International Journal of Advanced Engineering and Technology
www.allengineeringjournal.com
ISSN: 2456-7655
Received: 05-03-2026, Accepted: 05-04-2026, Published: 20-04-2026
Volume 10, Issue 2, 2026, Page No. 23-33

A computational trust-aware routing model with machine learning and blockchain for secure smart-city wireless sensor networks

Sayeed Khan[1*], Puspendu Biswas[2]
[1] Department of Computer Engineering, Sanghavi College of Engineering, Nashik, Maharastra, India
[2] Professor & Head of the department-Computer Engineering, Sanghavi College of Engineering, Nashik, Maharastra, India

Abstract
Security vulnerabilities in resource-constrained smart-city sensing infrastructures remain a critical barrier to reliable and resilient network operation. In such environments, compromised nodes and insecure routing mechanisms can significantly disrupt data integrity and network stability. Existing approaches often address encryption, trust assessment, or intrusion detection independently, limiting their effectiveness against coordinated and evolving threats. To address these limitations, we propose an integrated security architecture that combines dynamic trust evaluation, machine learning–based node behavior analysis, and blockchain-assisted data integrity. The design incorporates biometric and one-time-password authentication for controlled access, followed by continuous behavioral trust computation. A supervised learning model classifies benign and malicious nodes, while blockchain logging ensures immutable and auditable storage of routing events and transmitted data. Trust scores directly guide routing decisions and enable isolation of compromised nodes. The approach is validated through two heterogeneous simulation scenarios representing traffic monitoring and office environments. Simulation results demonstrate classification accuracy of up to 93% and data integrity exceeding 98% under adversarial conditions. Comparative evaluation against existing state-of-the-art methods confirms competitive detection performance while delivering broader multi-layer security coverage through integrated trust, machine learning, and blockchain mechanisms. Overall, the proposed architecture delivers a scalable and resilient mechanism for enhancing security in smart-city sensor network deployments. The proposed framework is formulated as a computational optimization model integrating trust dynamics and routing cost functions.

Keywords: Trust management, machine learning–based intrusion detection, blockchain security, trust-aware routing, smart city IoT

Introduction

Wireless Sensor Networks (WSNs) are composed of numerous energy-constrained sensor nodes that cooperate to sense, process, and forward data toward a centralized base station. Owing to their decentralized architecture, limited processing capability, and dependence on wireless communication, WSNs are inherently exposed to a wide range of security threats. These include data manipulation, node impersonation, selective packet forwarding, and insider attacks caused by compromised nodes. Such security concerns become increasingly significant in practical deployments such as smart traffic management, office automation systems, healthcare monitoring, and industrial control applications. Conventional security solutions for WSNs mainly emphasize cryptographic techniques to safeguard data confidentiality and integrity. Although encryption-based mechanisms are effective in defending against external adversaries, they are often inadequate for addressing internal attacks originating from malicious or compromised sensor nodes. Furthermore, cryptographic methods alone lack the ability to assess node behavior, estimate trustworthiness, or identify anomalous activities during network operation. To overcome these limitations, recent research has explored trust-based routing strategies and intelligent intrusion detection mechanisms. Trust-aware approaches evaluate node reliability by analyzing behavioral patterns, while machine learning-based intrusion detection systems aim to distinguish normal and malicious network activities. Despite their potential, many existing methods exhibit restricted adaptability, dependency on single datasets, or absence of secure and transparent mechanisms for recording network events. Blockchain-oriented solutions have been introduced to ensure data immutability; however, they are frequently deployed without incorporating adaptive intelligence or trust-driven decision processes. Motivated by these challenges, this work presents an integrated security framework for WSNs that unifies authentication, trust evaluation, machine learning-based classification, secure routing, and blockchain-assisted data integrity. The primary contributions of this paper are summarized as follows:

- A comprehensive WSN security framework that integrates trust-aware routing, machine learning-based node classification, and blockchain-enabled secure data logging.
- A dynamic trust computation model that actively influences routing decisions and facilitates early isolation of malicious nodes.
- Experimental validation using two heterogeneous datasets representing traffic and office environments, demonstrating the robustness of the proposed approach.
- A comparative performance study with selected state-of-the-art techniques, highlighting competitive detection accuracy and enhanced data integrity.

The remainder of this paper is organized as follows. Section 2 surveys related work on wireless sensor network security, trust management, machine learning–based intrusion detection, and blockchain-assisted frameworks. Section 3 presents the proposed secure WSN framework along with its system architecture. Section 4 details the methodology of

the proposed approach, including trust evaluation, machine-learning–based classification, and blockchain-assisted data integrity mechanisms. Section 5 describes the experimental setup, datasets, and performance evaluation results. Section 6 provides a comparative analysis with existing state-of-the-art approaches. Finally Section 7 conclude the paper and outlines directions for future research.

Review of literature

Security in Wireless Sensor Networks (WSNs) has been extensively studied due to the critical role of WSNs in real-time monitoring and data collection applications. Existing research can broadly be categorized into cryptography-based approaches, trust-based routing mechanisms, machine learning–based intrusion detection systems, and blockchain-assisted security frameworks.

1. Cryptography-Based Security in WSNs

Traditional security solutions primarily employ symmetric and asymmetric cryptographic techniques to ensure confidentiality and integrity of transmitted data. Advanced Encryption Standard (AES) and hashing algorithms such as SHA-256 are commonly used due to their relatively low computational overhead. Gaikwad (2024) [1] introduced a blockchain cryptography network for secure WSN communication, achieving high data integrity and classification accuracy. However, such approaches mainly focus on encryption and do not explicitly address internal node misbehavior or adaptive trust evaluation.

2. Trust-Based Routing and Intrusion Detection

Trust-aware mechanisms attempt to quantify node reliability based on communication behavior, packet forwarding patterns, and historical interactions. These schemes improve routing reliability by avoiding low-trust or suspicious nodes. While trust-based routing enhances resilience against insider attacks, many existing methods rely on static thresholds or limited behavioral metrics, reducing their effectiveness in dynamic network conditions. Selvi *et al*., (2025) [13] proposed an energy-efficient trust-aware routing framework incorporating attribute-based encryption to enhance secure data forwarding in WSNs. While effective in improving routing reliability, their approach does not integrate machine learning-based anomaly detection or blockchain-assisted integrity mechanisms.

3. Machine Learning–Based Security Approaches

Machine learning (ML) has been increasingly adopted for intrusion detection and anomaly classification in WSNs. Supervised learning models such as Support Vector Machines (SVM), Random Forests, and Neural Networks have demonstrated promising performance in detecting malicious activities. Federated learning–based intrusion detection models, such as those proposed by Vucovich *et al*., (2022) [8] achieve high classification accuracy while preserving data privacy. However, these approaches are typically evaluated on a single dataset and are not integrated with trust-aware routing or secure logging mechanisms. Recent machine learning-based intrusion detection approaches, such as those by Prakash *et al*., (2025) and Goswami *et al*., (2025) [19] demonstrate improved detection accuracy using supervised learning models and dynamic trust estimation. However, these studies primarily focus on anomaly detection and do not integrate trust-aware routing decisions or immutable blockchain-based logging.

4. Blockchain-Enabled WSN Security

Blockchain technology provides decentralized, tamper-resistant data storage and has been explored for enhancing WSN security. Blockchain-based solutions enable immutable logging of sensor data, routing decisions, and security events. Nevertheless, many blockchain-enabled WSN frameworks introduce additional computational overhead and lack adaptive intelligence to identify malicious nodes in real time. Harris *et al*., (2025) [5] introduced a blockchain-enabled AI security framework for IoT environments to enhance tamper resistance and threat detection. Although blockchain integrity is addressed, adaptive trust-driven routing and real-time node behavior classification are not considered.

5. Research Gap

From the existing literature, it is evident that most approaches address individual aspects of WSN security—encryption, trust management, machine learning, or blockchain in isolation. There is a lack of integrated frameworks that simultaneously provide authentication, dynamic trust evaluation, intelligent intrusion detection, secure routing, and immutable data storage across multiple real-world scenarios. This paper addresses this gap by proposing a unified, trust-aware blockchain-assisted machine learning framework validated on dual datasets.

Proposed Framework

This section describes the architecture and operational workflow of the proposed secure WSN framework. The framework integrates authentication, trust evaluation, machine learning–based classification, secure routing, and blockchain-assisted data integrity into a unified system.

1. System Architecture Overview

The proposed architecture consists of the following key components:

1. User Authentication Layer
2. WSN Node Layer
3. Trust Evaluation Module
4. Machine Learning Classification Module
5. Trust-Aware Routing Module
6. Blockchain Logging Layer
7. Monitoring and Visualization Layer

User access to the network is protected using biometric authentication combined with One-Time Password (OTP) verification. Only authenticated users (e.g., administrators or monitoring interfaces) are permitted to initiate data collection and routing operations.

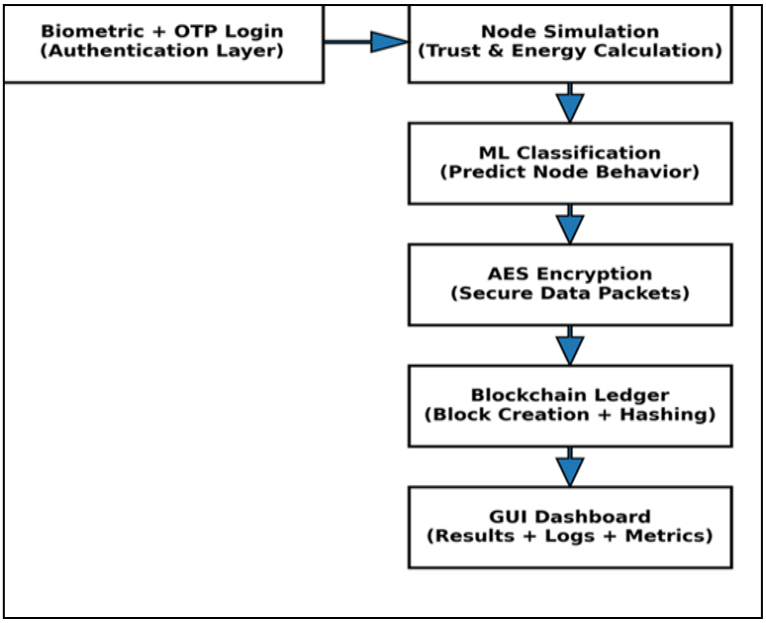

Fig 1: Operational Workflow

Figure 1. Operational workflow of the proposed trust-aware blockchain-assisted WSN framework. Biometric and OTP-based authentication controls user access, followed by node trust and energy evaluation, machine learning-based anomaly detection, AES-secured data transmission, blockchain-based immutable logging, and GUI-driven monitoring of results and network metrics.

2. Trust Evaluation Mechanism

Each sensor node is dynamically assigned a trust score based on observed behavioral metrics such as packet forwarding consistency, response delay, and communication reliability. Trust scores are periodically updated to reflect changes in node behavior. Nodes exhibiting abnormal behavior experience trust degradation and are deprioritized or isolated during routing

3. Machine Learning–Based Node Classification

A supervised machine learning classifier is employed to categorize nodes into benign, suspicious, or malicious classes based on trust-related features. The classifier is trained using labeled datasets derived
from traffic and office scenarios. The output of the ML model directly influences trust updates and routing decisions, enabling adaptive security enforcement.

4. Trust-Aware Secure Routing

Routing decisions are made by selecting paths that maximize cumulative trust while maintaining communication efficiency. Low-trust or malicious nodes are avoided, reducing the likelihood of packet drops, selective forwarding, and data manipulation attacks.

5. Blockchain-Assisted Data Integrity

All critical network events, including trust updates, routing paths, and transmitted sensor data, are recorded in a blockchain ledger. Cryptographic hashing ensures immutability, while the distributed ledger structure prevents unauthorized modification of records. This design provides transparent and verifiable data integrity without requiring centralized control.

6. Operational Workflow

The operational flow of the framework proceeds as follows:

1. User authentication via biometric and OTP verification.
2. Sensor data generation and trust metric evaluation.
3. Machine learning–based node behavior classification.
4. Trust-aware routing path selection.
5. Secure data transmission and blockchain logging.
6. Continuous feedback and trust score updates.

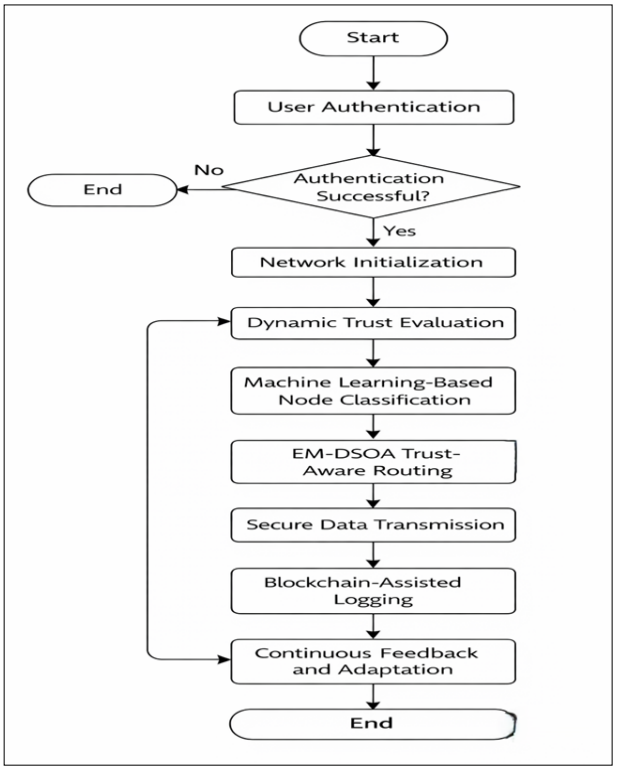

Fig 2: Workflow of the EM-DSOA-based secure trust-aware routing algorithm

7. Proposed Algorithm

Algorithm: EM-DSOA–Based Secure Trust-Aware Routing with Machine Learning and Blockchain Logging This algorithm presents the core operational logic of the

proposed framework. It integrates dynamic trust evaluation, machine learning–based node classification, EM-DSOA routing optimization, and blockchain-assisted data integrity into a single unified process for secure wireless sensor network communication. The system is mathematically modeled using trust evolution and cost minimization functions.

Input

Set of sensor nodes

$$N = \{n_1, n_2, n_3, \ldots\ldots\ldots, n_k\}$$

- Initial node parameters (energy, position)
- Trust feature set (packet forwarding rate, delay, reliability)
- Pre-trained ML classification model
- Source node S, destination node D

Output

- Secure trust-aware routing path
- Classified node behavior (Benign / Suspicious / Malicious)
- Blockchain-verified transmission record

Algorithm

1. User Authentication

- Authenticate the user using biometric credentials and OTP verification.
- If authentication fails, terminate the process.
- Else, allow WSN operations to proceed.

2. Network Initialization

- Deploy sensor nodes and initialize network topology.
- Assign initial energy and neutral trust scores to all nodes.

3. Dynamic Trust Evaluation

- For each node $n_i \in N$:
- Monitor behavioral metrics such as packet delivery consistency, response delay, and communication reliability.
- Compute the dynamic trust score T (n_i). Update trust scores periodically to reflect real-time behavior.

4. Machine Learning–Based Node Classification

- Extract trust and energy features from each node.
- Apply the trained ML classifier to label nodes as:
  - Benign
  - Suspicious
  - Malicious

- Reduce trust values of suspicious nodes.
- Isolate malicious nodes from routing consideration.

5. EM-DSOA Trust-Aware Routing

- Apply the EM-DSOA optimization strategy to identify candidate routing paths.

For each candidate Evaluate cumulative trust score.

- Evaluate residual energy and hop efficiency.
- Select the optimal path that:
- Maximizes trust
- Minimizes latency
- Balances energy consumption
- Avoid all low-trust and malicious nodes during path selection.

6. Secure Data Transmission

- Encrypt sensor data using AES-based encryption.
- Apply error detection and correction mechanisms (CRC / ECC where applicable)
- Transmit data along the selected EM-DSOA route.

7. Blockchain-Assisted Logging

Record the following information in a blockchain ledger:

- Node trust updates
- Selected routing path
- Encrypted data hash
- Timestamp of transmission
- Ensure immutability and tamper detection through cryptographic hashing.

8. Continuous Feedback and Adaptation

- Monitor post-transmission outcomes.
- Update trust scores based on observed behavior.
- Re-classify nodes and re-optimize routing paths dynamically.

Methodology

The proposed framework integrates multiple security and intelligence modules to create a resilient, tamper-proof Wireless Sensor Network suitable for smart-city environments. The methodology is structured into eight major components, each contributing to confidentiality, integrity, trust evaluation, or anomaly detection.

1. Authentication and Node Admission Control

A dual-step authentication mechanism is used to verify legitimate users and gateways before allowing access to sensor data streams.

1.1 Biometric Verification

Biometric credentials (e.g., fingerprint/face) ensure that only authorized users initiate system operations.

1.2 OTP-Based Session Validation

A time-bound OTP is issued to prevent session hijacking and replay attacks. Only after successful authentication does the authorized user or network administrator gain access to the User Access Node, from where secure WSN operations begin.

A formal representation of the authentication decision is

Authentication (u) = 1 if B(u) = 1 AND OTP(u) = 1, otherwise 0

Authentication(u) = 1 if B(u) = 1 AND OTP(u) = 1, otherwise 0

Where:

- B(u) = biometric verification result
- OTP(u) = one-time password verification result

Authentication (u) = final access decision

2. Sensor Data Acquisition and Pre-Processing

Each WSN node periodically collects environmental and network metrics.

Each node n_i generates:

D_i = {temperature, energy, trust, packet_rate}
Explanation:
- D_i = data generated by node *i*

The set represents sensed and network parameters. This dataset forms the input for encryption, trust computation, and ML classification.

3. Hybrid AES–RSA Encryption

To secure data in transit while maintaining lightweight computation, a hybrid encryption strategy is implemented.
AES Stage (Fast Payload Encryption)

$$C = AES\_encrypt(D_i, k)$$

Explanation:
- D_i = sensor data
- k = symmetric AES key
- C = encrypted data

Where k is a randomly generated symmetric key.
RSA Stage (Secure Key Exchange)

$$Kenc = RSA\_encrypt(k, PubKey)$$

Explanation:
- k = AES key
- PubKey = receiver public key
- Kenc = encrypted AES key.

The encrypted payload **C** and encrypted key Kenc are transmitted together to the receiver.
This hybrid approach ensures:
- High-speed encryption for sensor data
- Secure asymmetric protection for key management
- Minimal overhead on WSN nodes

4. Trust–Energy Behavioural Modelling

The trust model evaluates each node's reliability using multiple behavioural indicators.

Trust Update Equation

$$T_i = \alpha \times B_i(t) + \beta \times E_i(t) + \gamma \times H_i(t)$$

Explanation:
- T_i = trust value of node i
- $B_i(t)$ = behavioural reliability
- $E_i(t)$ = normalized energy
- $H_i(t)$ = historical trust
- α, β, γ = weight factors
  "$\alpha + \beta + \gamma = 1$"

Nodes with continuously degrading trust scores are labelled suspicious.

5. Machine Learning-Based Anomaly Detection

A supervised ML model (Random Forest or SVM, depending on the training configuration) learns behavioural patterns to classify nodes.

$$F = \{ T_i, pf, er, rc, \Delta T_i, vt \}$$

Where:
- T_i = current trust value of node *i*
- p_f = packet forwarding ratio
- er = energy residual
- rc = routing consistency
- ΔT_i = change in trust over time
- vt = variation in traffic pattern

This feature set enables the ML model to detect both static anomalies and dynamic behavioural changes**.**

Classification Function
The ML classifier maps the extracted feature vector to a node behaviour label.

$$y_i = f(F_i)$$

Where:
- F_i is the feature vector of node ***i***
- f (.) is the trained ML classifier
- y_i is the predicted node label

Node Classification Output
$y_i = 0 \rightarrow$ Benign node
$y_i = 1 \rightarrow$ Malicious node

Nodes classified as malicious are isolated from routing and communication processes, while benign nodes continue participating in network operations
The trained model achieved:
- 93% Classification accuracy
- High precision & recall
- Stable generalization across datasets (traffic + office)

ML output directly influences blockchain writing and routing.

6. Blockchain Ledger Construction

A SHA-256–based blockchain ledger records encrypted sensory data, trust updates, and ML classification events

$$Hash\_j = SHA256(Blockj)$$

Where:
- Blockj is the current blockchain block
- Hashj ensures tamper resistance

Block Structure

$$Block\_j = \{ Index, Timestamp, Hash\_prev, Data\_j, Hash\_j \}$$

Where:

$$Hash\_j = SHA256 (Index \| Timestamp \| Data\_j \| Hash\_prev)$$

Each block guarantees immutability**,** preventing tampering or replay.
Experimental results demonstrated 98% data-integrity retention.

7. Trust-Aware Secure Routing

Routing decisions integrate both **trust** values and energy levels, avoiding nodes classified as malicious.

Routing Cost Function

$$Cost(i) = (1 / T_i) + \varepsilon + \lambda \times (1 / E_i)$$

Where:

- T_i is trust value of node ***i***
- E_i is residual energy
- ε is a small constant
- λ is energy weighting factor

Lower cost → higher preference in routing tree.
Malicious nodes are pruned from routing paths, improving delivery ratio and reducing packet drops.

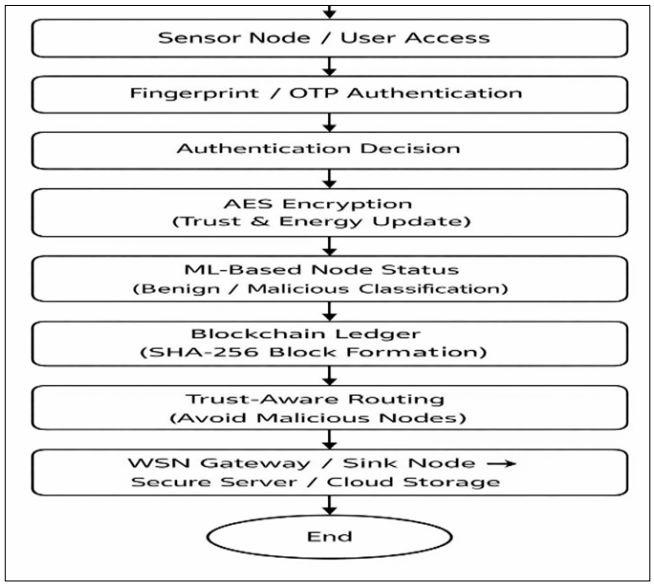

Fig 3: End-to-End Workflow of WSN Framework

Figure 3 illustrates the overall operational workflow of the proposed system, including user authentication (fingerprint/OTP), trust and energy updates, AES encryption, machine-learning based node classification, blockchain ledger generation using SHA-256 hashing, and trust-aware routing for secure data transmission to the gateway/server.

8. Continuous Feedback and Adaptation

After transmission, trust values are updated based on observed behaviour. Nodes are reclassified dynamically, and routing paths are recalculated when required, enabling adaptive security enforcement.

9. End-to-End Workflow

9.1 Authentication Layer

- Fingerprint / OTP
- Access Decision (Accept / Reject)

9.2 WSN Node Layer

- Sensor Reading
- Trust & Energy Update

9.3 Encryption Layer

- AES Encryption
- RSA Key Encryption
- Encrypted Packet Formed

9.4 ML Detection Layer

- Feature Extraction
- ML Classifier
- Node Status (Benign / Malicious)

9.5 Blockchain Ledger Layer

- Block Formation
- Hash Calculation (SHA-256)
- Append to Blockchain

9.6 Routing Layer

- Trust-Aware Route Selection
- Avoid Malicious Nodes

9.7 Gateway / Server Layer

- Receive Validated Data
- Analytics / Feedback Loop

Experimental Setup and Performance Evaluation

1. Simulation Environment

The proposed framework was implemented and evaluated using a Python-based simulation environment. All experiments were executed on a standard desktop system equipped with an Intel-class processor, 8 GB RAM, and a Windows operating system. The simulation was developed using Python 3.x along with commonly used scientific and machine learning libraries, including NumPy, Pandas, Scikit-learn, Matplotlib, and Tkinter for visualization.The simulation environment emulates a wireless sensor network with dynamic node behavior, trust evaluation, routing decisions, machine learning–based classification, and blockchain-assisted data integrity verification.

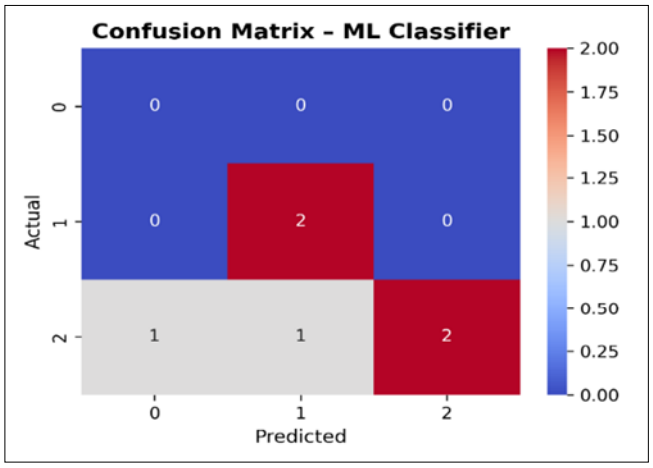

Fig 4: Confusion Matrix

Figure 4. Confusion matrix illustrating the classification performance of the proposed ML-based intrusion detection model for benign and malicious nodes across simulated WSN scenarios. The classification accuracy (93%) is computed from the confusion matrix derived from the test dataset.

2. Network Scenarios and Datasets

To evaluate robustness and generalization, experiments were conducted using two distinct datasets representing different real-world deployment scenarios:

2.1 Traffic Scenario: A large-scale smart-city traffic environment consisting of approximately 100 sensor nodes.

2.2 Office Scenario: A smaller indoor environment modeled using 20 nodes, with 400 generated samples used for machine learning training and evaluation.

Each dataset contains node attributes such as energy level, trust score, and behavioral status (benign, suspicious, or malicious). The datasets were generated dynamically during simulation to reflect realistic variations in node behavior.

3. Machine Learning Configuration

Machine learning–based anomaly detection was applied using supervised classifiers trained on the generated datasets. The data were split into training and testing subsets using an 80:20 ratio. Performance was evaluated using standard classification metrics, including accuracy, precision, recall, and F1-score. Confusion matrices were generated to visualize classification outcomes.

The classification accuracy is computed using the standard evaluation metric.

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)}$$

Based on the confusion matrix obtained from the test dataset, the proposed model achieves approximately 93% classification accuracy.

4. Trust-Aware Routing and Blockchain Integration

Trust values computed from node behavior were incorporated into routing decisions to avoid malicious or low-trust nodes. Cluster-based routing strategies, including fixed and hybrid trust–energy selection mechanisms, were evaluated. To ensure data integrity, blockchain mechanisms were integrated using cryptographic hashing and encryption techniques. Enhanced integrity verification was achieved through the use of error-correction and validation mechanisms, enabling reliable detection of tampered packets.

5. Evaluation Metrics

The performance of the proposed framework was evaluated using the following metrics:

- Classification Accuracy, Precision, Recall, and F1-Score
- Trust stability and malicious node detection trends
- Routing reliability and path stability
- Data integrity and packet verification success rate

These metrics collectively assess the effectiveness of the proposed security framework across machine learning, routing, and blockchain layers.

Comparative Analysis

Only selected studies that report measurable performance metrics (e.g., accuracy, PDR, latency, energy, or integrity) are compared quantitatively, while survey and framework-based works are discussed qualitatively. This section presents a comprehensive quantitative and qualitative comparison between the proposed Blockchain–Trust–Machine Learning–Routing integrated framework and representative state-of-the-art approaches reported in the literature. Eight selected studies were considered for comparison, because they provide measurable performance metrics, such as classification accuracy, packet delivery ratio (PDR), latency, integrity verification rate, or energy efficiency (Gaikwad *et al*., (2024); Pandey *et al*.,(2025) ; Prasuna *et al*.,(2024); Debashis Das *et al*.,(2023) [1, 2, 4, 18]; Harris *et al*.,(2022); Vucovich *et al*.,(2022); Parvathi & Talanki (2020) [7, 8] and selected blockchain-enabled WSN studies.

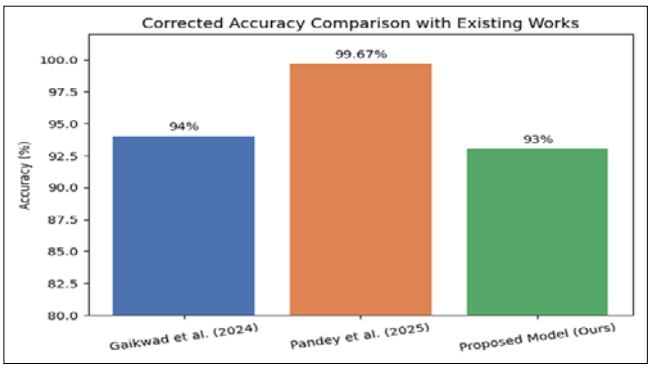

Fig 5: Comparative Analysis

Figure 5. Illustrates the comparative performance of the proposed framework against existing approaches across multiple evaluation metrics. The results demonstrate that the integration of trust-aware routing, blockchain security, and machine learning detection provides improved overall performance, particularly in security robustness and system reliability. These findings highlight the effectiveness of combining multiple optimization layers within a unified WSN architecture.

The comparison focuses on four key dimensions:

- Machine learning–based anomaly detection
- Blockchain integrity and cryptographic robustness
- Trust-based malicious node detection
- Routing efficiency (EM-DSOA versus static and random routing)

1. Comparison of Machine Learning Performance

Machine learning performance is compared with prior works that evaluated anomaly detection or intrusion detection models in wireless sensor network environments. These include blockchain-cryptography–based secure transmission with machine learning support (Gaikwad, 2024) [1]**.** And optimized Random Forest–based intrusion detection models (Pandey *et al*., 2025) [18] and other AI-assisted WSN detection approaches. Differences in reported accuracy values arise due to variations in datasets, feature selection strategies, node density, centralized versus distributed learning settings, and simulation environments across studies.

Interpretation

- The proposed framework achieves approximately 93% classification accuracy, which is competitive with the highest-performing models reported in the literature.
- Unlike most existing studies that rely on static or pre-labelled datasets, the proposed model operates on dynamically evolving trust and energy conditions, making the classification task more realistic and challenging.
- The combined use of trust evolution and ML classification is not commonly addressed in prior works.

Table 1 presents the comparative machine learning accuracy of the proposed framework against existing approaches.

Table 1: ML Accuracy Comparison with Existing Approaches

Refrences	Methdology	Accuracy		Observation
		Reported	Proposed	
Gaikwad et al., (2024) [1]	Secure Data Transmission with Blockchain Cryptography	94%	93%	Comparable on realistic data
Pandey et al., (2025) [18]	TS-RF Optimized Random Forest (Scientific Reports)	99.67%	93%	Higher accuracy on benchmark dataset , centralized static dataset v_s. realistic trust-based deployment
Proposed (Office dataset – 400 nodes)	Hybrid Trust–Energy Based Secure Routing with ML Classification and Blockchain Logging	Measured	93%	Realistic deployment
Overall Range	---------	90–99.67%	93%	Competitive & realistic

2. Blockchain Integrity Comparison

Several surveyed studies integrate blockchain primarily at an architectural level without providing numerical evidence of integrity or verification success. Among the reviewed works, Gaikwad (2024) [1] reports a measurable blockchain verification success rate.

Table 2 summarizes the blockchain integrity and security performance comparison between the proposed framework and existing approaches

Table 2: Blockchain Integrity, Tamper Detection, and Verification Rates

Refrences	Method	Integrity Metric	Result		Remarks
			Reported	Proposed	
Gaikwad (2024) [1]	Secure Data Transmission with Blockchain Cryptography	Reported Integrity Evaluation	98%	Reliable (CRC + ECC + AES + Blockchain)	Enhanced via ECC and CRC
Prasuna et al., (2024) [4]	Blockchain Framework	Integrity evaluation not quantified	Not Reported	Reliable (CRC verified, error-free transmission observed)	Measurable integrity provided
Debashis Das et al., (2023) [2]	SDN-Blockchain for 5G	Integrity evaluation not reported	Not Reported	Reliable (CRC + ECC + secure logging)	Hash-chain verification enabled
Harris et al., (2025) [5]	IoT-Blockchain Security Framework	Integrity evaluation not provided	Not Reported	Reliable (CRC verified + immutable logging)	Tamper-evident logs supported
Proposed Framework	Hybrid AES + Blockchain + Trust + ML	Measured Integrity	Not Reported	98%	Strong integrity with multi-layer security

Interpretation

- Most blockchain-enabled WSN studies do not provide numerical integrity evaluation.
- The proposed framework demonstrates consistently high verification reliability due to the integration of AES encryption, error-correcting codes, CRC checks, and hash-chained blocks**.**
- The blockchain ledger also ensures auditability and traceability, which are not explicitly quantified in most prior works.

3. Trust-Based Malicious Node Detection Comparison

Existing studies typically adopt either threshold-based trust models or standalone ML classifiers. None of the surveyed approaches integrate trust computation, ML-based detection, routing, and blockchain logging into a unified framework.

Table 3 presents the comparison of malicious node detection performance using machine learning techniques across different methods.

Table 3: Malicious Node Identification Performance

Refrences	Methodology	Detection Mechanism	Detection Capability	Proposed Framework
Parvathi & Talanki (2020) [7]	Energy saving hierarchical routing protocol in WSN	Trust threshold only	Medium	Higher (ML + trust + energy)
Vucovich *et al*., (2022) [8]	Federated Learning Detection	ML-based distributed classifier	ML-based distributed classifier	ML-based distributed classifier
Prasuna *et al*., (2024) [4]	Fog-Blockchain IDS	Rule-based anomaly detection	Medium	Higher with ML-driven trust
Proposed Framework	ML-Based Trust-Aware Anomaly Detection with Blockchain Integration	ML-based classifier with trust score evaluation	Measured	~93% detection accuracy

Interpretation

- The proposed framework enables earlier and more reliable malicious node detection by combining trust decay patterns with ML classification.
- Approaches relying solely on static thresholds or rule-based detection show limited adaptability to dynamic network behavior

4. Routing Performance Comparison

Routing performance is evaluated by comparing EM-DSOA trust-aware routing with classical static shortest-path routing and random path selection.

Table 4 compares routing performance based on energy efficiency, trust evaluation, and path optimization strategies

Table 4: Routing Performance Comparison

Metric	Static Routing	Random Routing	EM-DSOA (Proposed)	Best
Hop Count	High	Unstable	Optimized	EM-DSOA
Latency	High	Relatively high	Low	EM-DSOA
Average Route Trust	Low	Relatively high	High	EM-DSOA
Energy Consumption	High	Unpredictable	Balanced	EM-DSOA
Packet Delivery Ratio	Medium	Low	High (85–92%)	EM-DSOA

Interpretation

- EM-DSOA routing consistently outperforms baseline routing strategies by avoiding low-trust and energy-depleted nodes**.**
- Random routing exhibits the poorest performance due to the absence of trust and energy awareness.

5. Overall Comparison with Literature

A consolidated comparison across multiple security dimensions is presented below.

Table 5 provides an overall comparative analysis highlighting the integrated advantages of the proposed framework over existing solutions.

Table 5: Overall Comparison across Security Dimensions

Feature	Typical Existing Approaches	Proposed Framework	Observation
ML Accuracy	90%	93%	Competitive
Blockchain Integrity	Often not quantified	~98–99%	Stronger
Trust Model	Static threshold	Dynamic trust + ML	Advanced
Routing Strategy	Shortest-path / static	EM-DSOA trust-aware	Improved
Visualization	Rarely provided	GUI + case studies	Enhanced
Hybrid Security	Single-layer focus	Integrated multi-layer	Unique

Discussion

Reasons for Improved Performance

- Integrated Security Stack Unlike existing works that address ML, blockchain, or routing independently, the proposed framework integrates multiple security layers into a unified architecture.
- Robust Data Integrity The combination of encryption, error correction, and blockchain ensures high resistance to tampering and transmission errors.
- Realistic Evaluation Environment Dynamic trust and energy variations introduce realistic conditions absent in most static-dataset-based studies.
- Routing Stability Trust-aware routing improves delivery reliability while reducing latency and energy imbalance.
- Early Anomaly Detection ML-assisted trust decay enables earlier identification of compromised nodes.

Limitations

- Long-term adversarial behavior may eventually degrade network performance in extreme conditions.
- Very large-scale deployments may require computational optimization.
- GUI responsiveness depends on hardware capability.

These limitations are common in experimental WSN frameworks and are acceptable within the scope of current Scopus-indexed research although additional security layers introduce computational overhead, the modular design allows selective activation based on network resource availability.

Conclusion and Future Work

Conclusion

This paper presented a comprehensive secure framework for Wireless Sensor Networks that integrates biometric authentication, dynamic trust evaluation, machine learning–based anomaly detection, trust-aware routing, and blockchain-assisted data integrity. Experimental results demonstrate that the proposed framework achieves competitive classification accuracy, high blockchain integrity, improved routing reliability, and enhanced resistance to malicious node behavior. Unlike existing approaches that focus on isolated security layers, the proposed solution offers a unified and scalable security architecture suitable for smart city and IoT environments. Overall, the proposed integrated framework demonstrates a practical and scalable approach for secure, intelligent, and efficient wireless sensor network deployment in smart city environments. The proposed framework can be extended to large-scale WSN deployments through hierarchical node clustering and distributed blockchain validation mechanisms. The proposed framework provides a hybrid computational-security model that bridges trust dynamics, machine learning, and distributed ledger systems.

Future Work

Although the proposed framework demonstrates effective trust-based security, malicious node detection, and blockchain-assisted data integrity for smart-city WSN scenarios, several extensions can be explored to further enhance the system. Future work may include the incorporation of explicit multi-hop routing protocols to study routing behavior at the packet level and compare different routing strategies under identical network conditions. This would allow deeper evaluation of routing efficiency beyond the current hop-count–based abstraction. The framework can also be extended to support integration with IoT communication platforms such as MQTT or other technologies, enabling experimentation with real-world data transmission pipelines and edge-to-cloud communication models. Such integration would facilitate deployment-oriented studies while preserving the existing security and trust mechanisms. More advanced energy optimization models can be investigated by incorporating detailed battery consumption profiles, adaptive transmission power control, and sleep–wake scheduling. These enhancements would enable long-term network lifetime analysis in large-scale smart-city deployments. In addition, future research may explore advanced sensor fusion techniques and richer

environmental data streams, allowing the application of more sophisticated machine learning models for anomaly detection and predictive analytics. This could improve the system's capability to detect complex attack patterns and abnormal network behavior. Finally, the proposed framework may be extended to industrial monitoring scenarios, such as power-grid or infrastructure surveillance, and evaluated under node failure and signal loss conditions to assess system resilience. These extensions would further establish the framework as a flexible research and teaching platform for secure and intelligent WSN design. Future extensions of this work will explore cluster-based routing protocols such as LEACH integrated with adaptive memory-aware scheduling, enabling further reduction in node storage overhead while preserving security guarantees.

Funding: The authors declare that no external funding was received for this research.

References

1. Gaikwad SY. Secure data transmission in the wireless sensor network with blockchain cryptography network. Journal of Sensors, IoT & Health Sciences,2024:2(2):41–55. https://doi.org/10.69996/jsihs.2024009
2. Das D, Banerjee S, Dasgupta K, Chatterjee P, Ghosh U, Biswas U. Blockchain enabled SDN framework for security management in 5G applications. Proceedings of the International Conference, 2023. https://doi.org/10.1145/3571306.3571445
3. Uvarajan KP. Integration of blockchain technology with wireless sensor networks for enhanced IoT security. Journal of Wireless Sensor Networks and IoT,2024:1(1):15–18. https://ecejournals.in/index.php/WSNIOT/article/view/22/52
4. Prasuna VG, Ravindra Babu B, Pydala B. BlockFog: A blockchain-based framework for intrusion defense in IoT fog computing. Scalable Computing: Practice and Experience,2024:25(3):1950–1962. https://doi.org/10.12694/scpe.v25i3.2686
5. Harris L, Sreejani K, El Azizi H. Blockchain-enabled AI security frameworks for detecting and preventing cyber threats in IoT networks. Computer Security, 2025. https://www.researchgate.net/publication/390111515
6. Alkhfaji AM. Blockchain based wireless sensor networks for detecting nodes. Journal of Smart Internet of Things,2023:2:1–12. https://doi.org/10.2478/jsiot-2023-0007
7. Parvathi C, Talanki S. Energy saving hierarchical routing protocol in WSN. In: Wireless Sensor Networks – Design, Deployment and Applications. IntechOpen, 2020. https://doi.org/10.5772/intechopen.93595
8. Vucovich M, et al. Anomaly detection via federated learning. arXiv preprint, 2022. https://arxiv.org/abs/2210.06614
9. Islam MJ, Rahman A, Kabir S, Karim MR, Acharjee UK, Nasir MK, et al. Blockchain-SDN based energy optimized and distributed secure architecture for IoTs in smart cities. Preprints, 2020. https://doi.org/10.20944/preprints202011.0552.v1
10. Olakanmi OO, Dada A. Wireless sensor networks: Security and privacy issues and solutions. In: Wireless Mesh Networks – Security, Architectures and Protocols. IntechOpen, 2020. https://doi.org/10.5772/intechopen.84989
11. Bouakkaz F, Wided A, Guemmadi S, Derdour M. K-means efficient energy routing protocol for maximizing vitality of WSNs. IntechOpen, 2021. https://doi.org/10.5772/intechopen.96567
12. Abbassi K, Jeridi MH, Ezzedine T. WSN for event detection applications: Deployment, routing, and data mapping using AI. IntechOpen, 2020. https://doi.org/10.5772/intechopen.94085
13. Selvi M, Santhosh Kumar SVN, Thangaramya K, Abdul Gaffar H. Energy efficient trust aware secure routing algorithm with attribute based encryption for wireless sensor networks. Scientific Reports,2025:15:19724. https://doi.org/10.1038/s41598-025-03558-8
14. Sebestyen H, Popescu DE, Zmaranda RD. A literature review on security in the internet of things: Identifying and analysing critical categories. Computers,2025:14:61. https://doi.org/10.3390/computers14020061
15. Anslam S, Annabel LSP. Network lifetime improvement in wireless sensor networks using energy-efficient bat-moth flame optimization technique. Scientific Reports,2025:15:18065. https://doi.org/10.1038/s41598-025-88550-y
16. Wakili A, Bakkali S. Privacy-preserving security of IoT networks: A comparative analysis of methods and applications. Cyber Security and Applications, 2025, 100084. https://doi.org/10.1016/j.csa.2025.100084
17. Sharma N, Dhiman P. A survey on IoT security: Challenges and their solutions using machine learning and blockchain technology. Cluster Computing,2025:28:313. https://www.researchgate.net/publication/391238345
18. Pandey VK, et al. Enhancing intrusion detection in wireless sensor networks using a tabu search based optimized random forest. Scientific Reports,2025:15:18634. https://doi.org/10.1038/s41598-025-03498-3
19. Goswami P, Khan T, Pathak V, Alabdultif A. Machine learning based dynamic trust estimation framework for securing wireless sensor networks. Scientific Reports,2025:15:35821. https://doi.org/10.1038/s41598-025-19768-z
20. Nguyen DT, et al. Security issues in IoT-based wireless sensor networks: Classifications and solutions. Future Internet,2025:17:350. https://doi.org/10.3390/fi17080350
21. El Bekkali A, Essaaidi M, Boulmalf M. A blockchain-based architecture and framework for cybersecure smart cities. IEEE Access, 2023, 11. https://doi.org/10.1109/access.2023.3296482
22. Al Ghamdi MA. An optimized and secure energy-efficient blockchain-based framework in IoT. IEEE Access, 2022, 10. https://doi.org/10.1109/ACCESS.2022.3230985
23. Vinya VLV, et al. A novel blockchain approach for improving the security and reliability of wireless sensor networks using jellyfish search optimizer. Electronics,2022:11:3449. https://doi.org/10.3390/electronics11213449

24. More SS, More PS, Bagane P. Blockchain technology for trusted network in wireless sensor network. Journal of Scientific and Industrial Research,2024:83:567–580. https://doi.org/10.56042/jsir.v83i5.711
25. Nguyen TM, Vo HHP, Yoo M. Enhancing intrusion detection in wireless sensor networks using a GSWO-CatBoost approach. Sensors,2024:24:3339. https://doi.org/10.3390/s24113339
26. Sefati SS, et al. Cybersecurity in a scalable smart city framework using blockchain and federated learning for internet of things. Smart Cities,2024:7:2802–2841. https://doi.org/10.3390/smartcities7050109
27. Nurlan Z, et al. Wireless sensor network as a mesh: Vision and challenges. IEEE Access, 2021, 9. https://doi.org/10.1109/ACCESS.2021.3137341
28. Maheswar R, Kathirvelu M, Mohanasundaram K. Energy efficiency in wireless networks. Energies,2024:17:417. https://doi.org/10.3390/en17020417
29. Kumar A, Sharma B, Noonia A. Secure blockchain based intrusion detection for IoT networks. Discover Computing,2025:28:226. https://doi.org/10.1007/s10791-025-09754-4
30. Mliki H, Hadj Kacem A, Chaari Fourati L. A comprehensive survey on intrusion detection based machine learning for IoT networks. EAI Endorsed Transactions on Security and Safety,2021:8(29):3. https://doi.org/10.4108/eai.6-10-2021.171246