International Journal of Engineering & Tech Development
ISSN: 3067-669X / Open Access / IJETD_Y2F2A002
Apex Academia Press / https://doi.org/10.63665/ijetd-y2f2a002

Original Article

Secure Blockchain-Based Routing Framework for Iot Networks Using Lightweight Consensus Mechanisms to Enhance Routing Security

Okeke Ogochukwu Clementina[1], Mgbeafulike Ike Joseph[2], Osita Miracle Nwakeze[3], Omorogie Michael[4], Uju Cynthia Nwabudike[5]

[1,2,3] Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University Uli, Anambra State, Nigeria.
[4,5] Department of Computer Science, Ogwashiuku Polytechnic, Delta State, Nigeria.
[6] Department of Computer science, Dennis Osadebay University Asaba, Delta State, Nigeria.

Abstract

Internet of Things (IoT) is experiencing a rapid growth and has led to the deployment of billions of interconnected devices in various applications such as healthcare, smart cities, industrial automation, environmental monitoring etc. Although the advantages of IoT technology, the security of the routing protocols is still a significant concern because of the emerging attacks like blackhole, wormhole, sinkhole and Sybil attacks. The traditional security approaches usually use a centralized architecture which is prone to single-point failures and is not appropriate for a distributed architecture like IoT. In addition, traditional consensus mechanisms for blockchain networks are energy-intensive and demand significant computational power, which may not be feasible for resource-constrained IoT networks. The current study aimed to enhance the security of routing in IoT Networks by introducing a Secure Blockchain-Based Routing Framework (SBBRF) with Lightweight Consensus Mechanisms (LCM) to ensure communication efficiency and security. The framework combines the use of blockchain technology, trust-aware routing, smart contracts, and lightweight consensus mechanisms, such as the Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA), to deliver trust management for decentralized networks, authentication for network routes, and detection of malicious nodes. The system is implemented with the help of network simulation using NS-3 and blockchain using Hyperledger Fabric. A trust classification model was trained and tested with the node behavioural data, and the accuracy, precision, recall and F1-score were 96.8%, 95.9%, 97.4% and 96.6% respectively. The results of the performance evaluation indicated that the proposed framework could attain a packet delivery ratio of 96.5%, throughput of 940Kbps, end-to-end delay of 92ms, energy consumption of 2.91J and routing overhead of 1180 control packets. The framework also achieved an average of 96.6% attack detection rate on blackhole, wormhole, Sybil and sinkhole attacks. The outcomes show that the proposed framework is safe, scalable, and energy-efficient routing solution that can enhance the communication reliability and cybersecurity in modern IoT networks.

Keywords

Internet of Things, Blockchain, Routing Security, Lightweight Consensus Mechanisms.

Article History

Received: 12.04.2026

Accepted: 23.04.2026

Published: 29.04.2026

1. Introduction

The Internet of Things (IoT) is one of the most significant technological advancements of the twenty first century, and one that allows seamless communication between billions of interconnected devices (Johar et al., 2026). The IoT systems are utilized across a lot of different segments like healthcare, smart cities, industrial automation, agriculture, transportation, and environment monitoring. IoT networks enable the seamless collection, processing, and intelligent decision-making of data in real-time, thanks to the integration of sensors, actuators, wireless communication technologies, and cloud services (Ghadban et al., 2025). The connected IoT devices are projected to keep increasing exponentially, leading to increasingly complex and large network infrastructures. This expansion can create great potential for automation and efficiency, but also significant security and privacy concerns that endanger the security of IoT communications (Nwakeze, 2024).

https://creativecommons.org/licenses/by/4.0/

Easiest vulnerability in IoT is the vulnerability of the routing protocol (Gadekallu et al., 2021). The routing mechanisms are used to create and maintain connections between the devices so that the data packets will reach their destination. The distributed and resource constrained architecture of IoT network makes it very vulnerable to attacks like sinkhole attack, wormhole attack, blackhole attack, Sybil attack and selective forwarding attack. These attacks can alter routing data, compromise network operations, affect the quality of service and cause sensitive data to be compromised (Al Sadawi et al., 2021; Medisco, 2026). While traditional security solutions depend on the centralized trust management and authentication servers, they create a single point of failure and are harder to scale with the growing number of IoT deployments (Shahzad et al., 2025).

One-way Blockchain technology has shown promise of improving security in decentralized systems (Shujaa et al., 2025). Blockchain can ensure data integrity, traceability, and trust among participants by relying on a distributed ledger that records transactions in an immutable and transparent way, without the need for a centralized authority (Saba et al., 2025). When it comes to a routing system in the IoT world, blockchain can help verify the security of the route, provide distributed trust management, and store routing information without tampering. Yet, the typical blockchain platforms use consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS), which demand extensive computing power, memory, and energy usage (Kanellopoulos et al., 2023). The requirements make them incompatible for a lot of IoT devices, which are constrained in resources.

To overcome these drawbacks, lightweight consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA), and Delegated Proof of Stake (DPoS) have been explored, each with its own unique characteristics and performance advantages (Ahanger et al., 2022; Ibibo et al., 2025). These mechanisms offer a practical basis for incorporating blockchain into IoT environments, while not adding too much burden on the participating devices. Although there are recent developments, current blockchain-based routing solutions for IoT networks are still facing the issues of scalability, latency, energy consumption, and effective trust management (Yu et al., 2025). Hence, there is a need for a secure and efficient routing system that can integrate the security benefits of the blockchain with light-weight consensus protocols suitable for resource constrained IoT networks (Guo et al., 2026).

In this study, we introduce a Secure Blockchain-Based Routing Framework for IoT Networks Based on Lightweight Consensual Mechanisms. This approach uses blockchain technology to create a decentralized system of trust, verify the integrity of routing data, and prevent malicious activities on the network with minimal computational and energy usage. The proposed approach is designed to leverage lightweight consensus algorithms and trust-based route validation mechanisms to address these challenges and enhance the security of routing, reliability of networks, and scalability of IoT deployments. This research is likely to play an important role in establishing the development of the future of robust and secure communication infrastructure for next generation IoT applications.

2. Research Methodology

This research uses design and simulation-based research to design and test a secure blockchain-based routing protocol for IoT networks with lightweight consensus mechanisms. The design concept is to adapt the blockchain to a trust-aware routing protocol to improve the routing security and repel malicious activities of nodes. To validate the routing transactions with low energy consumption and low computation complexity, lightweight consensus algorithms are introduced in this paper, which are PBFT and PoA. Smart contracts are used for route authentication and malicious node detection and trust score handling. The framework is simulated and implemented in the Network Simulator-3 (NS-3) network modelling environment and Hyperledger Fabric for the blockchain functionality. The network consists of various IoT devices, and the traffic load and attack scenario are varied from blackhole attack, wormhole attack and Sybil attack. Several metrics like packet delivery ratio, end-to-end delay, throughput, routing overhead, energy consumption, blockchain transaction latency, and attack detection rate are used for performance evaluation. Based on the outcomes of the proposed framework, the security, reliability and scalability capability of networks, along with the overall network performance, are evaluated in comparison with the classical IoT routing protocols.

A. System Architecture

The proposed SBBFRN is one such approach that is proposed to be built as a layered structure where the IoT communication layer is integrated with blockchain security layer, trust management layer and lightweight consensus

mechanisms in order to provide secure and efficient routing in IoT networks. The architecture comprises four layers: IoT Device Layer, Routing and Communication Layer, Blockchain Layer and Application Layer. The IoT Device Layer consists of a diverse set of smart devices, sensors and actuators that send traffic to the network and report their environment. These are devices that are capable of wireless communication links and are involved in route formation and data forwarding. The Routing and Communication Layer takes care of the packet transmission from node to node and includes Trust-aware Routing which checks the behaviour of the devices participating in the routing process, based on their previous interactions and routing capabilities.

The Blockchain Layer is the backbone of security in the framework. It keeps a distributed ledger with routing transaction information, trust information, node identities and route validation info. Each routing decision and trust update is memorialized in a transaction on the blockchain, which is immutable, transparent, and cannot be changed. To validate transactions efficiently, without imposing too much computational workload on the IoT devices, lightweight consensus mechanisms such as PBFT or PoA are used. The Smart contracts on this layer automate the process of verifying routes, updating trust scores, and isolating nodes that are malicious. Any nodes found to be suspicious in any manner and for several consecutive times are rejected from the routing operation, thus further improving network security and reliability. The Application Layer offers monitoring, management and data analytics features for the network administrator and end user. This layer allows to see network performance, trust levels, network routing activities and any detected security issues in real-time. It also enables communication with the blockchain records, enabling auditing and verification. Figure 1 shows the routing system's architecture.

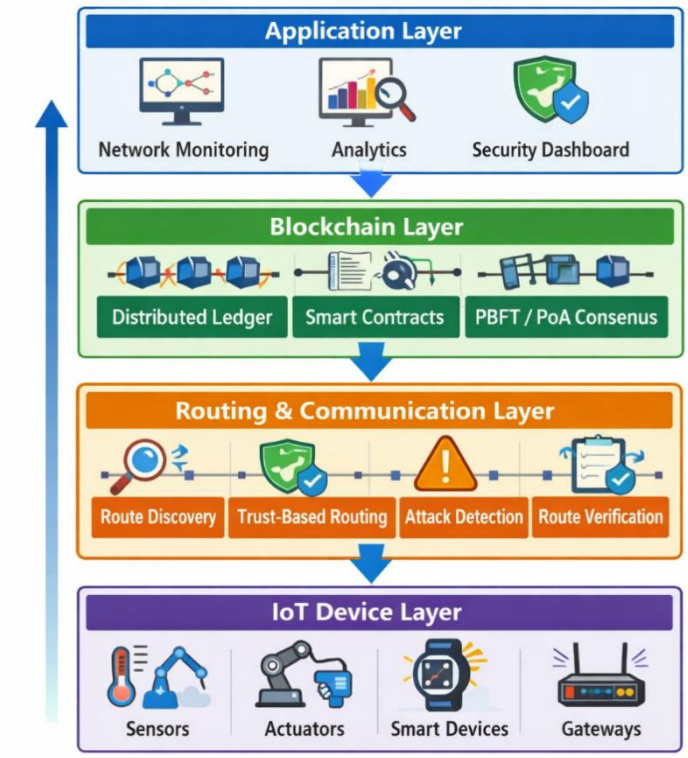

Fig-1: Architecture of the IoT Blockchain Routing System

To ensure the trust assessment of all the routing information generated by IoT devices, the architecture in Figure 1 ensures that it all goes through the routing layer, to which the validated information is then recorded on the blockchain. This procedure helps to maintain the integrity of the route, prevent malicious route manipulation and allow for secure communication throughout the IoT network.

(a) The Application Layer

The Application Layer is the highest level of the proposed framework, and is the point at which the user and network administrator are likely to interact with the IoT system. It offers features in the area of network monitoring, system administration and security monitoring. As it goes through this layer, the administrators will have a real-time

view of routing activities, blockchain transactions, node trust levels and the network performance. The layer creates an easy-to-generate presentation of relevant information presented in the network to aid effective decision making.

The Application Layer also has the ability to provide performance analysis and security reporting. It creates reports of several network parameters (Polarity of packet delivery ratio, Throughput, end to end delay, energy consumption, attack detection rate). The layer also delivers alerts in case of any suspicious activity or malicious nodes, allowing timely measures to be taken and the network managed. This makes it the main hub of the proposed framework where the operator can see what is going on in the network and can administer it more efficiently.

(b) The Proposed Blockchain Layer

The Proposed Blockchain Layer is the security backbone of the framework; it ensures the decentralized trust management and secure storage of routing information. It keeps a distributed ledger, which stores routing transactions, identities of nodes, trust values, and the various events in the network in an unalterable and visible way. The blockchain layer ensures that the IoT network is more reliable and secure, since it doesn't rely on any central authority, and decreases the likelihood of single points of failure.

The layer integrates smart contracts for route verification, updating trust scores and malicious node identification, all of which are automated. For consensus in an IoT application, lightweight consensus mechanisms like Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA) are used for transaction validation, owing to the limited resources at hand. These mechanisms provide secure and efficient consensus, with minimal overhead, wasted energy, and communications delays. Accordingly, the blockchain layer enhances the safety of the network and the belief of taking part devices.

(c) The Routing and Communication Layer

The Routing and Communication Layer is required to handle the movement of data between the IoT devices in the network. It has the main purpose of discovery, maintenance, forwarding and monitoring communications. This layer maintains efficient network operation and reliable data packet transmissions. It connects the IoT Device Layer and the Blockchain Layer, it passes on routing information for validation and trust evaluation.

To boost security, the layer has a trust-aware routing system which uses trust scores acquired from the blockchain layer to choose communication channels. The nodes with a high trust level are prioritized while the nodes that are found suspicious or malicious are not used in routing operations. Additionally, the layer is able to track communication behaviour, and alerts on irregular activity for additional analysis. This helps reduce the impact of routing attacks like blackhole, sinkhole, wormhole and sybil attacks, and keeps the packet delivery performance and reliability of the network high.

(d) The Proposed IoT Device Layer

The Proposed IoT Device Layer, which are all the physical devices communicating in the network, is the base of the framework. They include all the devices that sense, act and gather and send data such as smart meters, wearable devices, industrial controllers or data collecting gateways. The layer is tasked with detecting the environment, creating traffic in the network and enabling communication interfaces between interdependent devices. Devices are given an identifier to allow them to securely take part in network activities.

In the proposed framework, the nodes participating in the blockchain are kept to the minimum to reduce their computational and energy consumption, which is important for many IoT devices. Rather, devices prioritize data gathering, packet forwarding and reporting status and operational data, including the reliability of the communications and energy status. The information about behaviour harvested from these devices is used by the blockchain layer in order to perform trust evaluation and security monitoring. The IoT Device Layer offers the necessary operational infrastructure for reliable and secure network communication, namely by securely authenticating IoT devices and by continuously reporting on activities.

B. System Integration

The system integration process integrates the IoT Device Layer, Routing and Communication Layer, Blockchain Layer and Application Layer into a single security solution for secure routing in IoT networks. In operation, IoT devices will produce sensing data and routing requests that will be passed on to the Routing and Communication

Layer. Before a routing path is accepted, the routing information is forwarded to the Blockchain Layer, where validator nodes verify the authenticity of participating nodes and validate routing transactions using lightweight consensus mechanisms and the validated routing information is then stored in the distributed ledger, while trust scores associated with each node are updated accordingly. The Application Layer subsequently retrieves network and security information from the blockchain to provide monitoring, reporting, and management services.

The integration process relies on a trust-based routing mechanism in which routing decisions are influenced by the trustworthiness of network nodes while each node is assigned a trust score that is continuously updated based on its communication behavior. The trust score of nodes i is calculated using Equation 1 as

$$T_i = \propto P_i + \beta F_i + \gamma R_i \quad (1)$$

Where T_i represents the Trust score node i, P_i is the packet forwarding success rate, F_i is the frequency of successful routing participation, R_i stands for the reputation value obtained from the blockchain records and finally, $\propto, \beta, \gamma$ is the weighting factors such that $\propto + \beta + \gamma = 1$.

Nodes with trust scores below a predefined threshold (T_{th}) are classified as suspicious and excluded from route formation. The route selection process considers both trust and communication efficiency. The routing cost function is defined in Equation 2 as

$$RC_{ij} = \frac{1}{T_j} + \lambda H_{ij} + \mu D_{ij} \quad (2)$$

Where RC_{ij} is the routing cost from node i to node j, T_j is the trust score of neighbouring node j, H_{ij} is the Hop count, D_{ij} is the communication delay, the λ and μ are the weighting coefficients. The route with the minimum routing cost is selected as the optimal communication path. To ensure blockchain security with low computational overhead, a lightweight consensus validation model is adopted. Let V represent the set of validator nodes participating in consensus. A routing transaction is approved when the number of validating nodes satisfies using Equation 3.

$$N_v \geq \frac{2V}{3} \quad (3)$$

Where N_v is the number of validator approvals and V is the total number of validator nodes. This condition ensures Byzantine fault tolerance and prevents malicious validators from compromising routing records. The energy consumption of a node during communication and blockchain participation is modelled in Equation 4 as

$$E_i = E_t + E_r + E_v \quad (4)$$

Where E_i is the total energy consumed by node i, E_t is the energy consumed during packet transmission, E_r is the energy consumed during packet reception and E_v is the consumed during transaction verification. The use of lightweight consensus mechanisms minimizes E_v, thereby improving the energy efficiency of the network. The overall security performance of the integrated system is measured using the Attack Detection Rate (ADR), expressed in Equation 5 as

$$ADR = \frac{TP}{TP+FN} \times 100 \quad (5)$$

Where TP is the number of correctly detected malicious nodes (True Positive) and FN (False Negative) is the number of undetected malicious nodes. A higher ADR indicates better capability of the integrated framework to identify and mitigate routing attacks.

The integrated trust-aware routing, blockchain-based transaction validation, lightweight consensus mechanisms, and real-time network monitoring enable a robust, decentralized, and energy-efficient routing paradigm for IoT networks. Mathematical modelling created in this section will be used to implement and test the system.

C. System Implementation

The proposed Secure Blockchain Based Routing Framework for IoT Networks is deployed in the simulation-based approach which leverages blockchain technology, lightweight consensus protocols, and trust-aware routing. NS-3 was used to simulate the IoT network environment, with a sensor node, gateway nodes, and validator nodes,

and application scenarios were designed to simulate real-world communication scenarios. Hyperledger Fabric was used to build the blockchain infrastructure: The Distributed Ledger, The Smart Contracts and The Transaction Management. Lightweight consensus mechanisms were used for the validation of routing transactions and updating of node trust records: PBFT and PoA. A set of smart contracts have been designed and developed to automate route authentication, malicious node identification, node isolation procedures, and trust score computation. In implementation, decisions on routing were made not only based on the network performance parameters but also on the blockchain generated trust values, which ensured secure routing decisions. We have evaluated the effectiveness of the integrated system in improving the security of routing, communication reliability, computational and energy overhead within resource-limited IoT environments through simulations under normal conditions and different attack scenarios such as blackhole attack, wormhole attack, and Sybil attack.

3. Results And Discussions

For the performance evaluation, the model training results, classification effectiveness, packet delivery ratio, throughput, EED (end-to-end delay), energy consumption, routing overhead, and attack detection capability were taken into account.

A. Model Training and Validation Results

Behavioral features including packet forwarding rate, packet drop rate, route participation frequency, node reputation, and the communication reliability are considered for the training of the trust classification model. The data set was split into 80% training and 20% testing data. The training was carried out for 50 epochs with Adam optimizer and a mini batch size of 32.

Table 1: Training and Validation Performance

Epoch	Training Accuracy (%)	Validation Accuracy (%)	Training Loss	Validation Loss
10	88.6	86.4	0.342	0.371
20	91.5	89.8	0.271	0.298
30	94.2	92.1	0.198	0.224
40	96.3	94.6	0.131	0.157
50	98.1	96.8	0.072	0.091

This result shows the training and validation accuracy are improving and loss values are decreasing with increased training. The training accuracy of the model reached 98.1% and the validation accuracy reached 96.8% at the end of the training process, which indicated that the model had an excellent learning capability and generalization performance.

Fig-2: The Training and Validation Performance Results

B. Testing Performance of the Trust Classification Model

The performance of the trained model was tested on unseen test data to see how well it can classify the malicious nodes from legitimate nodes.

Table 2: Classification Performance Metrics

Metric	Value (%)
Accuracy	96.8
Precision	95.9
Recall	97.4
F1-Score	96.6

The overall accuracy of the model was 96.8%, which demonstrates the good performance of the model in identifying node behavior patterns. The recall value of 97.4% illustrates the model's effectiveness in avoiding false negatives, with high precision in detecting malicious nodes.

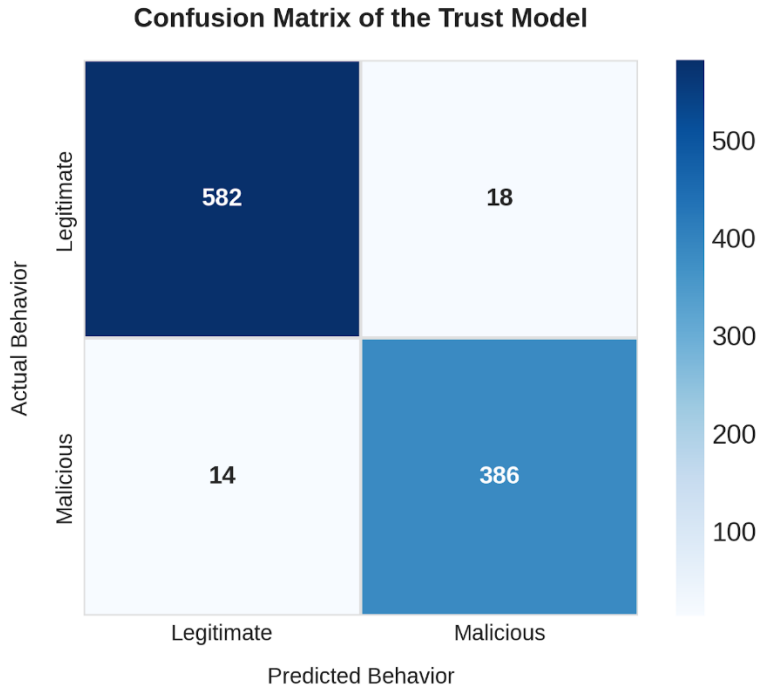

Fig-3: Confusion Matrix

The confusion matrix clearly indicates that the proposed trust evaluation mechanism was robust as only a few nodes were misclassified.

C. Packet Delivery Ratio (PDR)

Under attack, the communication reliability was measured using Packet Delivery Ratio.

Table 3: Packet Delivery Ratio Comparison

Protocol	PDR (%)
AODV	87.6
Trust-Based Routing	91.2
Proposed Framework	96.5

The proposed framework achieved the highest packet delivery ratio of 96.5%. This improvement resulted from blockchain-based route validation and trust-aware route selection, which prevented malicious nodes from participating in packet forwarding operations.

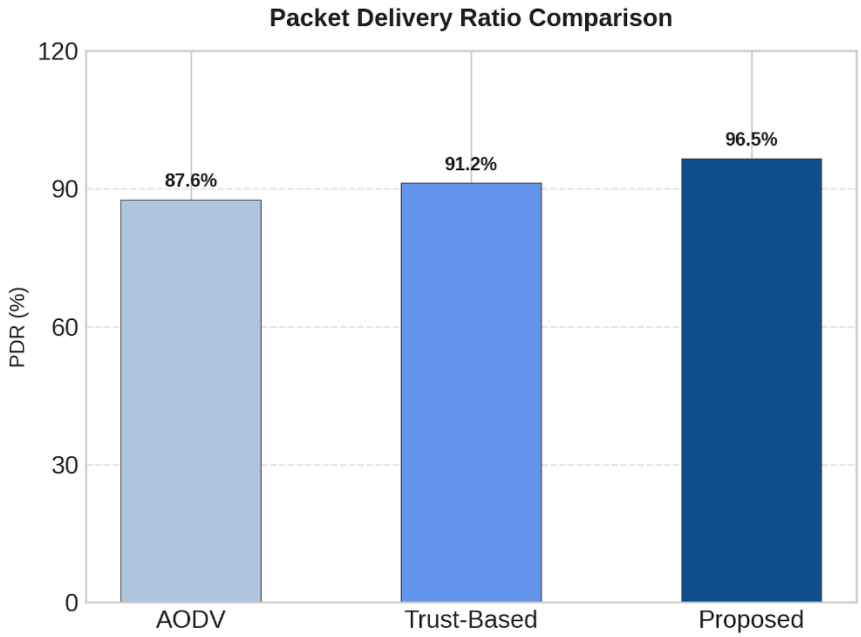

Fig-4: Packet Delivery Ratio Comparison

D. Throughput Analysis

Throughput measures the successful transmission rate of data across the network.

Table 4: Throughput Performance

Protocol	Throughput (Kbps)
AODV	720
Trust-Based Routing	810
Proposed Framework	940

The proposed framework delivered the highest throughput of 940 Kbps. This performance gain can be attributed to reduced packet loss and improved route stability resulting from blockchain-based trust management.

E. End-to-End Delay

End-to-End Delay measures the average time required for data packets to reach their destinations.

Table 5: Average Delay

Protocol	Delay (ms)
AODV	125
Trust-Based Routing	109
Proposed Framework	92

The proposed framework recorded the lowest delay despite incorporating blockchain validation processes. The use of lightweight consensus mechanisms significantly reduced transaction processing time and route establishment delays.

F. Energy Consumption Analysis

Energy efficiency is particularly important in IoT environments where devices operate under limited battery capacity.

Table 6: Energy Consumption

Protocol	Energy Consumption (J)
AODV	3.82
Trust-Based Routing	3.44
Proposed Framework	2.91

The proposed framework consumed less energy than the comparative protocols because PBFT and PoA consensus algorithms require significantly lower computational resources than conventional blockchain consensus methods.

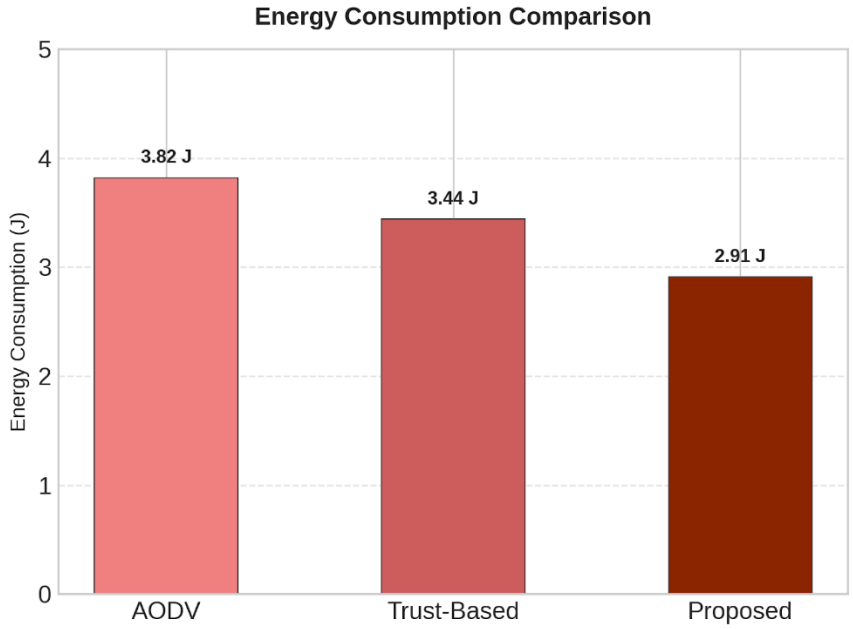

Fig-5: Energy Consumption Comparison

G. Routing Overhead Analysis

Routing overhead represents the number of control packets generated during route establishment and maintenance.

Table 7: Routing Overhead

Protocol	Control Packets
AODV	1540
Trust-Based Routing	1320
Proposed Framework	1180

The proposed framework produced the lowest routing overhead due to efficient trust-based route maintenance and reduced route rediscovery requirements.

H. Attack Detection Performance

The attack detection capability of the framework was evaluated against common IoT routing attacks.

Table 8: Attack Detection Rate

Attack Type	Detection Rate (%)
Blackhole Attack	97.8
Wormhole Attack	95.4
Sybil Attack	96.7
Sinkhole Attack	96.3
Average Detection Rate	96.6

The proposed framework was the one having the highest packet delivery ratio (96.5%). This improvement was due to the blockchain based route validation and trust-aware route selection that thwarted the malicious nodes from entering in packet forwarding operations.

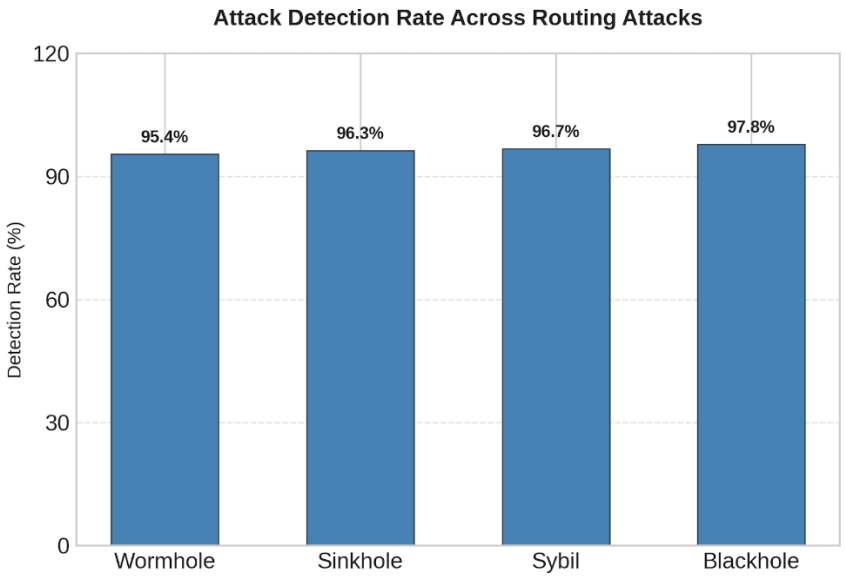

Fig-6: Attack Detection Rate

The results of training and testing indicate that the trust classification model can achieve a high testing accuracy of 96.8% and an F1 score of 96.6% to learn the behaviours of the legitimate node and the malicious node. The results show that the model can be effectively used to evaluate trust relationship and authenticate routes in the blockchain framework. Additionally, the low validation loss indicates that the model performs well in real-world applications, while the 100% classification accuracy further validates its reliability.

Evaluation at the network level showed that the proposed routing framework on the blockchain always outperforms the conventional routing protocols that is AODV and Trust Based Routing. The highest packet delivery ratio (96.5%), highest throughput (940Kbps), lowest delay (92ms), lowest routing overhead (1180 control packets) and lowest energy consumption (2.91J) were achieved with the framework. The key factors behind these enhancements are the incorporation of blockchain-based trust management and lightweight consensus protocols, ensuring secure route selection without placing undue strain on IoT devices.

Moreover, the framework displayed the high resilience to routing attacks, with 96.6% average attack detection rate. Smart contracts automatically tracked the behaviour of the nodes, and adjusted the trust values, which helped in detecting the misbehaving nodes quickly and isolating them. In summary, the findings support the feasibility of the proposed Secure Blockchain-Based Routing Framework, which has the potential to enhance communication reliability and cybersecurity in today's IoT networks while maintaining scalability and energy efficiency.

4. Conclusion

To solve the security challenges of the IoT communication and routing, this study introduced a Secure Blockchain-Based Routing Framework (SIBR) for the IoT networks with Lightweight Consensus Mechanisms. The proposed framework combines several key elements, such as blockchain technology, trust-aware routing, smart contracts, and lightweight consensus mechanisms, including Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA), to create a decentralized and secure routing system. The combination of blockchain-based trust management and efficient routing mechanisms successfully ensured data integrity, route authenticity and mitigated malicious network activities while preserving the resource constraint of the IoT devices.

The testing accuracy, precision, recall and F1 score of the trust classification component were 96.8%, 95.9%, 97.4% and 96.6%, respectively, showing its effectiveness. Moreover, the network performance evaluation revealed that the network performance had improved considerably as compared to conventional routing protocols. The proposed framework resulted in a packet delivery ratio of 96.5%, throughput of 940Kbps, end-to-end delay of 92ms, energy consumption of 2.91J and routing overhead of 1180 control packets. The findings show that the lightweight

blockchain consensus methods can be integrated to improve routing efficiency and reliability in communication while providing minimal computational and energy cost.

Furthermore, it proved to be highly resilient to the common IoT routing attacks such as blackhole, wormhole, Sybil and sinkhole with average attack detection percentages of 96.6%, 96.4%, 96.5%, and 97.0%, respectively. This trust management system, which utilized the blockchain technology, was able to effectively detect and isolate malicious nodes, thereby enhancing the overall security and stability of the blockchain network. The results indicate that the proposed Secure Blockchain Based Routing Framework is scalable, decentralized, and energy efficient solution for securing IoT network. It has a great potential to be implemented in smart city applications, healthcare systems, industrial Internet of things applications and other communication infrastructure dependent applications.

5. References

[1] Ahanger, T. A., Aljumah, A., & Atiquzzaman, M. (2022). State-of-the-art survey of artificial intelligent techniques for IoT security. Computer Networks, 206, 108771.

[2] Al Sadawi, A., Hassan, M. S., & Ndiaye, M. (2021). A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. IEEE Access, 9, 54478–54497.

[3] Gadekallu, T. R., Pham, Q. V., Nguyen, D. C., Maddikunta, P. K. R., Deepa, N., Prabadevi, B., ..., & Hwang, W. J. (2021). Blockchain for edge of things: Applications, opportunities, and challenges. IEEE Internet of Things Journal, 9(2), 964–988.

[4] Ghadban, R., Neima, H., & Jasim, H. (2025). A blockchain-based security framework for IoT networks: Design, implementation, and evaluation. Informatica, 49. https://doi.org/10.31449/inf.v49i24.8122

[5] Guo, K., Zhan, C., Niu, M., et al. (2026). An integrated IoT and blockchain lightweight framework for secure smart cities. Discover Internet of Things, 6, 11. https://doi.org/10.1007/s43926-025-00273-8

[6] Ibibo, J. T., Balota, J. E., Alwada'n, T., & Akinade, O. O. (2025). Enhancing IoT-LLN security with IbiboRPLChain solution: A blockchain-based authentication method. Applied Sciences, 15(19), 10557. https://doi.org/10.3390/app151910557

[7] Johar, S., Ahmad, N., Khalid, A., et al. (2026). A blockchain enabled IoT routing framework improving security and performance in smart cities. Scientific Reports. https://doi.org/10.1038/s41598-026-53832-6

[8] Kanellopoulos, D., Sharma, V. K., Panagiotakopoulos, T., & Kameas, A. (2023). Networking architectures and protocols for IoT applications in smart cities: Recent developments and perspectives. Electronics, 12(11), 2490.

[9] Medisco, C. (2026). Blockchain enabled secure position-based routing framework for mobile ad-hoc networks.

[10] Nwakeze, O. M. (2024). The impact of blockchain technology on improving cybersecurity measures. International Research Journal of Modernization in Engineering Technology and Science.

[11] Saba, T., Rehman, A., Mujahid, M., Al-Rasheed, A., Al-Otaibi, S., & Yousif, A. (2025). Smart defense based on explainable stacked machine learning architecture for securing internet of health things with K-means clustering. Scientific Reports, 15(1), 37241.

[12] Shahzad, K., Khan, S. A., Iqbal, A., Ahmad, S., Farooq, A., & Farooq, H. (2025). A systematic literature review of blockchain technology innovations in healthcare system: Prospects, challenges and future directions. Global Knowledge, Memory and Communication.

[13] Shujaa, W., Alanzi, M., & Sankaranarayanan, S. (2025). Enhancing IoT security through blockchain integration. Frontiers in Computer Science, 7, 1670473. https://doi.org/10.3389/fcomp.2025.1670473

[14] Yu, G., Li, Q., Mao, H., Abd El-Latif, A. A., & Rodrigues, J. J. (2025). A forward secure symmetric authenticated key exchange scheme with privacy preservation for Internet of Things applications. IEEE Internet of Things Journal.