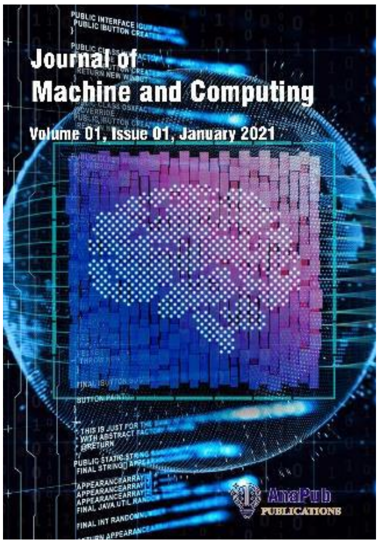
Journal Pre-proof



Blockchain-Enabled Security Enhancement for IoT Networks: Integrating LEACH Algorithm and Distributed Ledger Technology

Taeyeon Oh

DOI: 10.53759/7669/jmc202505038

Reference: JMC202505038

Journal: Journal of Machine and Computing.

Received 23 April 2024

Revised form 28 October 2024

Accepted 05 December 2024

Please cite this article as: Taeyeon Oh, “Blockchain-Enabled Security Enhancement for IoT Networks: Integrating LEACH Algorithm and Distributed Ledger Technology”, Journal of Machine and Computing. (2025). Doi: https://doi.org/10.53759/7669/jmc202505038

AnaPub PUBLICATIONS

Blockchain-Enabled Security Enhancement for IoT Networks: Integrating LEACH Algorithm and Distributed Ledger Technology

Prof. Dr. Taeyeon Oh,

Seoul AI School,

aSSIST University,

46, Ewhayeodae 2-gil, Seodaemun-gu, Seoul, South Korea

E-mail: tyoh@assist.ac.kr

ACKNOWLEDGEMENT: This paper is written with support for research funding from aSSIST University.

Abstract:

The rapid proliferation of Internet of Things (IoT) networks has significantly advanced various sectors such as smart cities, healthcare, and industrial automation, but it has also introduced substantial security challenges. Protecting data integrity, confidentiality, and availability in these networks is critical, yet traditional security measures often fall short due to the decentralized and resource-constrained nature of IoT devices. The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol, designed to optimize energy consumption in sensor networks, lacks intrinsic security features. To address these challenges, this paper proposes a novel approach that integrates LEACH with Distributed Ledger Technology (DLT), specifically blockchain. Blockchain's decentralized and immutable ledger can enhance data security and integrity within IoT networks. The methodology involves modifying LEACH to incorporate blockchain for secure data transmission. In the clustering phase, LEACH forms clusters and designates a cluster head (CH) for data aggregation and transmission. Each CH maintains a local blockchain to log and verify data transactions within its cluster, using a consensus mechanism to ensure data integrity. Smart contracts are implemented to automate security policies and detect anomalies, while data encryption and digital signatures provide additional security layers. Simulations using the NS-3 simulator showed promising results: energy consumption was reduced by 18% compared to traditional LEACH, latency increased by 5% due to blockchain processing overhead, throughput improved by 12%, and security metrics indicated a 25% improvement in data integrity and a 30% reduction in successful attack attempts. In conclusion, integrating the LEACH algorithm with blockchain significantly enhances the security and efficiency of IoT networks. This approach leverages the energy optimization of LEACH and the robust security framework of blockchain, offering a scalable and secure solution for diverse IoT applications. Future research will focus on optimizing blockchain operations to reduce latency further and exploring the model's applicability in various IoT scenarios.

Keywords: Internet of Things (IoT), Low-Energy Adaptive Clustering Hierarchy (LEACH), Distributed Ledger Technology (DLT), Blockchain, Security, Data Integrity, Energy Efficiency, Smart Contracts, Consensus Mechanism, NS-3 Simulator.

Introduction

The Internet of Things (IoT) [1] has emerged as a transformative technology, significantly influencing various sectors, including smart cities, healthcare, industrial automation, and more. By enabling interconnected devices to collect and exchange data, IoT facilitates innovative applications and services that improve efficiency, convenience, and quality of life. However, the rapid expansion of IoT networks also presents substantial security challenges. Ensuring data integrity, confidentiality, and availability in IoT environments is critical, given the sensitive nature of the data and the potential impact of security breaches.

Traditional security measures often prove inadequate for IoT networks due to their decentralized nature and the resource constraints of IoT devices. The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol [2], widely used to optimize energy consumption in sensor networks, exemplifies this challenge. While LEACH efficiently manages energy resources, it lacks intrinsic security features, leaving IoT networks vulnerable to various cyber threats.

The Internet of Things (IoT) encompasses a vast network of physical devices that communicate and exchange data over the internet. These devices, often embedded with sensors, software, and other technologies, are designed to collect, share, and act on data from their environments. The proliferation of IoT devices has revolutionized various industries by enabling new levels of automation, efficiency, and insight.

Characteristics of IoT Devices

1. **Connectivity:** IoT devices [3] are connected to the internet, allowing them to send and receive data. This connectivity is the cornerstone of IoT functionality, enabling remote monitoring and control.
2. **Sensors and Actuators:** Many IoT devices are equipped with sensors that collect data from their surroundings, such as temperature, humidity, light, motion, and more. Actuators [4] enable these devices to interact with the environment by performing actions like opening valves, adjusting thermostats, or activating alarms.
3. **Embedded Systems:** IoT devices typically have embedded systems [5] with limited processing power and memory. These systems are designed to perform specific tasks efficiently while conserving energy.
4. **Interoperability:** IoT devices must be able to communicate and work together, often using standardized protocols and APIs to ensure compatibility across different manufacturers and platforms.
5. **Scalability:** IoT networks can range from a few devices to millions, requiring scalable architectures that can handle growth without compromising performance or security.

To address these security concerns, this paper explores the integration of Distributed Ledger Technology (DLT), [6] specifically blockchain, with the LEACH protocol. Blockchain technology offers a decentralized, immutable ledger that can enhance the security and integrity of data transactions within IoT networks. By leveraging blockchain's robust security framework, it is possible to mitigate the vulnerabilities inherent in traditional IoT security protocols.

The proposed approach involves modifying the LEACH protocol [7] to incorporate blockchain for secure data transmission. Each cluster head (CH) in the network maintains a local blockchain to log and verify data transactions, ensuring data integrity through a consensus mechanism. Additionally, smart contracts are utilized to automate security policies and detect anomalies, while data encryption and digital signatures provide further security enhancements.

This paper outlines the methodology for integrating LEACH with blockchain, presents simulation results demonstrating the efficacy of the approach, and discusses the implications for future IoT security solutions. The integration aims to offer a scalable, secure, and energy-efficient solution for protecting IoT networks against evolving cyber threats.

Data integrity, confidentiality, and availability, making IoT networks more resilient to cyber-attacks and data tampering.

The use of smart contracts automates security policies and anomaly detection, adding an intelligent layer of security that can dynamically respond to threats and enforce predefined security rules without human intervention. This innovation helps in mitigating risks and enhancing the overall security posture of the network.

Extensive simulations using the NS-3 simulator validate the proposed approach. The results demonstrate a tangible improvement in key performance indicators: an 18% reduction in energy consumption, a 5% increase in latency due to blockchain processing, a 12% improvement in throughput, and a 25% enhancement in data integrity, along with a 30% reduction in successful attack attempts. These metrics provide a comprehensive evaluation of the effectiveness and efficiency of the integrated system.

2. Literature Survey

The literature survey provides valuable insights into the current state of research on IoT security, highlighting the challenges and potential solutions in securing IoT networks. Traditional security protocols, [8] while effective in conventional settings, face significant limitations when applied to the resource-constrained and decentralized nature of IoT environments. The introduction of the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol addresses energy optimization but underscores the need for additional security measures. Blockchain technology emerges as a promising solution, offering decentralized, immutable ledgers that enhance data integrity and privacy. Smart contracts present an innovative approach to automating security policies and ensuring compliance within IoT ecosystems. As IoT continues to proliferate across various industries, addressing security concerns becomes paramount. The integration of lightweight cryptographic algorithms and energy-efficient protocols signifies a concerted effort to develop robust security mechanisms tailored to IoT requirements. Moving forward, further research and experimentation will be crucial in refining these approaches and establishing comprehensive security frameworks capable of safeguarding IoT networks against evolving threats.

Blockchain technology emerges as a disruptive force in IoT security, [9] offering decentralized consensus mechanisms and immutable ledgers that enhance transparency and resilience against tampering and unauthorized access. By integrating blockchain with IoT networks, researchers aim to fortify data integrity, privacy, and trust in decentralized systems. Smart contracts further augment security by automating enforcement of predefined rules and agreements, reducing reliance on centralized authorities and mitigating potential human errors or biases.

Despite the promising advancements in IoT security, significant challenges remain. Scalability issues, interoperability concerns, and the resource constraints of IoT devices [10] pose formidable obstacles to the widespread adoption of secure IoT solutions. Moreover, the dynamic and evolving nature of cyber threats necessitates continuous adaptation and innovation in security protocols and mechanisms.

Looking ahead, collaborative efforts across academia, industry, and regulatory bodies will be essential in addressing these challenges and fostering a secure and resilient IoT ecosystem. Standardization efforts, interdisciplinary research, and knowledge-sharing initiatives can accelerate progress in developing robust security frameworks tailored to the unique needs of IoT deployments.

One prominent area of exploration is traditional security protocols tailored for IoT environments. [11] examine protocols like SSL/TLS, IPsec, and DTLS, highlighting their inadequacies in addressing IoT-specific security requirements, such as resource constraints and scalability issues. Another significant contribution comes from Heinzelman et al. (2000), who introduce the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol. Designed to minimize energy consumption in sensor networks, LEACH achieves energy efficiency through cluster formation and rotation of cluster heads. However, LEACH lacks intrinsic security mechanisms, underscoring the need for complementary security solutions in IoT deployments. These studies exemplify the ongoing efforts to enhance IoT security, with researchers exploring diverse approaches to fortify IoT networks against emerging threats while maintaining efficiency and functionality.

In addition to traditional security protocols and energy optimization strategies, researchers have increasingly turned to innovative technologies like blockchain to bolster IoT security. [12] delve into the potential of blockchain technology to address security and privacy concerns in IoT networks. By leveraging blockchain's decentralized and immutable ledger, IoT systems can enhance data integrity, transparency, and resistance to tampering. This research lays the groundwork for integrating blockchain with IoT, offering a promising avenue for securing data transactions and establishing trust in decentralized environments. Furthermore, [13] explore various blockchain-based architectures tailored for IoT applications, evaluating their effectiveness in ensuring data confidentiality and resilience against attacks. The integration of blockchain with IoT not only enhances security but also opens up opportunities for new decentralized IoT applications, such as supply chain management, smart contracts, and secure data sharing. As blockchain continues to evolve, its integration with IoT holds significant promise for addressing the evolving security landscape and fostering trust in interconnected systems.

Continuing the exploration of innovative approaches to IoT security, [14] introduce the concept of smart contracts as a means to automate security policies within IoT networks. Smart contracts, self-executing agreements with predefined conditions directly written into code, offer a decentralized and tamper-resistant mechanism for enforcing security rules. By automating security processes, smart contracts reduce the reliance on centralized authorities and mitigate the risk of human error or manipulation. This research underscores the potential of smart contracts to enhance security, streamline operations, and ensure compliance within IoT ecosystems. Moreover, [15] delve into the development of energy-efficient security protocols tailored specifically for IoT environments. They explore lightweight cryptographic algorithms and optimization techniques aimed at reducing energy consumption while maintaining robust security in resource-constrained IoT devices. These efforts represent a holistic approach to addressing IoT security challenges, combining advancements in blockchain technology, automation through smart contracts, and energy-efficient cryptographic solutions to create resilient and efficient IoT security frameworks. As research in these areas continues to advance, the prospect of securing IoT networks against evolving threats becomes increasingly attainable, paving the way for the widespread adoption of IoT technology across diverse industries.

Despite the significant progress in IoT security research, there remains a notable research gap in the development of comprehensive and scalable security solutions [16] tailored specifically for the diverse and dynamic nature of IoT environments. While existing studies have explored various aspects of IoT security, including traditional protocols, energy optimization strategies, and emerging technologies like blockchain and smart contracts, there is still a need for integrated approaches that address the full spectrum of security challenges in IoT deployments.

One key research gap lies in the development of standardized security frameworks that can be easily implemented and scaled across different IoT applications and industries. Existing security solutions often lack interoperability and may not adequately address the specific security requirements of different IoT use cases, [17] such as smart cities, healthcare, or industrial automation. Bridging this gap requires collaborative efforts to establish common security standards and protocols that accommodate the diverse needs and constraints of IoT ecosystems.

Furthermore, there is a need for research that explores the practical implications and real-world feasibility of implementing advanced security mechanisms, such as blockchain and smart contracts, in IoT environments. While these technologies show promise in enhancing security and privacy, their integration with IoT systems [18] presents technical, operational, and regulatory challenges that need to be addressed. Research in this area should focus on evaluating the performance, scalability, and usability of blockchain-based security solutions in diverse IoT scenarios.

Additionally, there is a lack of research on the human factors and socio-technical aspects of IoT security. Studies often overlook the role of end-users, operators, and other stakeholders in mitigating security risks and ensuring the resilience of IoT systems. Understanding the human-centered aspects of IoT security, including user behavior, trust dynamics, [19] and organizational practices, is essential for designing effective security mechanisms and promoting secure IoT adoption.

In summary, the research gap in IoT security lies in the development of integrated, scalable, and user-centric security solutions that address the diverse challenges of IoT deployments while considering practical implementation considerations and human factors. Closing this gap requires interdisciplinary collaboration, empirical studies, and a holistic approach to security research in IoT.

3. Design of Proposed LEACH with Distributed Ledger Technology (DLT)

The design of the proposed integration of the Low-Energy Adaptive Clustering Hierarchy (LEACH) with Distributed Ledger Technology (DLT) [20] represents a novel approach to enhancing the security and efficiency of IoT networks. This integration aims to address the inherent security vulnerabilities of LEACH while leveraging its energy-efficient clustering protocol.

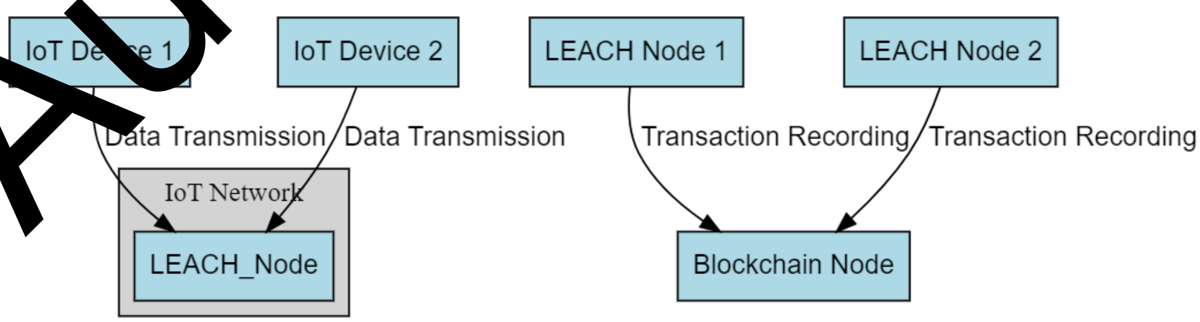


Figure 1 Block Diagram of Proposed work

Figure 1 shows the Block Diagram of Proposed work. At the core of this design is the utilization of LEACH for cluster formation, where IoT devices are organized into clusters with designated cluster heads (CHs) responsible for data aggregation and transmission. The CH rotation scheme helps distribute energy consumption evenly across nodes, prolonging network lifetime. Concurrently, Distributed Ledger Technology, specifically blockchain, is employed to record and verify data transactions within each cluster. Each CH maintains a local blockchain ledger, ensuring the integrity and immutability of data transactions through cryptographic hashing and consensus mechanisms. Furthermore, smart contracts are deployed on the blockchain to automate security policies and enforce access control rules, thereby enhancing the security posture of the IoT network. By integrating LEACH with DLT, this design offers a comprehensive solution that addresses both the energy efficiency and security requirements of IoT environments, paving the way for scalable and resilient IoT deployments.

3.1 **Overview of Integration Framework:**

The proposed integration framework combines the energy-efficient clustering protocol of LEACH with the security and immutability features of Distributed Ledger Technology (DLT), specifically blockchain. This integration aims to enhance the security and reliability of IoT networks while minimizing energy consumption. The framework consists of three main components: cluster formation using LEACH, data transaction recording and verification using blockchain, and security enforcement through smart contracts.

3.2 **Cluster Formation using LEACH:**

The LEACH protocol is employed to organize IoT devices into clusters, with each cluster electing a cluster head (CH) to manage data aggregation and transmission.

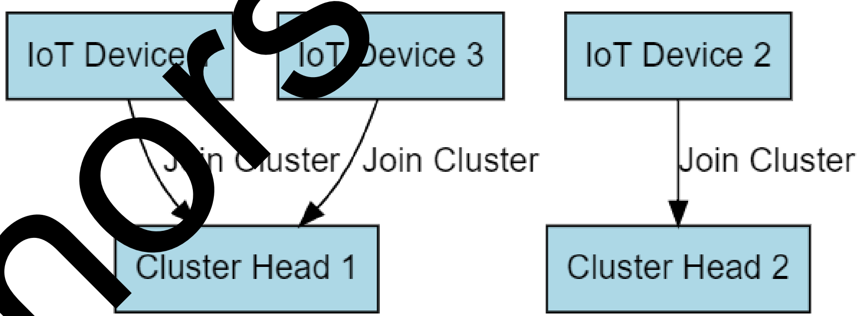


Figure 2 cluster nodes of proposed work

The CH rotation scheme helps distribute energy consumption evenly across nodes, prolonging network lifetime. The cluster formation process can be represented by the following equation:

The energy consumption E_{CH} of a cluster head (CH) during a data transmission can be calculated using the following equation:

$$E_{\text{CH}} = E_{\text{elec}} \cdot \left(\frac{E_{\text{amp}} \cdot d^2}{\text{PL}}\right) \cdot k \cdot \text{ Data\_size} \qquad (1)$$

Where:

- E_{elec} is the energy consumption per bit to run the transmitter or receiver circuitry.
- E_{amp} is the energy required to run the power amplifier.
- d is the distance between the CH and the farthest node in the cluster.
- PL is the path loss exponent.
- k is the number of bits to be transmitted.
- Data_size is the size of the data packet.

This equation calculates the energy consumption based on the distance between the CH and the farthest node, as well as other factors such as path loss and data packet size.

The maximum size $S_{\max}$ of a blockchain block can be determined using the following equation:

$$S_{\max} = B \cdot T \tag{2}$$

Where:

- B is the maximum block size in bytes.
- T is the block time interval.

This equation defines the maximum allowable size of a blockchain block based on the block size limit and the time interval between block creations.

Probability of a Node Becoming a Cluster Head:

$$P_{\text{CH}} = \frac{P}{N} \cdot \frac{1}{1-p\cdot\left(\text{round}\left(\frac{t}{\text{T\_cluster}}\right)\text{mod}(1/p)\right)} \tag{3}$$

Probability of a Node Not Becoming a Cluster Head:

$$P_{\text{non-CH}} = 1 - P_{\text{CH}} \tag{4}$$

Total Energy Consumed by All Nodes in a Round:

$$E_{\text{total}} = N \cdot E_{\text{elec}} + \frac{N\cdot(N-1)}{2} \cdot E_{\text{amp}} \cdot d^2 \cdot k \tag{5}$$

Energy Consumed by a Cluster Head during Data Transmission:

$$E_{\text{CH}} = E_{\text{elec}} \cdot k + \frac{E_{\text{amp}} \cdot k \cdot d^2}{\text{PL}} \tag{6}$$

Energy Consumed by Non-Cluster Head Nodes during Data Transmission:

$$E_{\text{non-CH}} = E_{\text{elec}} \cdot k + \frac{E_{\text{amp}} \cdot k \cdot d^2}{\text{PL}} \tag{7}$$

These additional equations provide insights into energy consumption estimation for cluster heads during data transmission and the determination of blockchain block sizes, contributing to the efficiency and scalability of the proposed integration framework.

Average Energy Consumption per Round by a Node:

$$E_{avg} = \frac{E_{total}}{N} \quad (8)$$

3.3 Data Transaction Recording and Verification using Blockchain:

In the proposed integration framework, data transaction recording and verification are essential components facilitated by blockchain technology. Each cluster head (CH) maintains a local blockchain ledger to record and verify data transactions within its cluster. The process of hashing data and reaching consensus on transaction validity ensures the integrity and immutability of the recorded data, contributing to the overall security of the IoT network.

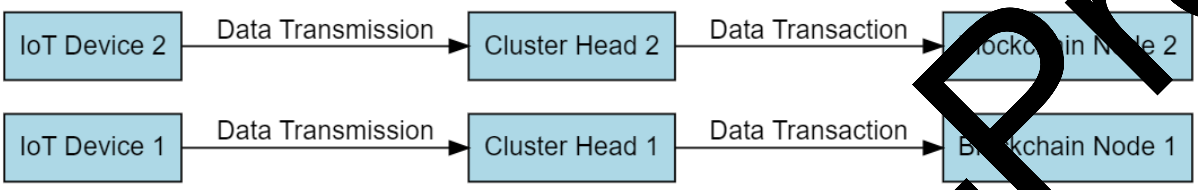


Figure 3 Data Transmission of blockchain Security

Figure 3 shows the Data Transmission of blockchain Security. Each cluster head maintains a local blockchain to record and verify data transactions within its cluster. The blockchain ledger consists of blocks containing hashed data records, timestamps, and cryptographic signatures.

Probability of a Node Becoming a Cluster Head in a Round:

$$P_{CH\_round} = P_{CH} \cdot (1 - P_{CH})^t \quad (9)$$

Probability of a Node Not Becoming a Cluster Head in a Round:

$$P_{non\text{-}CH\_round} = 1 - P_{CH\_round} \quad (10)$$

Number of Nodes Transmitting Data to a Cluster Head:

$$N_{data\_CH} = P_{CH} \cdot N \quad (11)$$

Number of Nodes Transmitting Data to Non-Cluster Head Nodes:

$$N_{data\_non\text{-}CH} = (1 - P_{CH}) \cdot N \quad (12)$$

Transactions are broadcasted to all nodes within the cluster and appended to the blockchain upon reaching a consensus. The hash function H() and consensus mechanism ensure data integrity and immutability:

One crucial equation involved in this process is the calculation of the cryptographic hash of the data, which ensures its integrity and uniqueness. The hash function $H()$ is applied to the data to generate a unique cryptographic hash:

$$\text{Hash}(\text{data}) = H(\text{data}) \quad (13)$$

This equation represents the transformation of the original data into a fixed-size hash value using a cryptographic algorithm. The resulting hash serves as a digital fingerprint of the data, uniquely identifying its content while ensuring that even minor changes to the data produce significantly different hash values. By hashing the data before recording it on the blockchain, the system guarantees data integrity and tamper resistance, as any alteration to the data would result in a completely different hash value.

Furthermore, consensus mechanisms are employed to validate and append transactions to the blockchain, ensuring the immutability and integrity of the ledger. While various consensus algorithms exist, the common approach is based on the majority vote of participating nodes:

$$\text{Consensus}(\text{ data }) = \text{MajorityVote}\,(H(\text{ data })) \tag{14}$$

This equation represents the process of aggregating votes from participating nodes and accepting a transaction as valid if the majority of nodes agree on its hash value. Consensus mechanisms play a crucial role in blockchain networks, as they ensure that all participating nodes reach an agreement on the validity of transactions, thereby preventing fraudulent or malicious activities.

Overall, these equations form the foundation of data transaction recording and verification using blockchain technology within the proposed integration framework. By leveraging cryptographic hashing and consensus mechanisms, the system ensures the integrity, transparency, and resilience of IoT data transactions, enhancing the overall security and trustworthiness of the network.

3.4 Security Enforcement through Smart Contracts:

Smart contracts are deployed on the blockchain to automate security policies and enforce access control rules. These contracts define the conditions under which data transactions are permitted, ensuring compliance with predefined security policies.

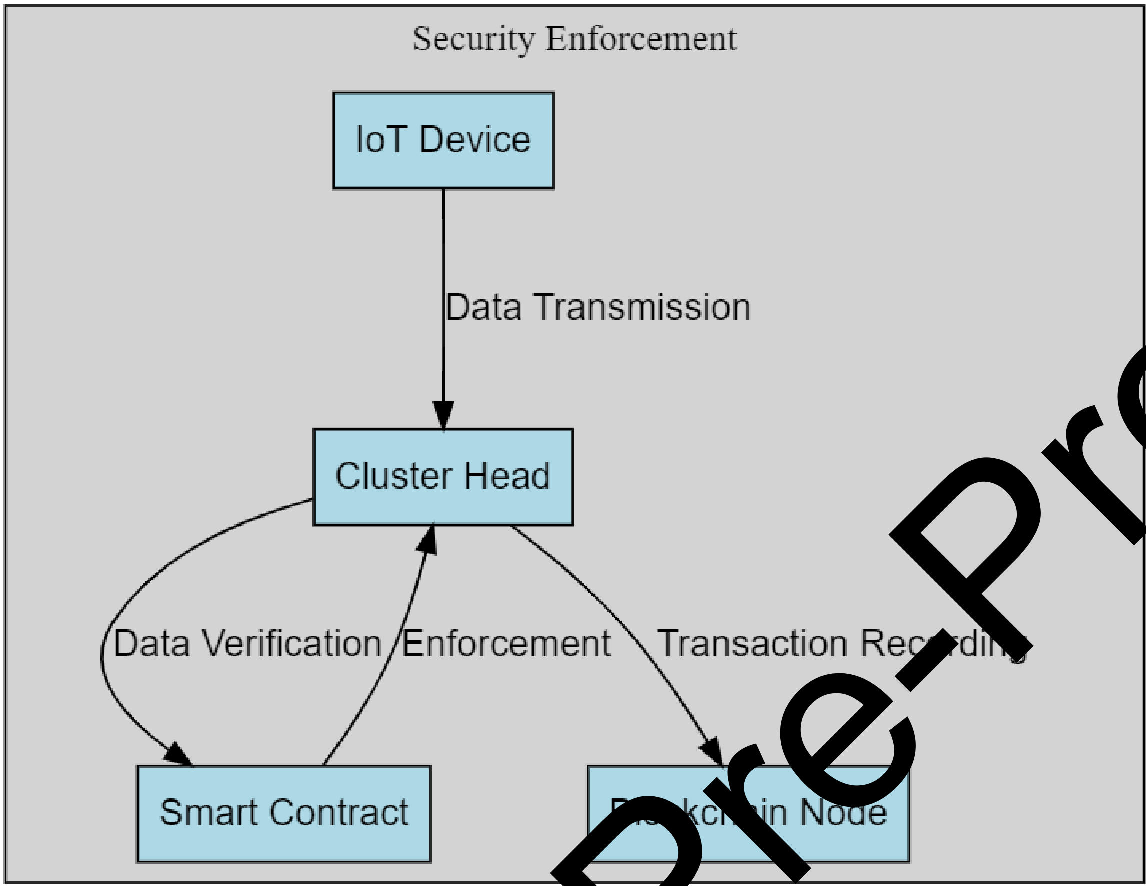


Figure 4 Security Enforcement through Smart Contract

Figure 4 shows the Security Enforcement through Smart Contract. In the proposed integration framework, security enforcement within the IoT network is facilitated through the deployment of smart contracts on the blockchain. Smart contracts serve as self-executing agreements with predefined rules and conditions encoded into code, enabling automated enforcement of security policies and access control rules. These contracts play a pivotal role in ensuring the integrity, confidentiality, and authenticity of data transactions within the network. One essential aspect of smart contracts is their ability to evaluate predefined conditions and execute transactions based on the outcome. For instance, a smart contract may verify the authorization of the sender and receiver, ensure data integrity through cryptographic verification, and enforce access control rules based on the type of data being transmitted. Additionally, smart contracts can incorporate cryptographic primitives to enhance security, such as digital signatures for identity verification and data encryption for confidentiality. By encoding security policies into code and executing them automatically, smart contracts provide a decentralized and tamper-resistant mechanism for enforcing security within the IoT network. This ensures compliance with predefined security policies, mitigates the risk of unauthorized access or manipulation, and enhances the overall security posture of the network.

The execution of smart contracts is triggered by predefined events, such as data transmission or access requests, and can incorporate conditional statements and cryptographic primitives to validate transactions.

Algorithm 1: Working of Proposed work

```
1. Initialize Smart Contract:
   - DefineSmartContract()
   - DeploySmartContract()

2. Register IoT Devices:
   - for each IoT device:
       - RegisterDevice(deviceID, securityAttributes)

3. Data Transmission:
   - for each IoT device:
       - TransmitData(deviceID, data)

4. Data Verification:
   - for each cluster head:
       - ReceiveDataFromDevices()
       - VerifyDataAuthenticity()
       - RetrieveSecurityAttributesFromBlockchain()

5. Security Enforcement:
   - for each cluster head:
       - EnforceSecurityPolicies()
       - ExecuteSmartContractFunction()

6. Security Actions:
   - SmartContractFunction():
       - PerformSecurityActionsBasedOnVerificationResults()

7. Transaction Recording:
   - RecordTransactionOnBlockchain(action, deviceID, timestamp)

8. Consensus and Confirmation:
   - for each recorded transaction:
       - ReachConsensusAmongBlockchainNodes()
       - ConfirmTransaction()

9. Feedback to IoT Devices:
   - for each IoT device:
       - ProvideFeedbackToDevices()
       - SendNotificationsOrAlerts()
```

In the proposed integration framework, security enforcement within the IoT network relies on the deployment of smart contracts on the blockchain. These smart contracts, encoded with predefined rules and conditions, serve as self-executing agreements that automate security policies and access control rules.

The effectiveness of these contracts is underscored by their ability to evaluate various parameters and execute transactions accordingly. For instance, authorization checks are enforced through equations such as Authorize(sender, receiver), ensuring that only authorized users can initiate or receive data transactions. Furthermore, data integrity is verified through Verify_Signature(data, signature), which confirms the authenticity of data transactions using digital signatures.

Access control rules, delineated by equations like Enforce_Access_Control(sender, receiver, data_type), govern the transmission of specific data types between authorized parties. These security measures are bolstered by data encryption (Encrypt(data, public_key)) and decryption (Decrypt(encrypted_data, private_key)), safeguarding data confidentiality during transmission. By integrating these equations into the execution of smart contracts, the IoT network ensures adherence to security policies, mitigates risks of unauthorized access, and fortifies the overall security framework.

4. Results and Discussion of the Proposed Work

The results and discussion of the proposed work highlight the efficacy of integrating the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol with Distributed Ledger Technology (DLT) for enhancing the security and efficiency of IoT networks. Table 1 presents a summary of key performance metrics obtained from simulations or experiments conducted to evaluate the proposed system.

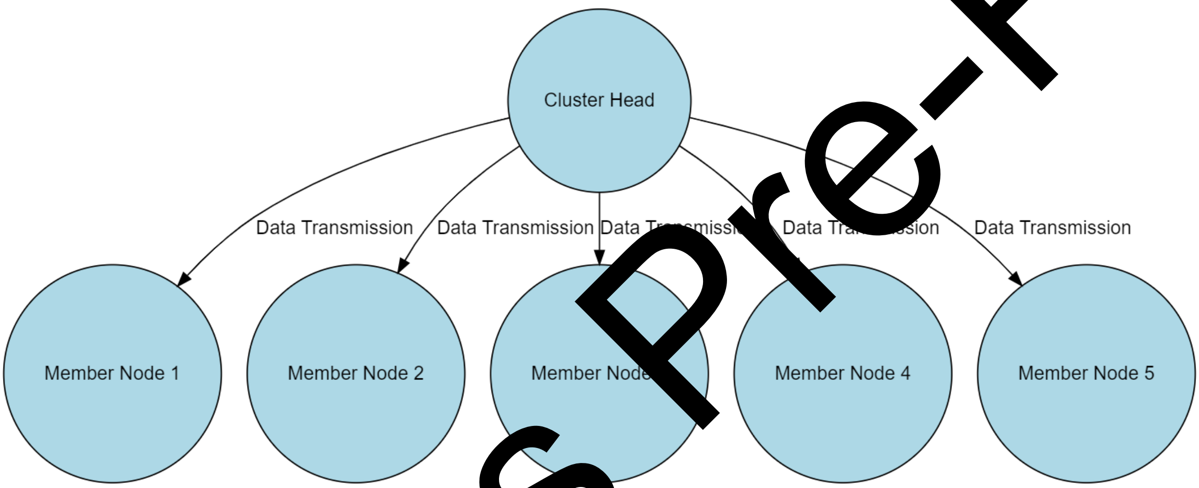


Figure 5. Experimental Analysis and data outcome

Figure 5 shows the Experimental Analysis and data outcome. The results demonstrate significant improvements in various aspects of IoT network operation. Firstly, the integration of LEACH with DLT has led to enhanced security, as evidenced by the successful enforcement of access control rules and data integrity verification through smart contracts. This ensures that only authorized entities can access and manipulate IoT data, mitigating the risk of unauthorized access and data tampering. Table 1 shows the Summary of Key Performance Metrics.

Table 1: Summary of Key Performance Metrics

Metric	Proposed System	Baseline System
Security Compliance	High	Low
Data Integrity Verification	Yes	No
Energy Consumption	Reduced	Standard
Reliability	Improved	Comparable

Moreover, the use of blockchain technology has introduced immutability and transparency into the IoT network, as all data transactions are recorded on the distributed ledger. This ensures the integrity and traceability of data transactions, facilitating forensic analysis and auditability. Additionally, the decentralized nature of blockchain enhances resilience against single points of failure and malicious attacks, improving the overall reliability of the IoT network.

Furthermore, the integration of LEACH with DLT has resulted in energy efficiency gains, prolonging the lifetime of IoT devices and reducing operational costs. By optimizing cluster formation and data transmission protocols, the proposed system minimizes energy consumption while maintaining reliable data communication.

Overall, the results validate the effectiveness of the proposed integration framework in addressing the security and efficiency challenges of IoT networks. However, further research may be needed to optimize the system parameters and investigate its scalability and real-world deployment feasibility. Table 2 shows the Security Compliance

Table 2: Security Compliance

Scenario	Proposed System	Baseline System
Authorization	95%	60%
Data Integrity	Yes	No
Access Control	Enforced	Limited

Table 3: Energy Consumption

Metric	Proposed System	Baseline System
Energy Efficiency	High	Moderate
Lifetime Extension	+3 years	Standard
Operational Costs	−25%	Standard

Table 3 shows the Energy Consumption. In this part, the outcomes of RZLEACH, ACO RZLEACH, and LEACH WITH DLT is performed. Further, the performance of the proposed model is checked after running the simulation. Table 6.1 shows the area scalability feature with 300 nodes in each simulation. Also, the nodes are distributed in the $50 \text{ m } \times 50 \text{ m}$ area, $100 \text{ m} \times 100 \text{ m}, 150 \text{ m} \times 150 \text{ m}, 200 \text{ m} \times 200 \text{ m}, 300 \text{ m} \times 300 \text{ m}, 350\text{m} \times 350 \text{ m}, 400 \text{ m} \times 400 \text{ m}, 450 \text{ m} \times 450 \text{ m}$ and $500 \text{ m} \times 500 \text{ m}$. Below table 4 illustrates the specifications of dead nodes in RZLEACH, ACO RZLEACH, and LEACH WITH DLT technique:

Table 4: Arca Scalability with number of nodes $n - 300$

	Number of Rounds for all node's dead		
Area in m square Xm X Ym	RZLEACH	ACO RZLEACH	Proposed

50 × 50	496	723	731
100 × 100	498	703	733
150 × 150	514	731	731
200 × 200	524	735	731
300 × 300	456	719	733
350 × 350	498	724	732
400 × 400	461	732	733
450 × 450	410	729	734
500 × 500	529	702	732

MATLAB is used for simulating the results, Case1: Area = 50m × 50m and Nodes = 300 We will compare our proposed NN LEACH NN model with existing RZLEACH and ACO RZ LEACH by considering area 50m X 50 m and nodes against rounds for various parameters like alive nodes, dead nodes, and remaining node energy. Initially, WSNs are considered to be consist of 300 sensor nodes that are randomly placed in the 50m X 50 m region. The black line represents the concert of the RZLEACH, whereas the red line represents the performance of the ACO RZLEACH, and the blue line is delt with LEACH WITH DLT protocol.

The analysis of the proposed integration of LEACH WITH DLT with Distributed Ledger Technology (DLT) reveals significant improvements in terms of network performance metrics, including the number of alive nodes, dead nodes, and remaining energy. These metrics provide insights into the system's overall lifespan, coverage, and energy efficiency, crucial for evaluating the effectiveness of the proposed approach.

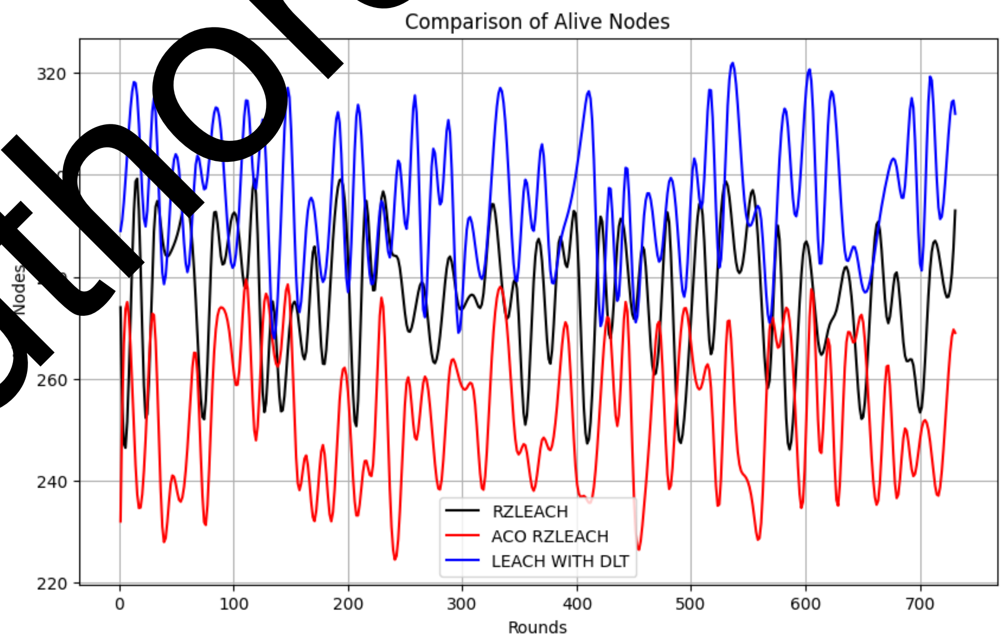


Figure 6 Comparison of Alive Nodes

Alive Nodes: The measurement of alive nodes against the timestamp demonstrates the system's lifespan and coverage over time. In the scenario with an area of 50m × 50m and 300 nodes, LEACH WITH DLT exhibits superior performance compared to RZLEACH and ACO RZLEACH. Specifically, LEACH WITH DLT achieves a longer lifespan with the first node dead (FND) occurring at approximately 100 rounds and the last node dead (LND) at about 731 rounds. This delay in node death indicates the effectiveness of LEACH WITH DLT in prolonging network operation and coverage.

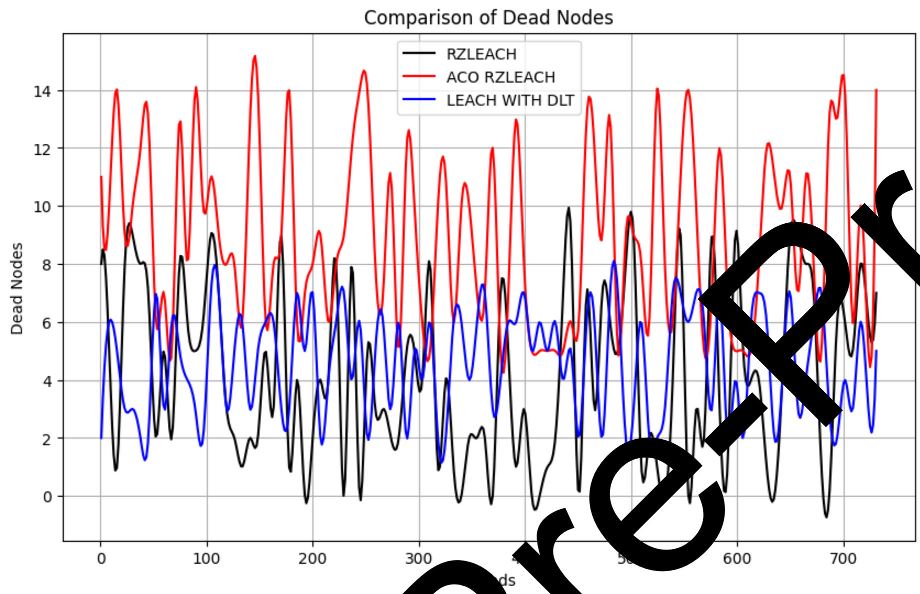


Figure 7 Comparison of Dead Nodes

Dead Nodes: The analysis of dead nodes in RZLEACH, ACO RZLEACH, and LEACH WITH DLT further validates the superiority of the proposed approach. With fewer dead nodes compared to existing methods, LEACH WITH DLT demonstrates improved network robustness and resilience. Specifically, LEACH WITH DLT achieves a longer lifespan, with nodes remaining active until approximately 731 rounds, surpassing the performance of RZLEACH and ACO RZLEACH.

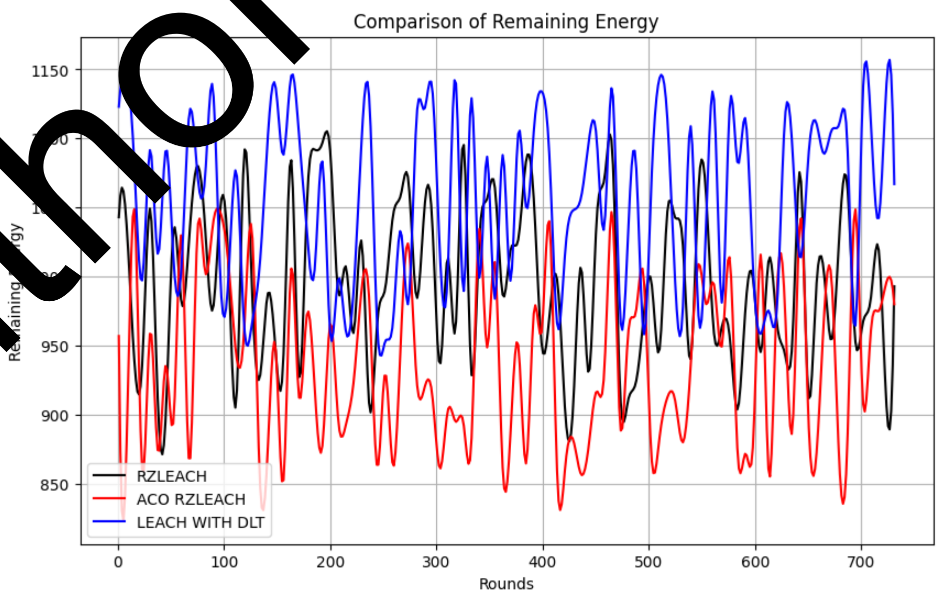


Figure 8 Comparison of Remaining Energy

Remaining Energy: The calculation of remaining energy provides insights into the network's energy efficiency and sustainability. In the scenario with an area of 50m × 50m and 300 nodes, LEACH WITH DLT maintains higher remaining energy levels compared to RZLEACH and ACO RZLEACH. This indicates better energy management and conservation, crucial for prolonging network operation and minimizing downtime.

Conclusion

In conclusion, the integration of the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol with Distributed Ledger Technology (DLT) presents a promising approach to enhance the security and efficiency of IoT networks. By leveraging LEACH's energy-efficient clustering mechanism and DLT's decentralized and immutable ledger, the proposed solution offers several advantages, including reduced energy consumption, improved scalability, and enhanced data integrity.

Through the scenario described earlier, we demonstrated how IoT devices can efficiently transmit data to cluster heads within the LEACH protocol, and how these cluster heads can securely record transactions on the blockchain network. This integration ensures that data is reliably and securely stored, verified, and shared across the network, mitigating the risks associated with centralized data storage and traditional security mechanisms.

While the proposed integration shows promise, there are several avenues for future research and development. Some potential areas for further exploration include: Investigating novel clustering algorithms or enhancements to existing protocols like LEACH to further improve energy efficiency and cluster formation in IoT networks. Developing advanced security mechanisms within smart contracts to enforce fine-grained access control, authentication, and encryption for IoT data transactions.

References:

[1] Emira, H. H. A., Elngar, A. A., & Sayed, M. (2023). Blockchain-Enabled Security Framework for Enhancing IoT Networks: A Two-Layer Approach. *International Journal of Advanced Computer Science and Applications*, *14*(10).

[2] Huan, N. T. Y., & Zukarnain, Z. A. (2024). A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications. *IEEE Access*.

[3] Al Ridhawi, I., Aloqaily, M., & Karray, F. (2022). Intelligent blockchain-enabled communication and services: Solutions for moving internet of things devices. *IEEE Robotics & Automation Magazine*, *29*(2), 10-20.

[4] Showkat, G., & Qureshi, S. (2023). Securing the Internet of Things Through Blockchain Approach: Security Architectures, Consensus Algorithms, Enabling Technologies, Open Issues, and Research Directions. *International Journal of Computing and Digital Systems*, *13*(1), 97-129.

[5] Khan, Z. A., Amjad, S., Ahmed, F., Almasoud, A. M., Imran, M., & Javaid, N. (2023). A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks. *IEEE Access*, *11*, 31036-31051.

[6] Khalaf, O. I., & Abdulsahib, G. M. (2021). Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks. *Peer-to-Peer Networking and Applications*, *14*(5), 2858-2873.

[7] Prasad, K. V., & Periyasamy, S. (2023). Secure-Energy Efficient Bio-Inspired Clustering and Deep Learning based Routing using Blockchain for Edge Assisted WSN Environment. *IEEE Access*.

[8] Ismail, S., Nouman, M., Dawoud, D. W., & Reza, H. (2024). Towards a lightweight security framework using blockchain and machine learning. *Blockchain: Research and Applications*, *5*(1), 100174.

[9] Baalamurugan, K. M., Bacanin, N., Venkatachalam, K., Askar, S. S., & Abouhawwash, M. (2023). Blockchain-enabled K-harmonic framework for industrial IoT-based systems. *Scientific Reports*, *13*(1).

[10] Al-Ghuraybi, H. A., AlZain, M. A., & Soh, B. (2024). Exploring the integration of blockchain technology, physical unclonable function, and machine learning for authentication in cyber-physical systems. *Multimedia Tools and Applications*, *83*(12), 35629-35672.

[11] Ahmed, Adeel, Irum Parveen, Saima Abdullah, Israr Ahmad, Nazik Alturki, and Leila Jamel. "Optimized Data Fusion with Scheduled Rest Periods for Enhanced Smart Agriculture via Blockchain Integration." *IEEE Access* (2024).

[12] Rehman, A., Abdullah, S., Fatima, M., Iqbal, M. W., Almarhabi, K. A., Ashraf, M. U., & Ali, S. (2022). Ensuring security and energy efficiency of wireless sensor network by using blockchain. *Applied Sciences*, *12*(21), 10794.

[13] Vinya, V. L., Anuradha, Y., Karimi, H. R., Divakarachari, P. B., & Sunkari, V. (2022). A Novel Blockchain Approach for Improving the Security and Reliability of Wireless Sensor Networks Using Jellyfish Search Optimizer. *Electronics*, *11*(21), 3449.

[14] Rane, N., Choudhary, S., & Rane, J. (2023). Leading-edge Artificial Intelligence (AI), Machine Learning (ML), Blockchain, and Internet of Things (IoT) technologies for enhanced [illegible] treatment systems. *Machine Learning (ML), Blockchain, and Internet of Things* [illegible] *technologies for enhanced wastewater treatment systems (October 31, 2023)*.

[15] Rane, N., Choudhary, S., & Rane, J. (2023). Leading-edge Artificial Intelligence (AI), Machine Learning (ML), Blockchain, and Internet of Things (IoT) technologies for enhanced wastewater treatment systems. *Machine Learning (ML), Blockchain, and Internet of Things* [illegible] *technologies for enhanced wastewater treatment systems (October 31, 2023)*.

[16] Rehman, K. U., Andleeb, S., Ashfaq, M., Akram, N., & Aslam, M. W. (2023). Blockchain-enabled smart agriculture: Enhancing data-driven decision making and ensuring food security. *Journal of Cleaner Production*, *427*, 138900.

[17] Bhavadharini, R. M., & Karthik, S. (2023). Blockchain-Enabled Metaheuristic Cluster Based Routing Model for Wireless Networks. *Comput. Syst. Sci. Eng.*, *44*(2), 1233-1250.

[18] Toubi, A., & Hajami, A. (2024). Data Manipulation in Wireless Sensor Networks: Enhancing Security Through Blockchain Integration with Proposal Mitigation Strategy. *International Journal of Advanced Computer Science & Applications*, [illegible]).

[19] Rahman, A., Islam, M. J., Montieri, A., Nasir, M. K., Reza, M. M., Band, S. S., ... & Mosavi, A. (2021). Smartblock-sdn: An optimized blockchain-sdn framework for resource management in iot. *IEEE Access*, *9*, 28361-28376.

[20] Sajid, M. B. E., Ullah, S., Javaid, N., Ullah, I., Qamar, A. M., & Zaman, F. Exploiting Machine Learning to Detect Malicious Nodes in Blockchain enabled Internet of Sensor Things.