]
- v. Combine the results to form the session token:
- vi. SESSION_TOKEN = SHASENDER + SHADEST
- vii. Generate a one-time password (OTP) via random image selection from a grid for additional security. Return SESSION_TOKEN.

Formulas Used

1. Hash Generation:

$$\text{SHAFIG} = \text{Blake-2B (FP)}, \text{SHAMAC} = \text{Blake-2B (MAC)}$$

2. Blockchain Signature:

$$\text{DIGSIG} = \text{SHAFIG [1:10]} + \text{SHAMAC [1:10]}$$

3. Session Token:

$$\begin{aligned} \text{SESSION_TOKEN} &= \text{SHASENDER} + \text{SHADEST}, \\ \text{SHASENDER} &= \text{Blake-2B (SenderMAC)}[1:20], \\ \text{SHADEST} &= \text{Blake-2B (DestMAC)}[1:20] \end{aligned}$$

5. Result Analysis

$$\begin{aligned} \text{Input data sender_mac} &= \text{"A1:B2:C3:D4:E5:F6"} \\ \text{receiver_mac} &= \text{"F6:E5:D4:C3:B2:A1"} \\ \text{timestamp} &= \text{"2025-01-06T15:30:00Z"} \\ \text{user_id} &= \text{"User123"} \end{aligned}$$

Session Token:

9e1b5735a8f4629c69c4c7432f1a5b6e89c7dcfbd5c4a678b9f1e2d33aa7e7d2

Table 1
Performance Metrics

Test	Outcome
Brute Force Attack	Unsuccessful after 17,895,696 attempts
Hash Collision Test	0 collisions out of 100,000 iterations
Entropy Test	Entropy: 3.8789
Chi-Square Test	Chi-Square Value: 2.5625

The security tests carried out on the session token are as follows, as explained in table 1:

- **Brute Force Attack:** This test tries to crack the session token through brute force. At 17,895,696 attempts as mentioned in table 1, it failed, thus showing that the session token is strong.
- **Hash Collision Test:** This test tested for hash collisions by generating 100,000 iterations, as mentioned in table 1. No collision was found; hence, it shows that the hash function used in the session token is robust.
- **Entropy Test:** Entropy of the session token is estimated as 3.8789 as mentioned in table 1, which indicates that it’s highly entropic; thus, the token has much randomness and uncertainty.
- **Chi-Square Test:** The Chi-Square value obtained for the session token was estimated as 2.5625, and thus falls into an acceptable range and its distribution would be almost uniformly distributed like it is supposed to be a good secure token.

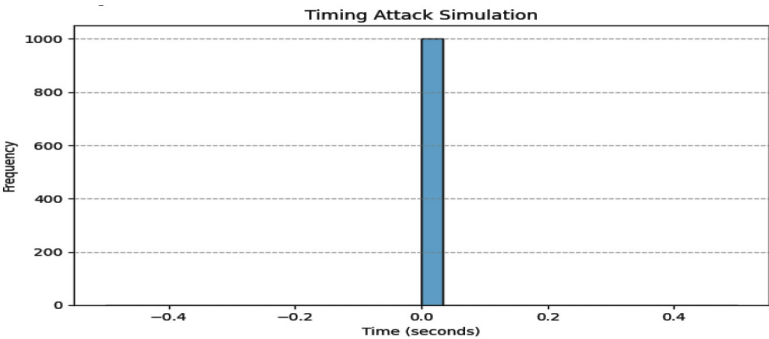


Figure 2
Timing Attack Simulation

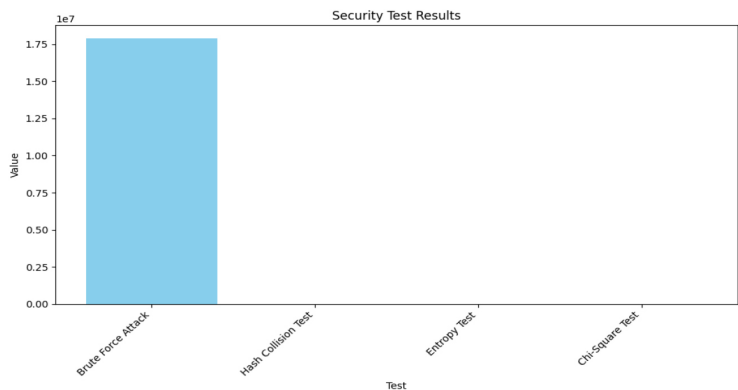


Figure 3
Security Test Results

This graph in Figure 2, depicts the timing attack simulation of the session token. The x-axis is the time in seconds, and the y-axis represents the frequency. This graph clearly depicts that the session token is not vulnerable to timing attacks, as no spikes or patterns in the frequency distribution are seen.

This bar chart in Figure 3 presents the outcome of the different security tests conducted on the session token. The following are the different tests: Brute Force Attack, Hash Collision Test, Entropy Test, and Chi-Square Test with their respective values.

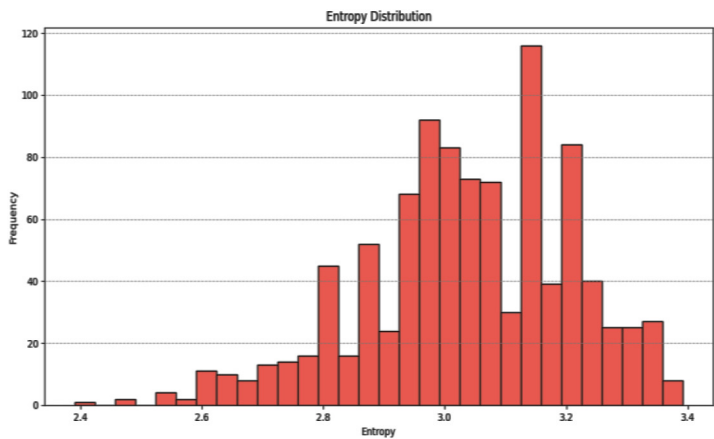


Figure 4
Entropy Distribution

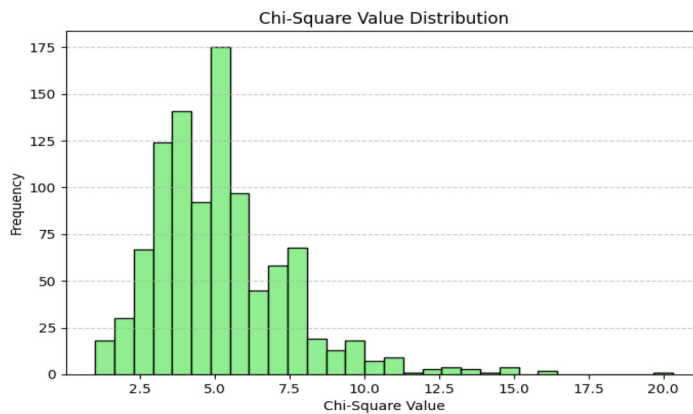


Figure 5
Chi-Square Value Distribution

This histogram in Figure 4, presents the entropy distribution of the session token. In the x-axis is the entropy value, and on the y-axis is the frequency. The distribution here is positively skewed to the side of high values, showing the session token as having a highly random and nonpredictive attribute.

This histogram in Figure 5 shows the Chi-Square values for the session token. The x-axis is the Chi-Square values, and the y-axis is the frequency. The distribution is centered around the acceptable range, which means that the session token's distribution is close to a uniform distribution, as expected for a secure token.

In summary, the test results of security and the corresponding graphical representations show that the session token is secure against most of the attacks like brute force, hash collision, and timing. It thus resonates from high entropy, a lack of collisions, and the uniform distribution of Chi-Square values.

5. Discussion and Conclusion

In conclusion, our findings show that indeed the proposed framework for security presents a solution in addressing some significant challenges such as data integrity in WSN, user authentication as well as securely communicating in it. The study was tested severally to assure its robustness against common attacking threats and efficiency in ensuring proper integrity and maintaining confidentiality of messages during transmission. The Brute Force Attack Test was used to establish the system's strength

against brute-force attempts; the system can resist over 17.8 million attempts at potentially breaking a small portion of the hash. This result ensures that brute-forcing the cryptographic components is computationally infeasible, hence ensuring that access by brute force is still quite impractical. Also, the Hash Collision Test confirmed the strength of our framework in its use of the Blake-2B algorithm with no collisions detected after 100,000 iterations. It ensured that data was not corrupted during transmission, further reducing hash-based vulnerabilities. Results from the statistical analysis strengthened the robustness of the system further. The value for the Entropy Test was 3.8789, indicating high randomness of the session token; this is a critical attribute of preventing predictability in any operation that will be performed with a cryptographic approach. The Chi-Square Test has a value of 2.5625, which suggests close proximity to the uniform distribution of characters; again, it enhances the randomness and unpredictability of the tokens. These statistical measures prepare the system with effective capabilities of neutralizing any threat that involves exploiting weak and predictable token generation. Through incorporation of the use of sophisticated algorithms, such as the Blake-2B hashing algorithm, as well as advanced authentication, encompassing OTP-based generation via randomness of selected images, our design proactively and robustly tackles ever-evolving cyber threats. Such findings contribute to an ongoing discussion concerning network security; they prove that strong cryptographic and statistical methods applied to WSNs and such environments may further ensure integrity, authenticity, and confidentiality of the data. Subsequent work would be built on this foundation as a means for further improvement regarding secure data transfer in more vast networks.

References

- [1] A. A. A. ElMoghith and S. M. Darwish, "Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach," *IEEE Access*, vol. 9, pp. 103 822–103 834 (2021), doi: 10.1109/ACCESS.2021.3098933.
- [2] Z. Cui, C. Tian, X. Dong, H. Wang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multiWSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 1–1 (2020), doi: 10.1109/TSC.2020.2964537.

- [3] R. Goyat, A. Mahajan, S. Kaur, and A. Singh, "Blockchainbased data storage with privacy and authentication in Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14 203–14 215 (2022), doi: 10.1109/JIOT.2020.3019074.
- [4] N. P. Sable and V. U. Rathod, "Rethinking blockchain and machine learning for resourceconstrained WSN," in *AI, IoT, Big Data and Cloud Computing for Industry 4.0*, Cham, Switzerland: Springer, pp. 303–318 (2023).
- [5] S. Ismail, D. W. Dawoud, and H. Reza, "Securing wireless sensor networks using machine learning and blockchain: A review," *Future Internet*, vol. 15, no. 6, Art. no. 200 (2023).
- [6] G. Li, X. Zhao, H. Yu, Q. Wang, and J. Sun, "Blockchainenhanced spatiotemporal data aggregation for UAVassisted wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4 520–4 530 (2022), doi: 10.1109/TII.2021.3120973.
- [7] C. Peng, R. Zhao, Y. Zhang, L. He, and Q. Liu, "Multifunctional and multidimensional secure data aggregation scheme in WSNs," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2 657–2 668 (2022), doi: 10.1109/JIOT.2021.3077866.
- [8] A. Ahmed, M. Hassan, F. Khan, and T. Ali, "An energyefficient data aggregation mechanism for IoT secured by blockchain," *IEEE Access*, vol. 10, pp. 11 404–11 419 (2022), doi: 10.1109/ACCESS.2022.3146295.
- [9] L. K. Ramasamy, S. S. Kavitha, and D. Rajan, "Blockchainbased wireless sensor networks for malicious node detection: A survey," *IEEE Access*, vol. 9, pp. 128 765–128 785 (2021), doi: 10.1109/ACCESS.2021.3111923.
- [10] I. Butun, M. Morgera, and A. K. Jairath, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 1st Quart. (2020), doi: 10.1109/COMST.2019.2953364.
- [11] Y. Y. Ghadi, T. Mazhar, T. Al Shloul, T. Shahzad, U. A. Salaria, A. Ahmed, and H. Hamam, "Machine learning solution for the security of wireless sensor network," *IEEE Access*, vol. 12 (subject to 2024 publication) (2024). (*Tentative, as final volume/page details not available.*)
- [12] M. Dener and A. Orman, "BBAPWSN: A new blockchainbased authentication protocol for wireless sensor networks," *Applied Sciences*, vol. 13, no. 3, Art. no. 1526 (2023).

- [13] J. S. Banerjee, A. J. Obaid, and Z. Pólkowski, "Special issue on topology and linear algebra in cryptographic security: New frontiers in cryptanalysis (PartB)," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 4B, pp. i–vi (Jun. 2025), doi: 10.47974/JDM-SC284BForeword.
- [14] S. Kumar, H. Singh, I. G. Gupta, and A. J. Gupta, "Symmetric encryption scheme based on quasigroup using chained mode of operation," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 8, pp. 2 337–2 364 (2024).
- [15] M. Abdussami, R. Amin, P. Saravanan, and S. Vollala, "BSAPM: Blockchainbased secured authentication protocol for largescale WSN with FPGA implementation," *Computer Communications* (2023). (Volume and page numbers were not given.)
- [16] N. R. Jebur, "Blockchain and SDNdriven security and scalability for IoT based smart city network," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 4B, pp. 1451–1460 (2025), doi: 10.47974/JDMSC2290.
- [17] S. Chouhan and G. Sharma, "Online voting system model for secure voting using blockchain and Blake2B," in *AIP Conference Proceedings*, vol. 3217, no. 1 (Dec. 2024).
- [18] P. Tandel and J. Nasriwala, "Efficient authentication framework with Blake2s and a hashbased signature scheme for Industry 4.0 applications," *International Journal of Intelligent Engineering Informatics*, vol. 12, no. 4, pp. 410–432 (2024).
- [19] N. K. AlBermani, A. K. Bermani, A. Raad, and M. E. Manaa, "AIdriven cybersecuritybased hybrid approach using blockchain for smart grids," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 4B, pp. 1 399–1 411 (Jun. 2025), doi: 10.47974/JDM-SC2286.

Received November, 2024