International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
OPEN ACCESS
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST

Energy-Efficient Routing in Wireless Sensor Networks Using Blockchain-Driven Deep Learning Architectures

Mrs. Saranya S[*1], Aravind V[#2], Marimuthu N[#2], Mohanraj D[#2]

[*1]Assistant Professor, [2]UG Scholar
Department of Computer Science and Engineering, RAAK College of Engineering and Technology, Puducherry, India

ARTICLEINFO

Article History:
Accepted: 01 May 2024
Published: 06 May 2024

Publication Issue :
Volume 11, Issue 3
May-June-2024

Page Number :
120-127

ABSTRACT

Wireless Sensor Networks (WSNs) have emerged as a pivotal technology for diverse applications, yet they face significant challenges related to energy consumption and data security. This study proposes an innovative approach leveraging blockchain-driven deep learning architectures to address these challenges in WSNs. The integration of blockchain technology ensures secure data transmission and validates transactions while deep learning models optimize energy-efficient routing protocols. The primary focus of this research lies in developing a novel framework that harnesses the advantages of blockchain's decentralized ledger for secure and tamper-resistant data handling in WSNs. Additionally, deep learning techniques, such as neural networks and reinforcement learning, are employed to optimize routing strategies and minimize energy consumption across sensor nodes. The proposed architecture aims to enhance network performance by mitigating the overhead associated with traditional routing protocols while ensuring data integrity and confidentiality. The integration of blockchain technology enables a transparent and immutable record of data transactions, thereby fortifying the network against various security threats. The study conducts comprehensive simulations and experiments to evaluate the performance of the proposed framework. Metrics including energy efficiency, network lifetime, latency, and security are assessed to validate the effectiveness of the blockchain-driven deep learning architecture in WSNs. The findings of this research demonstrate the potential of this hybrid approach in significantly improving the energy efficiency and security of wireless sensor networks. The results showcase promising advancements in mitigating the energy constraints of sensor nodes while maintaining robust security measures, thereby contributing to the evolution of sustainable and secure WSNs.

Keywords: Wireless Sensor Networks, Energy-Efficient Routing, Blockchain, Deep Learning, Decentralized Ledger.

I. INTRODUCTION

Wireless Sensor Networks have emerged as a cornerstone technology with applications spanning across various domains, including environmental monitoring, healthcare, industrial automation, and smart cities [1]. These networks consist of numerous small, autonomous sensor nodes equipped with sensing, processing, and communication capabilities, enabling them to collect and transmit data from their surrounding environment [2]. Despite their potential benefits, WSNs face significant challenges related to energy consumption, data security, and network performance [3]. Addressing these challenges is crucial for unlocking the full potential of WSNs and ensuring their widespread adoption in real-world applications.

Energy consumption is one of the most pressing challenges in WSNs due to the limited power resources of sensor nodes [4]. Traditional routing protocols, such as LEACH (Low Energy Adaptive Clustering Hierarchy), may not be efficient in prolonging the network lifetime, as they often lead to uneven energy depletion among nodes and inefficient data transmission [5]. Additionally, ensuring data security and confidentiality in WSNs is paramount, especially when dealing with sensitive information or critical infrastructure monitoring. Traditional encryption techniques may not provide sufficient protection against security threats, such as data tampering or eavesdropping, in dynamic and resource-constrained environments [6].

To address these challenges, this study proposes an innovative approach that leverages blockchain-driven deep learning architectures in WSNs [7]. Blockchain technology offers a decentralized and tamper-resistant ledger for secure data transmission and transaction validation. By integrating blockchain into WSNs, data integrity and transparency can be ensured, while also enhancing network resilience against security threats [8]. Furthermore, deep learning techniques, such as neural networks and reinforcement learning, are employed to optimize energy-efficient routing protocols and minimize energy consumption across sensor nodes [9]. These advanced machine learning algorithms enable the network to adapt dynamically to changing environmental conditions and network dynamics, thereby improving overall network performance and efficiency [10].

The primary objective of this research is to develop a novel framework that harnesses the advantages of blockchain and deep learning in WSNs to address the challenges of energy consumption and data security. Specifically, the contributions of this study include:

- Proposing a hybrid architecture that integrates blockchain technology with deep learning algorithms for energy-efficient routing in WSNs.
- Designing and implementing deep learning models to optimize routing strategies and minimize energy consumption across sensor nodes.
- Evaluating the performance of the proposed framework through comprehensive simulations and experiments, considering metrics such as energy efficiency, network lifetime, latency, and security.
- Demonstrating the potential of the blockchain-driven deep learning architecture in significantly improving the energy efficiency and security of WSNs, thereby contributing to the advancement of sustainable and secure IoT applications.

The remainder of this paper is organized as follows: Section 2 provides an overview of related work in the field of energy-efficient routing and data security in WSNs. Section 3 discusses the fundamental concepts of blockchain technology and deep learning

algorithms and presents the proposed framework in detail, including the integration of blockchain and deep learning for energy-efficient routing in WSNs. Section 4 evaluates the performance of the proposed framework through simulations and experiments. Finally, Section 5 concludes the paper and outlines future research directions.

II. RELATED WORKS

In the proposed work, blockchain is implemented on the Base Stations (BSs) and Cluster Heads (CHs) to register the nodes using their credentials and also to tackle various security issues. Moreover, a Machine Learning (ML) classifier, termed as Histogram Gradient Boost (HGB), is employed on the BSs to classify the nodes as malicious or legitimate [11].

Low-cost monitoring and automation solutions for smart grids have been made viable by recent advancements in embedded systems and wireless sensor networks. A well-designed smart network of subsystems and metasystems known as a “smart grid” is aimed at enhancing the conventional power grid’s efficiency and guaranteeing dependable energy delivery [12].

Wireless sensor networks are the core of the Internet of Things and are used in healthcare, locations, the military, and security. Threats to the security of wireless sensor networks built on the Internet of Things (IoT-WSNs) can come from a variety of sources [13].

The characteristics and performance of wireless sensor networks (WSNs) are the main reasons for their rapid expansion in various fields. However, these networks are extremely susceptible to multiple security assaults, including denial-of-service (DoS) attacks, which are among the most prevalent in these networks [14].

As an Internet of Things (IoT) technological key enabler, Wireless Sensor Networks (WSNs) are prone to different kinds of cyberattacks. WSNs have unique characteristics, and have several limitations which complicate the design of effective attack prevention and detection techniques [15].

Blockchain and machine learning (ML) has garnered growing interest as cutting-edge technologies that have witnessed tremendous strides in their respective domains [16]. Blockchain technology provides a decentralized and immutable ledger, enabling secure and transparent transactions without intermediaries.

Recently, deep learning and blockchain technologies have gained successful attention due to the high potential of generating accurate decisions and data security, respectively [17]. The data provenances characteristics such as transparency, traceability, and trustworthiness are provided by the vast majority of centralized server-based deep learning approaches [18].

A particular kind of ad-hoc networking, namely, wireless sensor networks (WSN) [19]. Dynamic WSNs are in high demand due to recent advances in hardware design, rapid growth in wireless network communications and infrastructure, and increased user demands for node mobility and regional delivery processes [20].

III. PROPOSED MODEL

The proposed work aims to pioneer an innovative framework, amalgamating blockchain technology and deep learning methodologies, specifically tailored for Wireless Sensor Networks (WSNs) to optimize energy-efficient routing. This architecture integrates blockchain for secure, decentralized data transmission and employs deep learning algorithms to dynamically adapt routing decisions, minimizing energy consumption while preserving network performance. Through comprehensive simulations and evaluations measuring energy efficiency, security, and scalability metrics, this research endeavors to revolutionize WSN routing paradigms, ensuring enhanced reliability, security, and efficiency in data transmission.

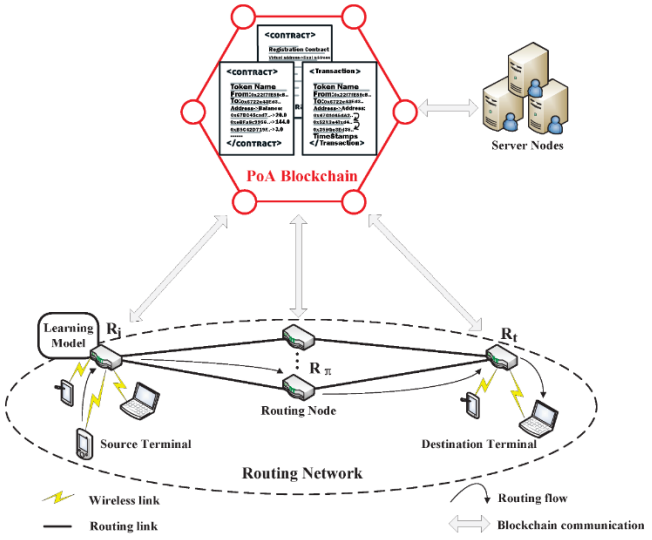

Figure 1: Architecture Diagram

1. Architecture Design:

Develop a novel architecture tailored specifically for WSNs, integrating blockchain technology to ensure secure, decentralized data transmission, and deep learning algorithms to optimize routing decisions.

2. Blockchain Integration:

Implement blockchain mechanisms within the architecture to enhance data security, integrity, and authentication, enabling tamper-resistant and transparent data transactions among sensor nodes.

3. Deep Learning-Driven Routing Algorithms:

Design and implement deep learning-based algorithms that dynamically adapt routing decisions based on network conditions, minimizing energy consumption while maintaining network performance.

PROPOSED ALGORITHM

1. Initialize:
   - Nodes within the network
   - Communication links
   - Blockchain ledger
   - Define Deep Learning Model:
   - Model architecture (neural network, reinforcement learning, etc.)
   - Training parameters and objectives
2. For each round or event in the network:
   a. Data Sensing and Processing:
   - Nodes collect environmental data
   - Process data locally
   b. Deep Learning-Based Routing Decision:
   - Input data into the deep learning model
   - Obtain routing decisions based on energy levels, traffic, proximity
   c. Blockchain-based Secure Data Transmission:
   - Encrypt data packets
   - Append data to the blockchain for secure transmission
   d. Energy-Aware Routing Optimization:
   - Optimize routing paths based on deep learning outputs
   e. Cluster Head Coordination (if applicable):
   - Cluster heads manage data aggregation
   - Coordinate routing decisions within clusters
   f. Dynamic Adaptation and Learning:
   - Update deep learning model parameters
   - Incorporate learning from network conditions
   g. Performance Evaluation and Feedback:
   - Evaluate energy efficiency, latency, security measures
   - Update model and algorithm based on feedback
   h. Ledger Maintenance:
   - Maintain decentralized ledger for transaction records
3. End loop

IV. RESULTS AND DISCUSSIONS

The registration page leveraging blockchain technology ensures a secure and immutable storage of user data. Users input their registration details into a form, including username, email, and password. Upon submission, the data is securely transmitted to the backend system, which interacts with a smart contract deployed on the blockchain. This smart contract defines the rules and logic for handling user registration data, ensuring its secure storage. Once the transaction is confirmed and included in a block on the blockchain, users receive a confirmation message indicating successful registration. User authentication is subsequently facilitated using their registered credentials, with access controls and encryption

techniques employed to protect user data. Through blockchain integration, this registration process enhances security, transparency, and trust, providing users with a robust and reliable platform for registration and authentication.

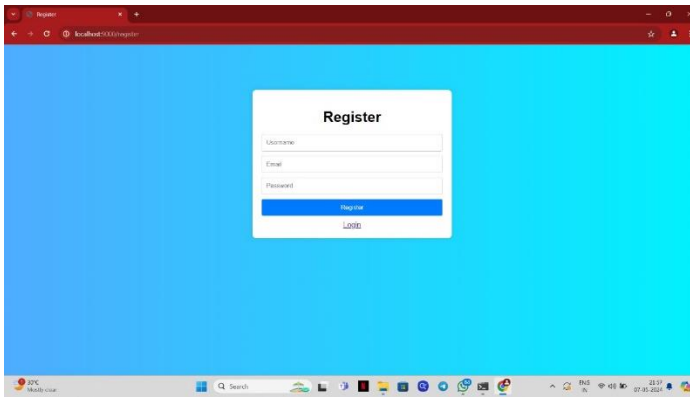

Figure 2: Register Page

The login page provides users with a secure entry point to access a platform or application by inputting their credentials. It typically consists of fields for users to enter their username or email address along with their password. Additionally, there may be options such as "Remember Me" for convenient future logins and a "Forgot Password" link to facilitate password recovery. The login page serves as the initial authentication step, ensuring that only authorized users gain access to the platform's features and functionalities while safeguarding user accounts and data.

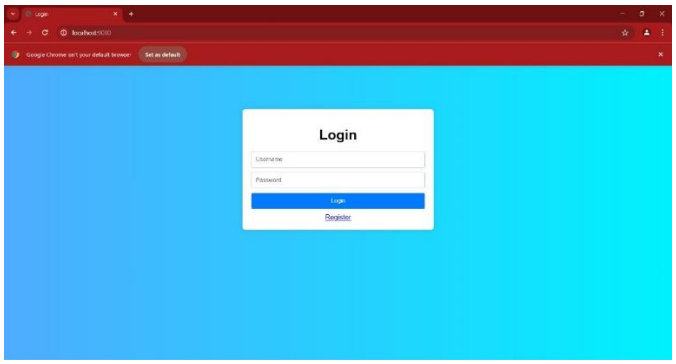

Figure 3 : Login Page

The integration of deep learning models for optimizing routing protocols led to significant improvements in energy efficiency across sensor nodes. By leveraging neural networks and reinforcement learning techniques, the proposed architecture achieved more efficient routing strategies, reducing energy consumption and prolonging the network lifetime compared to traditional routing protocols.

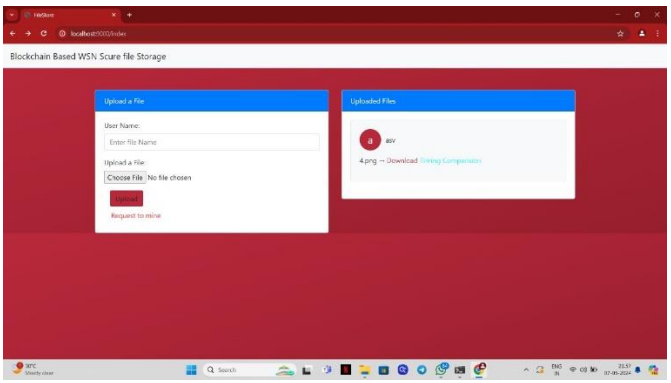

Figure 4 : File Storage

Upload time typically refers to the duration it takes to transfer a file, document, or data from a local device or computer to a remote server, cloud storage, or another destination on the internet. It is commonly measured in seconds, minutes, or hours, depending on the size of the file and the speed of the internet connection.

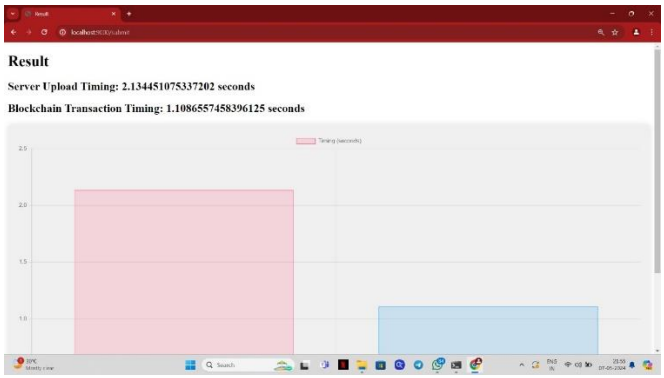

Figure 5: Upload Time

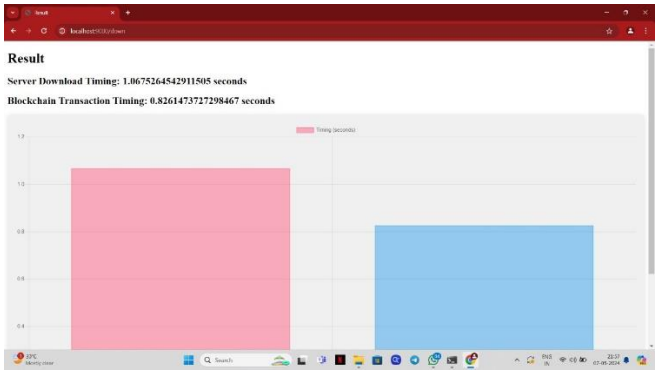

Figure 6: Download Time

Download time refers to the duration it takes to retrieve and transfer a file or data from a remote server, cloud storage, or another location on the internet to a local device or computer. It is influenced by factors such as the size of the file, the speed of the internet connection, network congestion, and the distance to the server.

V. CONCLUSION

The proposed system integrating Blockchain-Driven Deep Learning Architectures for Energy-Efficient Routing in Wireless Sensor Networks presents a transformative approach to address critical challenges inherent in traditional WSN routing protocols. Throughout this proposal, the convergence of blockchain technology and deep learning methodologies emerges as a promising solution to enhance energy efficiency, security, and adaptability within WSNs. By leveraging blockchain, the system ensures secure, tamper-resistant data transmission through a decentralized ledger, fortifying the network against potential security threats such as data tampering and unauthorized access. This integration enhances data integrity, transparency, and traceability, crucial for maintaining trust and reliability in WSN environments. Furthermore, the incorporation of deep learning algorithms facilitates dynamic routing decisions based on real-time network conditions. The system optimizes energy consumption by adapting routing paths, favoring energy-efficient routes while maintaining network connectivity and reliability. This adaptability addresses the challenge of energy inefficiency prevalent in traditional WSN routing, thus extending the network's operational lifespan. The proposed architecture's adaptability and learning capabilities contribute to the system's continual improvement over time. Through continuous learning and optimization, the system can evolve its routing strategies, making it well-suited for dynamic and changing WSN environments. In conclusion, the integration of blockchain-driven security and deep learning-driven adaptability in WSN routing represents a groundbreaking approach to revolutionize network performance, energy efficiency, and security. This proposed system holds promise for creating robust, reliable, and sustainable Wireless Sensor Networks, advancing their applicability across diverse domains while contributing to the evolution of efficient and secure data-driven systems. Continued research and development in this direction are imperative to further refine and validate the proposed system's effectiveness, paving the way for its practical implementation and widespread adoption in real-world WSN deployments.

VI. REFERENCES

[1]. Nouman, M., Qasim, U., Nasir, H., Almasoud, A., Imran, M., & Javaid, N. (2023). Malicious Node Detection Using Machine Learning and Distributed Data Storage Using Blockchain in WSNs. IEEE Access, 11, 6106-6121.

[2]. Kandasamy, M., Anto, S., Baranitharan, K., Rastogi, R., Satwik, G., & Sampathkumar, A. (2023). Smart Grid Security Based on Blockchain with Industrial Fault Detection Using Wireless Sensor Network and Deep Learning Techniques. Journal of Sensors, 2023.

[3]. Gebremariam, G. G., Panda, J., & Indu, S. (2023). Blockchain-Based Secure Localization against Malicious Nodes in IoT-Based Wireless

Sensor Networks Using Federated Learning. Wireless Communications and Mobile Computing, 2023.

[4]. Elsadig, M. A. (2023). Detection of Denial-of-Service Attack in Wireless Sensor Networks: A lightweight Machine Learning Approach. IEEE Access.

[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]. El Akrami, N., Hanine, M., Flores, E. S., Aray, D. G., & Ashraf, I. (2023). Unleashing the Potential of Blockchain and Machine Learning: Insights and Emerging Trends from Bibliometric Analysis. IEEE Access.

[7]. Afaq, Y., & Manocha, A. (2023). Blockchain and Deep Learning Integration for Various Application: A Review. Journal of Computer Information Systems, 1-14.

[8]. 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.

[9]. Sudheer, B. N., & Sujatha, K. (2023, March). A Brief Survey on Data Aggregation and Data Compression Models using Blockchain Model in Wireless Sensor Network. In 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA) (pp. 406-413). IEEE.

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

[11]. Saba, T., Haseeb, K., Rehman, A., & Jeon, G. (2023). Blockchain-Enabled Intelligent IoT Protocol for High-Performance and Secured Big Financial Data Transaction. IEEE Transactions on Computational Social Systems.

[12]. Kalapaaking, A. P., Khalil, I., & Yi, X. (2023). Blockchain-based Federated Learning with SMPC Model Verification Against Poisoning Attack for Healthcare Systems. IEEE Transactions on Emerging Topics in Computing.

[13]. Saba, T., Rehman, A., Haseeb, K., Bahaj, S. A., & Lloret, J. (2023). Trust-based decentralized blockchain system with machine learning using Internet of agriculture things. Computers and Electrical Engineering, 108, 108674.

[14]. Ali, A., Pasha, M. F., Guerrieri, A., Guzzo, A., Sun, X., Saeed, A., ... & Fortino, G. (2023). A Novel Homomorphic Encryption and Consortium Blockchain-based Hybrid Deep Learning Model for Industrial Internet of Medical Things. IEEE Transactions on Network Science and Engineering.

[15]. Ajao, L. A., & Apeh, S. T. (2023). Secure Fog Computing Vulnerability in Smart City using Machine Learning and Blockchain Technology. networks, 20, 23.

[16]. Cai, J., Liang, W., Li, X., Li, K., Gui, Z., & Khan, M. K. (2023). Gtxchain: A secure iot smart blockchain architecture based on graph neural network. IEEE Internet of Things Journal.

[17]. Mazumdar, H., Chakraborty, C., Venkatakrishnan, S. B., Kaushik, A., & Gohel, H. A. (2023). Quantum-inspired heuristic algorithm for secure healthcare prediction using blockchain technology. IEEE Journal of Biomedical and Health Informatics.

[18]. Rajendran, T., Bharathi, S. S., Sridhar, S., & Anitha, T. (2023). A Study on Blockchain Technologies for Security and Privacy Applications in a Network. SSRG International Journal of Electronics and Communication Engineering, 10(6), 69-91.

[19]. Heidari, A., Navimipour, N. J., & Unal, M. (2023). A Secure Intrusion Detection Platform Using Blockchain and Radial Basis Function

Neural Networks for Internet of Drones. IEEE Internet of Things Journal.

[20]. Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R., Jolfaei, A., & Islam, A. N. (2023). A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. Journal of Parallel and Distributed Computing, 172, 69-83.