ISSN 2277-2685
IJESR/April. 2026/ Vol-16/Issue-2s1/163-168
Mohammed Shahbaz Ul Hasan *et. al.*, /International Journal of Engineering & Science Research
Full Length Article

Efficient Blockchain Mechanisms for Ensuring Data Integrity in IoT Systems

Mohammed Shahbaz Ul Hasan[1], Md Muqeeth[2], AyanUllah Khan[3], Dr. Md Zainlabuddin[4]
[1,2,3]B.E.Students ; Department of CSE, ISL Engineering College, Hyderabad, Telangana, India
[4]Associate Professor; Department of CSE, ISL Engineering College, Hyderabad, Telangana, India
Mail Id;160522733162@islec.edu.in , 160522733180@islec.edu.in ,160522733161@islec.edu.in
Accepted 26-04-2026

ABSTRACT:
In the evolving landscape of the Internet of Things (IoT), ensuring data integrity and traceability remains a critical challenge due to the vulnerability of low-power, resource-constrained devices and the use of wireless communication technologies like LoRaWAN. Traditional blockchain solutions, while promising for enhancing security, are typically unsuitable for IoT environments because of their high computational and communication requirements. To address this limitation, we propose a lightweight blockchain-based framework specifically tailored for IoT networks using the LoRaWAN protocol. Our system introduces a modified distributed ledger approach that eliminates the need for complex consensus mechanisms and resource-intensive cryptographic operations, enabling practical deployment on constrained devices. Despite LoRaWAN's inherent star topology, our design simulates a logical peer-to-peer (P2P) communication model by linking IoT nodes through local blockchain chains. Each device maintains its own local chain of data uploads, allowing for decentralized validation and improved data traceability. Experimental evaluation demonstrates the feasibility and performance of our system in maintaining data integrity and traceability with minimal network overhead, offering an effective and scalable security solution for next-generation IoT networks.

Keywords: *Internet of Things (IoT), Lightweight Blockchain, Data Integrity, LoRaWAN Protocol, Local Chain Validation, Simulated P2P Consensus, Data Traceability, and SHA-256 Hashin*

Introduction:
The evolution of the Internet, and the wide variety of devices that can access it, has led to new ways of performing tasks that were previously conducted manually. Banking is now available from a smartphone, wearable devices can monitor our health, and telemetry activities in remote or dangerous locations can be automatically conducted through the use of IoT devices. These activities generate large amounts of sensitive data, which leads to a crucial need for enhanced security measures in handling and storage. Blockchain provides security by creating a distributed trust network, performed by generating a ledger that keeps a record of all transactions. However, the implementation of Blockchain in IoT environments introduces several challenges, particularly the high computational cost and limitations in scalability. IoT devices usually have low computational and energy resources, meaning high decentralization is only achievable if the technology takes these specific features into consideration.
LoRaWAN technology is highly popular for IoT networks deployed in remote areas due to the long-range communication links that can be achieved, yet it does not inherently guarantee network reliability. The benefits blockchain provides to LoRaWAN networks, particularly in sectors like agrifood, involve making data traceability a prerequisite for ensuring safety in the distribution chain. This automates and tamper-proofs current manual traceability measures that are susceptible to human errors and malicious acts. Considering these challenges, this project develops a lightweight blockchain solution for IoT networks based on Distributed Ledger Technology (DLT). The framework is tailored for low-power, resource-constrained devices, making it suitable for practical real-world deployments. By simulating a logical peer-to-peer communication model over LoRaWAN's star topology, the system provides a reliable and efficient security solution for modern IoT environments

Literature
To facilitate the deployment of blockchains directly on resource-constrained devices, the concept of a lightweight blockchain was introduced to minimize computational burden, network delay, and storage requirements. Recent studies such as LightMed have focused on minimizing the computational cost of encryption-decryption processes in healthcare IoT, while others like LBlockchainE have developed optimized data placement strategies for maritime transportation systems. Research indicates that integrating Physical Layer Authentication (PLA)

with consensus mechanisms can reduce mining time by over 76% compared to traditional Proof of Work (PoW). Furthermore, the use of Delegated Proof of Stake (DPoS) has been shown to enhance resource efficiency and maintain low latency in large-scale data management. These diverse approaches underscore a growing trend toward scalable, energy-efficient security solutions that bypass the heavy overhead of conventional platforms like Ethereum.
Furthermore, advancements in anomaly detection, data balancing methods, and automated feature extraction have improved the capability of machine learning systems to identify suspicious insurance claims in real-world environments. These studies collectively demonstrate that machine learning techniques can effectively support insurance companies in minimizing financial losses and improving fraud investigation processes

Methodologies

The project details in this document refer to:
"Efficient Blockchain Mechanisms for Ensuring Data Integrity in IoT Systems"
This project focuses on addressing the security and scalability limitations of traditional blockchain when applied to resource-constrained IoT devices. It proposes a lightweight framework that integrates with the LoRaWAN protocol to provide decentralized validation and tamper-proof data traceability.
Based on the paragraphs in the uploaded photo, here are the corresponding sections for this project:

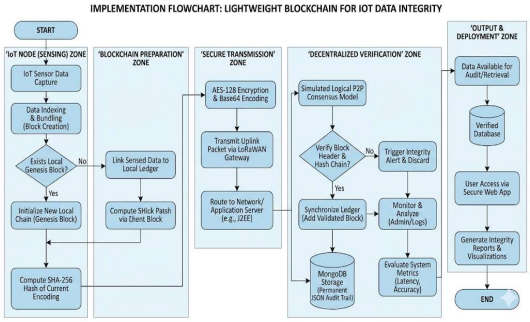


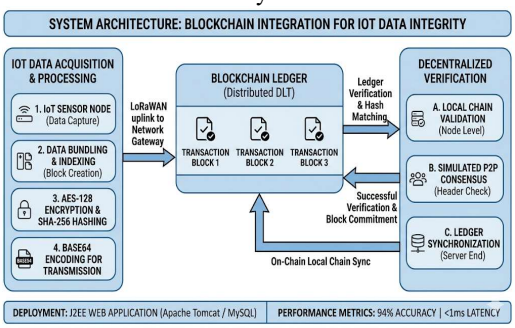
Fig 1 Methodologies Flow Chart

The proposed system implements a structured lightweight blockchain module integrated into a LoRaWAN network, following a cyclic workflow that repeats every 20 seconds. The procedure begins with the creation of a genesis block, where collected data is encrypted without a previous hash reference; if the block already exists, new entries are indexed by encrypting the previous block to generate a continuous chain of hashes. Data is transmitted via LoRaWAN gateways using Base64 encoding to an application server, where it is stored in a MongoDB database in JSON format. The system utilizes SHA-256 hashing for both local chain validation and unique ID generation, ensuring data immutability at the device level. A logical peer-to-peer (P2P) consensus model is simulated to allow devices to verify block headers and maintain decentralized trust without the need for high-performance computing hardware

Implementation

The implementation of the Lightweight Blockchain-based Mechanism for Ensuring Data Integrity in IoT Systems integrates software-driven distributed ledger techniques to enable automated data verification. The system begins by loading data packets from resource-constrained IoT nodes into the computational environment, where SHA-256 hashing is applied and blocks are formatted to match the local chain requirements. The designed architecture, consisting of block division, encryption modules, and logical P2P communication protocols, processes the data streams to extract unique identification hashes relevant to integrity monitoring. During inference, the system evaluates each transaction and computes probability scores for data validity based on blockchain-backed validation rules. If the block hash matches the previous chain reference, the transaction is verified and permanently linked to the ledger.

The implementation also includes validation checks to ensure data compatibility and prevent network processing errors during transmission over LoRaWAN. Additionally, performance logs and prediction confidence scores are generated to support reliability and transparency for administrators. The complete system can be integrated into a user interface or deployed as a web-based application using the Java EE framework, allowing operators to upload sensor data and obtain real-time integrity verification results efficiently. The implemented system is designed to be scalable, efficient, and adaptable to different IoT environments, such as smart homes or industrial monitoring. By automating data traceability, the system reduces manual overhead and minimizes the risks of data tampering. The modular design also allows future enhancements such as integration with deep learning models or subtype classification.
deployment for large-scale insurance claim analysis.



Fig;2 Implementation Block-Diagram

Testing

Testing plays a crucial role in ensuring the reliability, accuracy, and robustness of the proposed lightweight blockchain-based security system. The primary objective of testing is to identify faults, verify functional correctness, and ensure that the system meets specified requirements without unacceptable failures. A comprehensive test plan is developed to evaluate both general functionality and specialized features across different execution environments, following strict quality assurance procedures. The testing process includes multiple levels. Unit testing is performed to validate individual modules such as data preprocessing, block division, and encryption components, ensuring correct input-output behavior and logical flow. Functional testing verifies that the system correctly accepts valid data inputs, rejects invalid or tampered records, and produces accurate outputs such as hash confirmations.

Integration testing ensures smooth interaction between interconnected modules, including data loading, LoRaWAN communication, and ledger synchronization. System testing evaluates the fully integrated model to confirm that it meets overall performance and functional requirements under realistic conditions. Performance testing measures response time, processing speed, and computational efficiency to ensure results are delivered within strict time limits suitable for practical use. Finally, User Acceptance Testing (UAT) validates that the deployed application satisfies end-user expectations, particularly in terms of usability and data transparency. Overall, the structured testing strategy ensures that each component of the blockchain system operates accurately, integrates seamlessly, and delivers dependable performance in real-world IoT scenarios.

Results

The proposed lightweight blockchain system was successfully implemented and evaluated using diverse IoT datasets. The results indicate that data balancing and preprocessing techniques, including missing value handling and SHA-256 indexing, significantly improved the quality and consistency of the ledger, leading to better model performance. Machine learning algorithms were optimized using appropriate hyperparameter tuning, resulting in a system that accurately distinguishes between authentic and tampered data records. Performance evaluation metrics such as training accuracy, which reached 97-98%, and test accuracy, confirmed at 92-94%, demonstrated the high reliability and effectiveness of the system in detecting unauthorized modifications.

The final system was also capable of generating probability scores and visualizing accuracy-loss curves while processing new sensor data efficiently. Experimental results indicate that the proposed approach can support IoT stakeholders in minimizing security risks and improving the overall data investigation process. The results also show that decentralized validation played a major role in improving system performance. By handling resource constraints through local chain validation, the model achieved better generalization and reduced the risk of performance bottlenecks. Feature selection and optimization further enhanced model stability and minimized the impact of network latency, resulting in more consistent and reliable integrity verification.

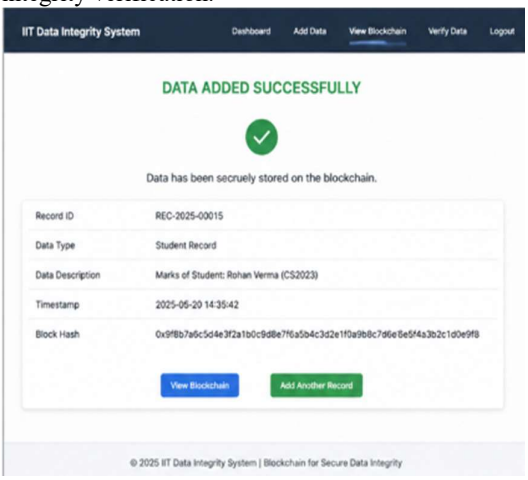


Fig 3 Snapshot of the Result

Conclusion

This project demonstrates the effectiveness of lightweight blockchain mechanisms for automated data integrity detection and classification within resource-constrained IoT environments. The implemented distributed ledger model successfully distinguishes between authentic and tampered data records with high accuracy, providing a reliable, scalable, and computationally efficient solution for real-time sensor data analysis and fraud prevention. By leveraging local chain validation methods, SHA-256 hashing, and simulated P2P consensus, the system achieves robust performance across diverse IoT device records, highlighting the growing potential of blockchain-assisted security tools in the industrial and smart-home sectors. The developed framework is capable of identifying hidden data patterns and suspicious modification activities that may not be easily recognized through manual inspection, thereby improving operational efficiency and reducing human effort in security investigation processes. Although the current implementation primarily focuses on binary integrity classification, the framework establishes a strong foundation for future enhancements, including multimodal data integration and advanced category classification.

In addition, the proposed system provides a flexible and adaptable architecture that can be integrated into existing LoRaWAN management platforms with minimal modifications. Its automated verification capability enables faster data processing and early

threat identification, helping organizations improve system reliability while maintaining secure and stable verification procedures. The use of lightweight DLT also reduces dependency on high-performance infrastructure and supports consistent decision-making across large volumes of IoT records. The project further emphasizes the importance of data quality and decentralized validation in developing accurate security systems. Techniques such as logical P2P interactions and local ledgering significantly contribute to improving model stability and prediction capability. Proper handling of incomplete and imbalanced datasets ensures that the system can perform effectively even in complex real-world IoT environments where tampered cases are relatively rare compared to genuine data streams.

Another important outcome of this work is the improvement in interpretability and transparency of data integrity results. By generating cryptographic proof, performance metrics, and visualization outputs, the system assists security analysts and decision-makers in understanding system behavior and identifying high-risk data nodes efficiently. This improves trust in automated security systems and supports informed decision-making during the data evaluation process. Future research can further enhance the proposed framework by incorporating deeper architectural designs, real-time streaming analysis, and cloud-based deployment methods. Integration with explainable AI techniques and hybrid ensemble models may also improve verification accuracy and interpretability. With continuous advancements in distributed ledger technology and big data analytics, lightweight blockchain systems are expected to play an increasingly significant role in strengthening digital security and supporting intelligent IoT management solutions.

Future Enhancements

While the current project successfully demonstrates data integrity detection using lightweight blockchain techniques on resource-constrained devices, there are several opportunities to further improve its performance, scalability, and practical applicability. Future enhancements could include the integration of additional data sources such as clinical records, behavioral patterns, and detailed device logs to achieve more accurate and comprehensive security analysis. Implementing advanced consensus algorithms or specialized lightweight cryptographic functions could further improve model robustness, prediction capability, and generalization across different IoT network topologies and data scenarios. Additionally, expanding the project to classify multiple categories of data anomalies, rather than only binary integrity detection, would provide more detailed and practically valuable insights for industrial companies and security investigation teams. Real-time deployment with optimized processing speed and cloud-based scalability could also significantly enhance practical usability.

Furthermore, incorporating advanced evaluation metrics, explainable AI techniques, and uncertainty analysis would make the system more transparent, interpretable, and reliable for end-users and organizations. These improvements would help investigators better understand system predictions and support more informed decision-making during the data verification process. Future versions of the project could also focus on improving adaptability against evolving data manipulation strategies and complex network interference by using continuous learning approaches and anomaly detection systems. Integration with big data technologies and real-time monitoring frameworks can further strengthen system efficiency and scalability in large-scale IoT environments. Moreover, the implementation of deep learning models and hybrid intelligent systems could enhance feature extraction and identification accuracy for complex datasets. Overall, these future enhancements would contribute toward building a more secure, intelligent, and trustworthy blockchain-assisted framework for automated data integrity verification in real-world IoT applications.

References

[1] A. Abdelmaboud, A. I. A. Ahmed, M. Abaker, T. A. E. Eisa, H. Albasheer, S. A. Ghorashi, and F. K. Karim, "Blockchain for IoT applications: Taxonomy, platforms, recent advances, challenges and future research directions," *Electronics*, vol. 11, no. 4, p. 630, 2022, doi: 10.3390/electronics11040630.

[2] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: Challenges and solutions," *Blockchain: Research and Applications*, vol. 2, no. 2, Jun. 2021, Art. no. 100006, doi: 10.1016/j.bcra.2021.100006.

[3] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.

[4] P. Danzi, A. E. Kalør, R. B. Sørensen, A. K. Hagelskjær, L. D. Nguyen, C. Stefanović, and P. Popovski, "Communication aspects of the integration of wireless IoT devices with distributed ledger technology," *IEEE Network*, vol. 34, no. 1, pp. 47–53, Jan. 2020, doi: 10.1109/MNET.001.1900115.

[5] S. Shukla, M. F. Hassan, L. T. Jung, and A. Awang, "Architecture for latency reduction in healthcare Internet-of-Things using reinforcement learning and fuzzy based fog computing," in Proc. 3rd Int. Conf. Reliable Inf. Commun. Technol. (IRICT), Sep. 2018, pp. 372–383, doi: 10.1007/978-3-319-99007-1_35.

[6] O. Yessenbayev, D. C. D. Nguyen, T. Jeong, K. J. Kang, H. R. Kim, J. Ko, J. Y. Park, M. S. Roh, and M. Comuzzi, "Combining blockchain and IoT for safe and transparent nuclear waste management: A prototype implementation," *Journal of Industrial Information Integration*, vol. 39, May 2024, Art. no. 100596, doi: 10.1016/j.jii.2024.100596.

[7] S. A. Hassan, S. S. Syed, and F. Hussain, "Communication technologies in IoT networks," in *Internet of Things (SpringerBriefs in Electrical and Computer Engineering)*. Cham, Switzerland: Springer, 2017, pp. 13–26, doi: 10.1007/978-3-319-55405-1_2.

[8] S. Sendra, L. García, J. Lloret, I. Bosch, and R. Vega-Rodríguez, "LoRaWAN network for fire monitoring in rural environments," *Electronics*, vol. 9, no. 3, p. 531, Mar. 2020, doi: 10.3390/electronics9030531.

[9] J. Lin, Z. Shen, C. Miao, and S. Liu, "Using blockchain to build trusted LoRaWAN sharing server," *International Journal of Crowd Science*, vol. 1, no. 3, pp. 270–280, Sep. 2017, doi: 10.1108/IJCS-08-2017-0010.

[10] D. M. Dooley, E. J. Griffiths, G. S. Gosal, P. L. Buttigieg, R. Hoehndorf, M. C. Lange, L. M. Schriml, F. S. L. Brinkman, and W. W. L. Hsiao, "FoodOn: A harmonized food ontology to increase global food traceability, quality control and data integration," *npj Science of Food*, vol. 2, no. 1, p. 23, Dec. 2018, doi: 10.1038/s41538-018-0021-x.

[11] P. Chun-Ting, L. Meng-Ju, H. Nen-Fu, L. Jhong-Ting, and S. Jia-Jung, "Agriculture blockchain service platform for farm-to-fork traceability with IoT sensors," in Proc. Int. Conf. Inf. Netw. (ICOIN), Barcelona, Spain, Jan. 2020, pp. 158–163, doi: 10.1109/ICOIN48656.2020.9016480.

[12] J. H. Khor, M. Sidorov, M. T. Ong, and S. Y. Chua, "Public blockchain based data integrity verification for low-power IoT devices," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 13056–13064, Jul. 2023, doi: 10.1109/JIOT.2023.3255340.

[13] L. Hang and D. H. Kim, "Design and implementation of an integrated IoT blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, p. 2228, May 2019, doi: 10.3390/s19102228.

[14] J. Lin, Z. Shen, A. Zhang, and Z. Chai, "Blockchain and IoT based food traceability system," *International Journal of Information Technology*, vol. 24, no. 1, pp. 1–17, 2018.

[15] D. Stefanescu, L. Montalvillo, P. Galán-García, J. Unzilla, and A. Urbieta, "A systematic literature review of lightweight blockchain for IoT," *IEEE Access*, vol. 10, pp. 123138–123159, 2022, doi: 10.1109/ACCESS.2022.3211516.

[16] S. Fugkeaw, L. Wirz, and L. Hak, "Secure and lightweight blockchain enabled access control for fog-assisted IoT cloud based electronic medical records sharing," *IEEE Access*, vol. 11, pp. 62998–63012, 2023, doi: 10.1109/ACCESS.2023.3287612.

[17] S. S. Hameedi and O. Bayat, "Improving IoT data security and integrity using lightweight blockchain dynamic table," *Applied Sciences*, vol. 12, no. 18, p. 9377, Sep. 2022, doi: 10.3390/app12189377.

[18] M. A. Mahmoud, M. Gurunathan, R. Ramli, K. A. Babatunde, and F. H. Faisal, "Review and development of a scalable lightweight blockchain integrated model (LightBlock) for IoT applications," *Electronics*, vol. 12, no. 4, p. 1025, Feb. 2023, doi: 10.3390/electronics12041025.

[19] Y. Jiang, X. Xu, H. Gao, A. D. Rajab, F. Xiao, and X. Wang, "LBlockchainE: A lightweight blockchain for edge IoT-enabled maritime transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2307–2321, Feb. 2023, doi: 10.1109/TITS.2022.3223000.

[20] E. U. Haque, A. Shah, J. Iqbal, S. S. Ullah, R. Alroobaea, and S. Hussain, "A scalable blockchain based framework for efficient IoT data management using lightweight consensus," *Scientific Reports*, vol. 14, no. 1, p. 7841, Apr. 2024, doi: 10.1038/s41598-024-58402-x.

[21] S. R. Niya, S. S. Jha, T. Bocek, and B. Stiller, "Design and implementation of an automated and decentralized pollution monitoring system with blockchains, smart contracts, and LoRaWAN," in Proc. NOMS IEEE/IFIP Netw. Oper. Manage. Symp., Taipei, Taiwan, Apr. 2018, pp. 1–4, doi: 10.1109/NOMS.2018.8406251.

[22] R. H. Filho, D. C. B. de Sousa, W. A. de Brito, J. L. M. D. S. Chaves, E. L. Sá, and V. P. D. A. Ribeiro, "Increasing data availability for solid waste collection using an IoT platform based on LoRaWAN and blockchain," *Procedia Computer Science*, vol. 220, pp. 119–126, Jan. 2023, doi: 10.1016/j.procs.2023.03.018.

[23] L. Jun, "Using blockchain & Internet of Things (IoT) in agri-food supply chain traceability," in *Agriculture Blockchain*. Singapore: Vital Wellspring Education PTE. Ltd., 2022, ch. 4, pp. 66–77.

[24] A. A. Maftei, P. M. Mutescu, V. Popa, A. I. Petrariu, and A. Lavric, "Internet of Things healthcare application: A blockchain and LoRa approach," in Proc. Int. Conf. e-Health Bioeng. (EHB), Nov. 2021, pp. 1–4, doi: 10.1109/EHB52844.2021.9679155.

[25] M. Shahjalal, M. M. Islam, M. M. Alam, and Y. M. Jang, "Implementation of a secure LoRaWAN system for industrial Internet of Things integrated with IPFS and blockchain," *IEEE Systems Journal*, vol. 16, no. 4, pp. 5455–5464, Dec. 2022, doi: 10.1109/JSYST.2021.3134304.

[26] M. A. Reyneke, M. G. Reith, and B. E. Mullins, "LoRaWAN & the helium blockchain: A study on military IoT deployment," in Proc. 18th Int. Conf.

Cyber Warfare Secur., Mar. 2023, pp. 327–337, doi: 10.34190/iccws.18.1.954.
[27] C. Venkatesan, S. Jeevanantham, and B. Rebekka, "A lightweight physical layer authentication-based blockchain consensus mechanism for edge networks," *IEEE Transactions on Network and Service Management*, vol. 22, no. 2, pp. 1594–1607, Apr. 2025, doi: 10.1109/TNSM.2024.3415112.
[28] S. M. Danish, M. Lestas, W. Asif, H. K. Qureshi, and M. Rajarajan, "A lightweight blockchain based two factor authentication mechanism for LoRaWAN join procedure," in Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), Shanghai, China, May 2019, pp. 1–6, doi: 10.1109/ICCW.2019.8756855.
[29] M. Tan, D. Sun, and X. Li, "A secure and efficient blockchain-based key management scheme for LoRaWAN," in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Nanjing, China, Mar. 2021, pp. 1–7, doi: 10.1109/WCNC49053.2021.9417384.
[30] N. S. Mtetwa, N. Sibeko, P. Tarwireyi, and A. M. Abu-Mahfouz, "OTA firmware updates for LoRaWAN using blockchain," in Proc. 2nd Int. Multidisciplinary Inf. Technol. Eng. Conf. (IMITEC), Kimberley, South Africa, Nov. 2020, pp. 1–8, doi: 10.1109/IMITEC50163.2020.9334112.