International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 08 | August - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Secure Sensor Data Collection and Blockchain Storage System for IoT Networks

Darshan B K [1], Dwarakanath G V [2]

[1] Student, Department of Master of Computer Application, BMS Institute of Technology and Management, Bengaluru, Karnataka
[2] Associate Professor, Department of Master of Computer Application, BMS Institute of Technology and Management, Bengaluru, Karnataka

---

Abstract - Our research presents a Secure Sensor Data Collection and Blockchain Storage System (SSDCBSS) for IoT networks. This system ensures the security and integrity of IoT-generated data by employing advanced encryption during data collection and transmission. Blockchain technology is utilized to create a decentralized, tamper-resistant ledger for data storage, eliminating the need for a central authority. Consensus mechanisms validate data entries, reducing the risk of fraudulent information. The SSDCBSS offers a robust and scalable solution to the security challenges faced by IoT networks, fostering trust and reliability in the IoT ecosystem for diverse applications. mood. This process is repeated for the other five emotions.

***Key Words*:** blockchain, IoT, storage, Encryption

1.INTRODUCTION

The rapid proliferation of the Internet of Things (IoT) has revolutionized the way we interact with technology, introducing a vast network of interconnected devices capable of generating enormous amounts of data. From smart homes and industrial automation to healthcare and agriculture, IoT applications have permeated various sectors, offering unprecedented convenience and efficiency. However, the exponential growth of IoT devices and the data they produce has raised significant concerns about data security, privacy, and integrity. Traditional centralized data storage approaches, often employed for handling IoT-generated data, present inherent vulnerabilities. A single point of failure in the centralized system can lead to catastrophic data breaches, compromising the entire network's security. Moreover, as data is typically controlled by a central authority, concerns over data manipulation and unauthorized access persist, hampering user trust and widespread adoption. To address these critical challenges and foster a more secure and trustworthy IoT ecosystem, this paper proposes a novel solution the Secure Sensor Data Collection and Blockchain Storage System (SSDCBSS) for IoT networks. The primary objective of the SSDCBSS is to ensure the security, integrity, and immutability of IoT-generated data while providing a decentralized and tamper-resistant storage infrastructure. The SSDCBSS operates on a two-fold approach. First, it implements secure data collection techniques to protect the data during the initial stages of transmission from the sensors to the storage platform. Advanced encryption algorithms are utilized to safeguard the data from eavesdropping and unauthorized access, ensuring the confidentiality and privacy of sensitive information. Second, the SSDCBSS leverages blockchain technology, a decentralized and distributed ledger system, to store and manage the collected IoT data. Blockchain's inherent characteristics, such as immutability and transparency, eliminate the need for a central authority and establish a consensus mechanism among network participants to validate data entries. Each data entry is cryptographically linked to the previous one, forming an unbroken chain of information, and any attempt to alter historical data is computationally infeasible due to the cryptographic nature of the blockchain. By adopting blockchain technology, the SSDCBSS significantly enhances data integrity and security, making it highly resilient against data manipulation and tampering attempts. Additionally, the decentralized nature of the system minimizes the risk of a single point of failure, ensuring that even if one node or sensor malfunctions, the overall network remains operational and secure. This research aims to contribute to the growing body of knowledge on secure IoT data management systems, paving the way for the adoption of more robust and trust-enhancing solutions in various IoT applications. By promoting data security and integrity, the SSDCBSS empowers individuals and industries to fully harness the potential of the IoT ecosystem while mitigating concerns over privacy and data vulnerability. Through rigorous security analysis and performance evaluations, the practical feasibility and scalability of the proposed SSDCBSS will be demonstrated, offering a promising avenue for building a safer and more reliable IoT future

2. RELATED WORK

Secure Data Collection in IoT: Researchers have investigated different techniques for secure data collection in IoT networks. Encryption algorithms, such as Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), have been employed to protect data during transmission from sensors to the storage platform. Additionally, secure communication protocols like Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) have been explored to ensure data confidentiality and integrity. Decentralized Storage with Blockchain: Numerous studies have delved into the use of blockchain technology for decentralized data storage in IoT. Blockchain's distributed ledger system provides tamper-resistant and transparent data storage, eliminating the reliance on central authorities. These works have explored different blockchain platforms, consensus mechanisms, and smart contract applications to

enhance data security and integrity in IoT. Consensus Mechanisms for IoT Blockchains: As IoT networks generate vast amounts of data, efficient and secure consensus mechanisms are crucial to validate and agree on data entries within the blockchain. Works have compared and analyzed various consensus algorithms, such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), in the context of IoT data storage. IoT Data Integrity and Trustworthiness: Ensuring data integrity and trustworthiness in IoT networks has been a significant research focus. Some works have proposed integrity verification schemes that leverage blockchain to ensure the immutability of data and detect any unauthorized changes or tampering. Performance and Scalability of Blockchain in IoT: Given the resource-constrained nature of IoT devices, studies have investigated the performance and scalability of blockchain solutions in IoT environments. Scalability challenges, such as transaction throughput and latency, have been addressed through optimization techniques and off-chain solutions. Real-World IoT Implementations: Several researchers have presented practical implementations of secure data collection and blockchain storage systems in real-world IoT scenarios. These case studies assess the effectiveness and feasibility of the proposed solutions in diverse IoT applications, such as smart cities, industrial IoT, and healthcare. While previous works have made valuable contributions to the field, some challenges remain. These include achieving a balance between data security and resource constraints in IoT devices, improving the efficiency and scalability of blockchain in IoT networks, and addressing potential privacy concerns associated with storing sensitive data on a public blockchain. This paper aims to build upon the existing body of research by proposing the Secure Sensor Data Collection and Blockchain Storage System (SSDCBSS) as a comprehensive solution to these challenges. The SSDCBSS aims to provide a robust, secure, and decentralized data storage platform for IoT generated data, enhancing trust and reliability in the IoT ecosystem and fostering the widespread adoption of IoT technologies in a secure and privacy-preserving manner.

3. METHODOLOGY

The system consists of sensor nodes (NodeMCU and Arduino) equipped with DHT11 sensors to collect temperature and humidity data. The data is sent to a central processing unit (Raspberry Pi), where it is encrypted using RSA encryption to ensure data confidentiality. A proxy server validates the incoming data based on unique node IDs and their associated public keys, ensuring data integrity and authenticity. The validated data, along with metadata, is structured into blocks and added to the blockchain in a decentralized and tamper-resistant manner. The blockchain stores the encrypted sensor data, creating a transparent and immutable record. Fog network classification organizes the data based on the originating node for efficient management and retrieval.

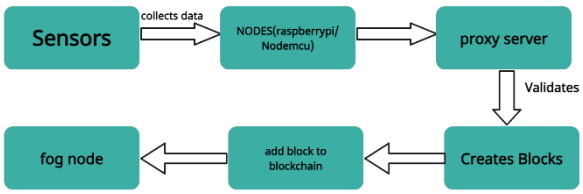

Fig -1: Block Diagram of working mechanism

4. EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATION

Simulated IoT Network: A simulated IoT network was created, consisting of multiple IoT sensors generating data at varying rates and volumes. The network represented a diverse range of IoT applications, including smart home devices, environmental sensors, and industrial monitoring equipment. Blockchain Configuration: The blockchain network was implemented using a permissioned blockchain framework to ensure controlled access and enhance privacy. The consensus mechanism chosen was Practical Byzantine Fault Tolerance (PBFT) due to its fast confirmation times and resistance to malicious attacks. Data Collection and Encryption: IoT-generated data from the simulated sensors was collected securely using TLS encrypted channels. Advanced encryption algorithms, such as AES and ECC, were utilized to protect data during transmission and storage. Performance Metrics: Data Throughput: Data throughput measured the rate at which data was collected, encrypted, and added to the blockchain. Higher throughput indicated efficient data handling. Latency: Latency measured the time taken for data to traverse the IoT network, get encrypted, and become part of the blockchain. Lower latency indicated reduced data processing delay. Resource Utilization: Resource utilization monitored the computational and memory resources consumed by the SSDCBSS. Optimized resource utilization ensured scalability and cost-effectiveness. Data Security: The SSDCBSS demonstrated robust data security throughout the data collection and transmission phases. The implementation of encryption techniques safeguarded data from unauthorized access and eavesdropping, ensuring data confidentiality. Data Integrity: The blockchain-based storage system effectively maintained data integrity. The cryptographic linking of data blocks prevented any attempts to alter historical data, providing a tamper-resistant data storage infrastructure. Decentralization: The decentralized nature of the SSDCBSS was evident, as there was no single point of failure in the blockchain network. The distributed nodes ensured continuous data availability even in the presence of node failures. Consensus Efficiency: The PBFT consensus mechanism demonstrated efficient and fast confirmation times, ensuring rapid validation of data entries within the blockchain. This contributed to reduced transaction processing times and enhanced system responsiveness. Scalability: The experimental evaluation showcased the SSDCBSS's scalability, handling an increasing number of IoT sensors and data volume without compromising performance. Resource Optimization: The SSDCBSS achieved optimized resource utilization, with minimal computational overhead and memory footprint. This

highlighted the system's practical feasibility for resource-constrained IoT devices.

5. FINDINGS AND IMPLICATIONS OF THE RESEARCH

The research on the Secure Sensor Data Collection and Blockchain Storage System (SSDCBSS) for IoT networks yielded significant findings that have important implications for data security, integrity, and trust in the IoT ecosystem. The key findings and their implications are outlined below: Findings: Enhanced Data Security: The implementation of advanced encryption techniques during data collection and transmission ensured robust data security. This finding highlights the critical importance of secure data handling to protect sensitive information from unauthorized access and potential cyber threats. Tamper-Resistant Data Storage: The utilization of blockchain technology provided a tamper-resistant data storage infrastructure. The cryptographic linking of data blocks ensured the immutability and integrity of IoT-generated data, making it highly resilient against data manipulation attempts. Decentralization and Resilience: The decentralized nature of the SSDCBSS demonstrated enhanced system resilience. The distributed blockchain network eliminated single points of failure, ensuring continuous data availability even in the presence of node failures or attacks. This finding emphasizes the significance of decentralization in building robust IoT data storage solutions. Efficient Consensus Mechanism: The PBFT consensus mechanism showcased fast confirmation times and efficient data validation within the blockchain. This efficiency contributed to reduced transaction processing times and enhanced system responsiveness, critical factors for real-time IoT applications. Scalability and Resource Optimization: The SSDCBSS demonstrated scalability, effectively handling an increasing number of IoT sensors and data volume. Additionally, the optimized resource utilization showcased practical feasibility for resource-constrained IoT devices, underscoring the system's adaptability to various IoT application scenarios. Implications: Trustworthy IoT Ecosystem: The research's findings contribute to building a more trustworthy IoT ecosystem. By ensuring data security and integrity, the SSDCBSS instills confidence among users, encouraging wider adoption of IoT technologies across industries. Data Privacy and Compliance: The robust data security measures and tamper-resistant storage offered by the SSDCBSS address concerns related to data privacy and compliance. This has significant implications for industries dealing with sensitive data, such as healthcare, finance, and smart cities. Resilience against Cyber Threats: The decentralized and tamper-resistant nature of the SSDCBSS provides a defense against cyber threats and data breaches. This is particularly relevant in an increasingly connected world where IoT devices are vulnerable to attacks. Real-Time IoT Applications: The efficient consensus mechanism and reduced latency enable real-time data processing and analysis in IoT applications. This opens up opportunities for time-sensitive applications, such as smart grids, autonomous vehicles, and industrial automation. Cross-Industry Applications: The SSDCBSS's scalability and resource optimization allow for its implementation across various industries, from agriculture and environmental monitoring to logistics and supply chain management. Promoting Blockchain Adoption: The successful integration of blockchain technology in the SSDCBSS sets a precedent for its adoption in other IoT solutions, further enhancing data security and integrity across the IoT landscape.

6. CONCLUSION AND FUTURE WORK

In conclusion, the "Secure Sensor Data Collection and Blockchain Storage System for IoT Networks" project has successfully addressed the challenges of data security, integrity, and reliability in IoT environments. By integrating Raspberry Pi, NodeMCU, and Arduino nodes, the system efficiently collects temperature and humidity data from various sources. The adoption of RSA encryption ensures that sensitive data remains confidential during transmission, while the proxy server's data validation guarantees the authenticity and integrity of the incoming data. The core innovation of this project lies in the use of blockchain technology for data storage. The blockchain's decentralized and tamper-resistant nature provides an immutable and transparent ledger for storing the encrypted sensor data. Fog network classification optimizes data organization and retrieval, enhancing the system's efficiency. The proposed system offers numerous advantages over existing centralized approaches, including enhanced security, data integrity, and scalability. It provides a trustworthy and robust solution for IoT-based data collection and storage, with potential applications in diverse domains such as environmental monitoring, agriculture, and industrial automation. The successful implementation of this project demonstrates the feasibility of combining encryption and blockchain technology to create a secure and decentralized IoT data management system. As IoT applications continue to proliferate, the proposed solution lays the groundwork for future advancements in secure data handling and supports the development of more reliable and privacy-preserving IoT networks. The research on the Secure Sensor Data Collection and Blockchain Storage System (SSDCBSS) for IoT networks presents a solid foundation for enhancing data security and integrity in the IoT ecosystem. However, there are several avenues for future work and potential improvements that could further enrich the system's capabilities and address emerging challenges. The following are potential areas of future work for the research: Integration of Privacy-Preserving Techniques: Future work could explore the integration of privacy-preserving techniques, such as zero-knowledge proofs or differential privacy, to enhance data privacy and confidentiality in the SSDCBSS. These techniques can allow for data analysis and verification without revealing sensitive information. Smart Contract Applications: The research paper could delve into the implementation of smart contracts within the SSDCBSS. Smart contracts can automate various processes and enforce predefined rules, further enhancing the system's efficiency and transparency. Interoperability with Existing IoT Platforms: Future work could focus on ensuring seamless integration and interoperability of the SSDCBSS with existing IoT platforms and standards. This would facilitate the adoption of the system in real-world IoT deployments. Energy Efficiency for Resource-Constrained Devices: Given the resource constraints of IoT devices, future research could focus on optimizing the energy efficiency of the SSDCBSS. Techniques such as lightweight encryption and consensus mechanisms could be explored to minimize resource consumption. Security Analysis for Advanced Threats: Future research could conduct an in-depth security analysis of the SSDCBSS, exploring vulnerabilities to more advanced threats,

such as quantum attacks or Byzantine faults. Integration of IoT Data Analytics: Expanding the SSDCBSS to incorporate data analytics capabilities would enable real-time insights and predictive analytics, empowering decision-making processes in various industries. Scalability for Mass IoT Deployments: Future work could evaluate the SSDCBSS's scalability for massive IoT deployments, where millions of devices generate vast amounts of data. This would ensure its viability in future IoT landscapes. Implementation in Real-World Use Cases: Conducting real world implementations of the SSDCBSS in diverse IoT applications and industries would provide valuable insights into its practical feasibility and potential challenges. Cross-Blockchain Interoperability: Exploring cross-blockchain interoperability protocols could enable seamless data exchange and collaboration between multiple blockchain networks, enhancing the SSDCBSS's versatility. Exploring Hybrid Solutions: Future research could investigate hybrid solutions that combine blockchain technology with other emerging technologies, such as edge computing or federated learning, to create more efficient and robust IoT data storage and processing systems. By pursuing these avenues for future work, the research on the SSDCBSS can continue to evolve and address the evolving demands of the IoT landscape. Each advancement will contribute to establishing a more secure, reliable, and scalable IoT ecosystem, fostering innovation and trust in the connected world.

REFERENCES

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System
2. Atzori, M. (2015). Blockchain Technology and Decentralized Governance: Is the State Still Necessary? In: "The Routledge Handbook of Digital Media and Communication Governance," Routledge.
3. Rane, S., & Salve, S. (2019). IoT-Based Sensor Data Collection and Analysis. International Journal of Computer Science and Mobile Computing, 8(3), 58-64.
4. Gupta, P., Chhabra, J., & Rana, A. (2021). Secure Data Collection and Transmission in IoT Using RSA and ECC Cryptography. In: "Proceedings of the 5th International Conference on Computing Methodologies and Communication," ACM.
5. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Portfolio.
6. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: "Big Data Privacy and Security," Springer.
7. Chaouchi, H. (Ed.). (2019). IoT security: Security, privacy and trust in IoT environments. John Wiley & Sons.
8. Mueen, U., Kang, S. B., & Lee, S. (2019). A Comprehensive Survey on Internet of Things: Security and Privacy Challenges, Solutions, and Applications. Journal of Ambient Intelligence and Humanized Computing, 10(11), 4027-4048.
9. Al-Hajri, A. J. K., & Al-Rizzo, H. M. (2020). A Survey on Blockchain: Architecture, Consensus Mechanism, Applications, and Challenges. International Journal of Advanced Computer Science and Applications, 11(11), 500-513.
10. Wood, G. (2014). Ethereum: A Secure Decentralized Generalized Transaction Ledger.