Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 05 Issue: 06 | June-2025

Enhancing IOT Data Security in Wireless Sensor Networks Using Blockchain Technology

Rajesh Naik.N[1], Charan Tej.P[2], Afroz Basha.A[3], Shiva Kumar.N[4], Ravinder.G[5]

[1]JNTUH, Dept. of CSE, Siddhartha Institute of Technology and Sciences, Hyderabad, Telangana, India
[2]JNTUH, Dept. of CSE, Siddhartha Institute of Technology and Sciences, Hyderabad, Telangana, India
[3]JNTUH, Dept. of CSE, Siddhartha Institute of Technology and Sciences, Hyderabad, Telangana, India
[4]JNTUH, Dept. of CSE, Siddhartha Institute of Technology and Sciences, Hyderabad, Telangana, India
[5]JNTUH1, Asst.Prof, Dept. of CSE, Siddhartha Institute of Technology and Sciences, Hyderabad, Telangana, India

---

Abstract -The rapid growth of Internet of Things (IoT) devices within wireless sensor networks (WSNs) is reshaping various sectors, including smart cities, healthcare, and environmental monitoring. While these advancements bring new opportunities, they also raise serious security concerns—particularly around data integrity, privacy, and access control. Conventional security methods often struggle to keep up due to the decentralized and resource-limited nature of WSNs. This paper investigates how blockchain technology can be used to strengthen the security of IoT data in these networks. By taking advantage of blockchain's core features—decentralization, transparency, and immutability—we introduce a framework that enhances secure data transmission, user authentication, and accountability. Our approach helps protect against common threats like data tampering, spoofing, and unauthorized access. In addition to outlining the technical design, we examine both the benefits and the practical challenges of implementing blockchain in real-world WSN environments. The goal is to assess whether blockchain can offer a scalable and reliable security solution for the evolving IoT landscape. Ultimately, our findings suggest that blockchain holds strong potential to reinforce trust, ensure data protection, and support the safe expansion of IoT applications

Key Words: Wireless sensor networks, Blockchain technology network security, IOT

1.INTRODUCTION

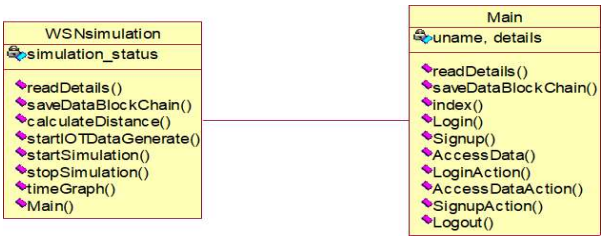
The rapid growth of the Internet of Things (IoT) has brought about a new era of connectivity, allowing everyday devices—from home appliances to industrial sensors—to interact and exchange data seamlessly. At the heart of this ecosystem are Wireless Sensor Networks (WSNs), which collect and transmit real-time data for applications in smart cities, healthcare, agriculture, and environmental monitoring. However, the widespread adoption of IoT also comes with serious security concerns. Due to their distributed and resource-constrained nature, WSNs are particularly vulnerable to cyber threats like data tampering, eavesdropping, spoofing, unauthorized access, and denial-of-service attacks. As these networks increasingly handle sensitive personal information and manage critical infrastructure, ensuring the integrity, authenticity, and privacy of data becomes crucial. Traditional security methods—such as centralized control systems and conventional encryption techniques—often fall short in these environments. They struggle with scalability, are limited by processing power, and introduce single points of failure that can compromise entire networks. In this context, blockchain technology presents a promising solution. Originally designed for secure financial transactions, blockchain offers a decentralized, tamper-proof, and transparent way to store and validate data. By integrating blockchain into WSNs, we can create a secure and trustworthy framework for IoT data sharing without relying on centralized servers. This project proposes a blockchain-based architecture to safeguard IoT data in WSNs, improving resilience against common attacks while enhancing trust among network participants. The proposed solution aims to strengthen the security foundation of IoT systems and support their continued growth in critical real-world applications.

2. Proposed System

To address the security challenges in Wireless Sensor Networks (WSNs), this proposed system leverages blockchain technology to ensure secure and tamper-resistant data handling. Blockchain's decentralized architecture stores data across multiple nodes, where each piece of data is saved as a block linked by unique hash codes. When a new block is added, all nodes verify the previous hash to ensure consistency. If any data is altered at a single node, the hash mismatch is detected across the network, exposing the tampering attempt. In the proposed framework, small sensor nodes are organized into groups, each managed by a Mobile Database Node (MDN). These MDNs collect data from their respective groups, validate it, and then mine new blocks to store the data securely on the blockchain.

Advantages of Proposed System:

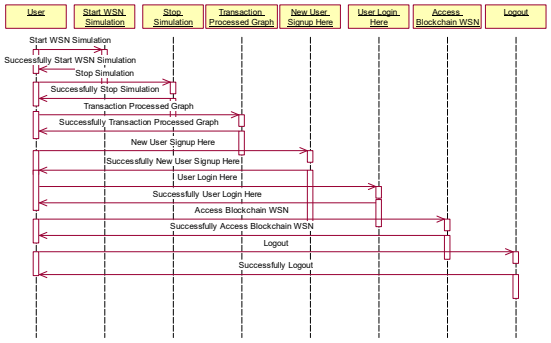
1. Data Integrity
2. Decentralization:
3. Enhanced Security
4. Transparency and Traceability
5. Scalable
6. Smart Contract Automation



2.1 Class Diagram

The given diagram is a UML class diagram that represents the structure of a system designed for simulating Wireless Sensor Networks (WSNs) integrated with blockchain technology and managed through a user interface. It contains two primary classes: WSNsimulation and Main. The WSNsimulation class is responsible for handling the simulation logic and includes methods such as startSimulation(), stopSimulation(), startIOTDataGenerate(), and calculateDistance(), which suggest it manages the behavior of sensor nodes and the generation of IoT data. It also contains a simulation_status attribute to track the current state of the simulation, and methods like saveDataBlockChain() and timeGraph() to save data securely and visualize it.

The Main class, on the other hand, manages user interactions. It contains attributes like uname and details for storing user information, and methods for handling user activities such as Login(), Signup(), Logout(), and corresponding action methods like LoginAction() and SignupAction(). It also allows users to access and interact with the blockchain-secured data using methods like AccessData() and saveDataBlockChain(). There is a relationship between the WSNsimulation and Main classes, indicating that the user interface communicates with the simulation logic, enabling users to initiate simulations and interact with the data generated. This structure supports a secure, user-driven WSN simulation environment with blockchain integration.



2.2 Sequence Diagram

The provided diagram is a sequence diagram that illustrates the step-by-step interaction between a user and the system components during the simulation and access process of a blockchain-enabled Wireless Sensor Network (WSN) application. It outlines the sequence of messages exchanged over time across various modules such as “Start WSN Simulation,” “Stop Simulation,” “Transaction Processed Graph,” “New User Signup,” “User Login,” “Access Blockchain WSN,” and “Logout.”

The process begins with the user initiating the WSN simulation by sending a request to the “Start WSN Simulation” component, which responds by confirming that the simulation has started successfully. Next, the user stops the simulation, receiving a success message in return. The user then requests the transaction-processed graph, which is generated and returned to them. Following this, the user moves to the registration process through the “New User Signup Here” module, successfully signing up and then logging in via the “User Login Here” component. Once authenticated, the user accesses data stored in the blockchain through the “Access Blockchain WSN” module, which confirms successful access. Finally, the user logs out, and the system confirms the successful logout.

Overall, this sequence diagram provides a clear visualization of user interaction with the blockchain-WSN system, covering simulation control, user management, blockchain data access, and session handling, ensuring a smooth and secure workflow.

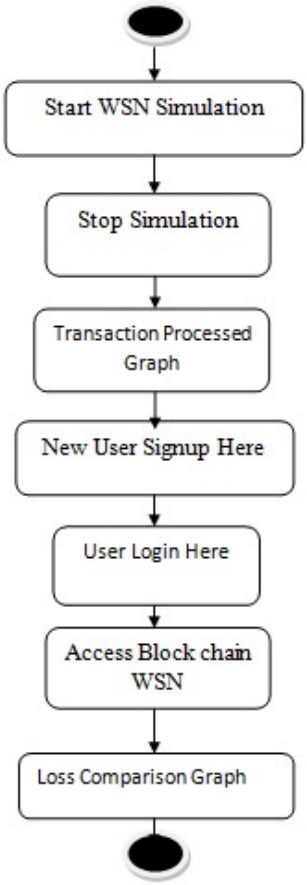
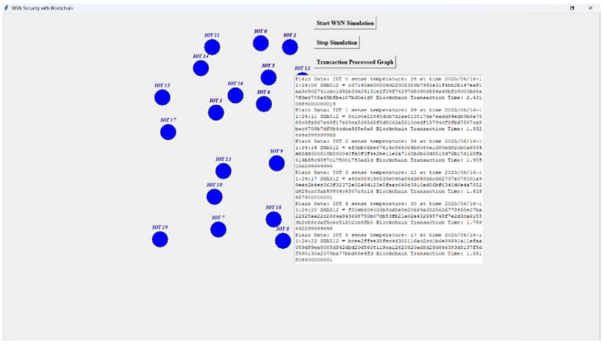


Fig -1: Activity Diagram

Results:



CONCLUSIONS

Integrating blockchain technology into Wireless Sensor Networks (WSNs) offers promising improvements in data security, integrity, and transparency. However, several challenges still need to be addressed for effective implementation. One major concern is data transmission delay. Blockchain operations involve cryptographic processing and verification of previous block sequences before new data can be added, which can slow down real-time data updates and transmission. Another issue is the increased computational load as data volume grows. Hash functions and encryption keys are essential for blockchain security, but with larger datasets, the time required for encryption and verification also increases, reducing overall system efficiency. This is especially problematic in resource-constrained environments like WSNs. To overcome these limitations, our system proposes solutions such as a blockchain resetting mechanism that regularly updates the blockchain to reflect the latest data and reduce processing delays. We also explore simplifying hash calculations and switching from asymmetric to symmetric encryption to reduce computation overhead. Despite these challenges, blockchain remains a strong candidate for securing IoT data. Its decentralized and tamper-proof nature ensures data reliability and traceability. When

applied to WSNs, blockchain can serve as a trusted, time-stamped ledger, similar to its use in financial systems, significantly enhancing the security of sensor data networks.

FUTURE WORKS

The future of enhancing IoT data security in Wireless Sensor Networks (WSNs) using blockchain technology is very promising. As IoT applications continue to expand rapidly in areas like smart cities, healthcare, agriculture, and industrial automation, ensuring data integrity, confidentiality, and trust is more critical than ever. Blockchain offers a decentralized and tamper-proof method for securing data exchanges, allowing transparent and verifiable transactions without relying on centralized authorities. To make blockchain practical for WSNs, future work will focus on developing lightweight consensus algorithms optimized for resource-constrained IoT devices, which can reduce energy consumption and latency. Enhancing interoperability between various blockchain platforms will also be essential for seamless integration across diverse IoT systems. Additionally, integrating blockchain with artificial intelligence (AI) could enable real-time threat detection and automated security responses, further strengthening data protection. Advancements in privacy-preserving techniques and switching to more efficient encryption methods, like symmetric encryption, will help balance security with the limited computational resources of WSN devices. Ultimately, these developments could lead to scalable, standardized, and cost-effective security frameworks that support a wide range of IoT ecosystems, ensuring safer and more reliable wireless sensor networks in the future.

REFERENCES

1] Smith, John. "The Importance of Evidence Integrity in Legal Proceedings." Journal of Legal Studies, vol. 25, no. 3, 2021, pp. 45 62.

[2] Jones, Emily. "Challenges in Traditional Methods of Evidence Management." International Journal of Investigative Sciences, vol. 10, no. 2, 2019, pp. 78–91.

[3] Brown, David. "Vulnerabilities in Conventional Evidence Management Systems." Journal of Digital Security, vol. 15, no. 4, 2020, pp. 102–115.

[4] Lee, Sarah. "Ensuring Security in Evidence Management: A Review of Current Practices." Journal of Legal Technology, vol. 8, no. 1, 2018, pp. 32–47.

[5] White, Michael. "Blockchain Technology in Legal and Financial Domains." International Conference on Blockchain Applications, 2022, pp. 205–218.

[6] Johnson, Robert. "A Review of Blockchain Based Evidence Protection Systems." Journal of Cybersecurity Research, vol. 12, no. 3, 2023, pp. 145–160.

[7] Miller, Samantha. "The Role of Blockchain in Ensuring Evidence Integrity." Proceedings of the International Conference on Digital Forensics, 2019, pp. 75–88.

[8] Ethereum Foundation. "Ethereum: A Platform for Decentralized Applications." [Online]. Available: https://ethereum.org.

[9] Clark, William. "Challenges in Centralized Evidence Management Systems." Journal of Legal Technology, vol. 9, no. 2, 2020, pp. 65–78.

[10] Anderson, Jennifer. "Transparency Issues in Legal Evidence Management." International Journal of Legal Studies, vol. 28, no. 1, 2021, pp. 112–125.