I. J. Computer Network and Information Security, **2026, 2, 210-229**
Published Online on April 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2026.02.12

Blockchain-enhanced Detection of Malicious Nodes in WSNs Using Parallel Triple Graph Attention-based Convolution Network

J. Jabez*
Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology Chennai, Tamil Nadu, India
E-mail: jabez.it@sathyabama.ac.in
ORCID iD: https://orcid.org/0000-0002-6337-032X
*Corresponding author

N. Jayanthi
Department of Information Technology, JJ College of Engineering and Technology, Trichy, Tamil Nadu, India
E-mail: jayanthi483@gmail.com
ORCID iD: https://orcid.org/0009-0008-5583-413X

Elangovan Muniyandy
Department of Biosciences, Saveetha School of Engineering.Saveetha Institute of Medical and Technical Sciences, Chennai - 602 105, Tamil Nadu, India
Applied Science Research Center. Applied Science Private University, Amman, Jordan
E-mail: elangovanm2@outlook.com
ORCID iD: https://orcid.org/0000-0003-2349-3701

R. Mohanapriya
Department of Electronics and Communication Engineering, Paavai Engineering College, Paavai Nagar, NH-44, Pachal -637 018.Namakkal, Tamil Nadu, India
E-mail: mohanapriyaramalingampec@paavai.edu.in
ORCID iD: https://orcid.org/0000-0002-1071-5021

Received: 19 November 2025; Revised: 08 January 2026; Accepted: 03 February 2026; Published: 08 April 2026

Abstract: A Wireless Sensor Network (WSN) is an efficient system for monitoring distributed areas and controlling environments; however, such networks are susceptible to malicious node attacks that bring forth network insecurity and untrustworthy data. WSNs are vulnerable to malicious nodes and cyber attackers that can interfere with data transmission, leading to compromised decision-making systems. Traditional security techniques against WSNs lack flexibility in real-time detection and data integrity because of constrained processing resources and vulnerabilities from centralized storage. This work aims to improve detection accuracy through a multi-stage strategy, which constitutes the general objective of this research. The presented model uses WSN-DS and WSN-BFSF datasets. The data are pre-processed using Localized-Global Depth Normalization for uniformity, followed by feature selection via Boosted Tern-Cat Hunting Optimization, which combines Cat Hunting Optimization and Boosted Sooty Tern techniques to reduce dimensionality. The attack detection is performed by a Parallel Triple Graph Attention-based Convolution Network, which employs Quantum Parallel Deep Convolution and Triple Graph Attention Networks. The RMRO optimizes the model's parameters to classify more accurately, and the benign data are safely stored through the Consensus-Aided PoA Decision Blockchain Engine and InterPlanetary File System. This approach achieved 99.4% accuracy, 99.3% recall, and 99.5% F1 score on the WSN-DS dataset and 99.2% accuracy, 99.1% precision, and 99.3% F1 score on the WSN-BFSF dataset while showing robustness across different combinations of sensors. Hence, the Tri-QPdCNet offers a pioneering approach toward securing WSNs from dynamic and persistent attacks by providing an improved framework for anomaly detection using a strong, scalable architecture, augmented with blockchain technology. That leads to more robust WSN infrastructures that can be more securely and smoothly deployed in real-time critical environments.

Index Terms: Blockchain, InterPlanetary File System, Intrusion Detection System, Malicious Node, Wireless Sensor Networks, WSN-BFSF, WSN-DS.

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

1. Introduction

The advent of blockchain-enhanced Wireless Sensor Networks (WSNs) introduces a new defense in preventing malicious node attacks with decentralized trust and secure data management [1]. Classical WSNs, exposed to diverse attacks owing to the relative independence of the nodes [2], are now strengthened with blockchain, which ensures data tamper-proofing and subsequently achieves nodes' identity validation [3]. The integration of blockchain with WSNs increases the security protocols to a significant extent [4], primarily in the detection and mitigation process of malicious nodes present [5]. Blockchain is a decentralized framework that allows validation [6], authentication, and recording of all transactions or exchanges within the network [7]; hence, it prevents the unwanted meddling of unauthorized elements and provides substantial traceability [8].

Integrating blockchain with an elaborate intrusion detection mechanism for WSNs provides robust security against different attacks [9]. The distributed ledger technology empowers blockchain technology that enhances node accountability through an immutable log of interactions [10]. This also facilitates quick identification of anomalies that may occur for improving detection accuracy over time, as datasets enable real-time training and evaluation of the detection algorithms [11]. Moreover, the InterPlanetary File System (IPFS) integration ensures efficient storage of data by reducing redundancy and improving node efficiency [12].

For applications such as smart cities that operate in real time, the fundamental concept is monitoring. For instance, a city is equipped with thousands of sensor nodes as part of its core infrastructure, including control of traffic management and utilities. A malicious node might transmit false information to a control center that could disrupt traffic or bring down electrical supplies [13]. In this case, the Intrusion Detection System (IDS) backed by blockchain is designed to analyze each node's behavior to detect malicious activities, while the IPFS distributes verified data among the nodes [14], containing the threat and maintaining data integrity [15]. They help to minimize adversarial activity and ultimately keep both the network and its users safe, all while enabling decisions to be made much more quickly at a local level.

Contributions

- The primary data gathering employs WSN-DS and WSN-BFSF datasets, which record several node varieties and patterns of malevolent operations essential for model development and testing.
- Collected data is then processed using Localized-Global Depth Normalization (Lo-GDN), which improves uniformity by normalizing both local and global depth, making it a normalized dataset.
- The Boosted Tern-Cat Hunting Optimization (BoT-CHO) method effectively selects the features from the datasets, which decreases the dataset size and increases the dimensionality of effective features that improve the intrusion detection model.
- Malicious activities in nodes are classified accurately using the Parallel Triple Graph Attention-Based Convolution Network (Tri-QPdCNet). Tri-QPdCNet involves Quantum Parallel Convolution and Triple Graph Attention to probe deeply into complex node relationships.
- The weight parameters are optimized by the Resilient Mud Ring Optimizer (RMRO), which makes the modality adaptive to threats, thereby fine-tuning the network performance.
- After classification, benign data will be stored securely in a Consensus Aided PoA Blockchain Engine (CA-PoA-BE) with InterPlanetary File System (IPFS), ensuring the integrity and availability of the data is safe and decentralized.

This work is organized as follows: Existing works are illustrated in Section 2. The proposed Tri-QPdCNet is explained in Section 3. In Section 4, the performance analysis of the suggested methodology is presented. Section 5 draws the article to a conclusion.

2. Literature Survey

Among the extensive studies in this field, a selection of key works is reviewed to highlight foundational and recent advancements.

In 2023, Nouman, M., et al. [16], have examined malicious node detection and secure data storage in WSNs by integrating Machine Learning and Blockchain (BC). Blockchain was applied at Base Stations and Cluster Heads for node registration and security management, while Histogram Gradient Boost (HGB) classified nodes as malicious or legitimate. Malicious nodes were revoked, and legitimate data were stored in IPFS with hashes maintained in BC. Verifiable Byzantine Fault Tolerance replaced Proof of Work for consensus. Unlike prior works relying solely on ML classifiers such as Adaptive Boost, Gradient Boost, Extreme Gradient Boost, Linear Discriminant Analysis, and Ridge, this framework critically combined distributed storage with consensus efficiency, highlighting a more resilient workflow for WSN security.

In 2023, Elsadig, M.A., [17], investigated denial-of-service (DoS) detection in WSNs through a lightweight ML framework. The study examined vulnerabilities and limitations of WSNs under DoS attacks and evaluated earlier detection methods, emphasizing trade-offs between accuracy and computational cost. A Decision Tree (DT) classifier

with Gini feature selection was applied for efficient detection, trained and tested on an enhanced WSN-DS dataset. Unlike Random Forest, Extreme Gradient Boosting, and k-Nearest Neighbor, which demanded higher computational overhead, this design aligned with WSN constraints by balancing detection accuracy with reduced resource consumption, demonstrating stronger scalability compared to prior works.

In 2024, Talukder, M.A., et al. [18], have addressed intrusion detection in WSNs by combining ML with the Synthetic Minority Oversampling Technique and Tomek Link (MLSTL-WSN) to overcome class imbalance. The approach balanced datasets by generating minority samples and eliminating overlapping instances, while feature scaling ensured consistent inputs for training. Evaluation on WSN-DS highlighted improved precision in both binary and multiclass detection. Compared to earlier intrusion detection systems that suffered from false alarms, redundancy, and computational overhead, this design demonstrated higher robustness and efficiency, offering stronger adaptability than conventional classifiers reliant on unbalanced data.

Table 1. Summary of the existing methods

Reference Number	Dataset Used	Methods	Highlights	Challenges
[16]	WSN-DS	HGB	1. Achieved good accuracy for intrusion detection. 2. Enhanced detection of specific attack types.	1. High computational cost. 2. Limited real-time processing capabilities.
[17]		DT	1. Simple and interpretable model. 2. Fast training and inference times.	1. Lower accuracy on complex attacks. 2. Limited scalability for large datasets.
[18]		MLSTL-WSN	1. Improved multi-layer analysis of network traffic. 2. Increased accuracy on varied attacks.	1. High memory usage. 2. Slower model convergence.
[19]	WSN-BFSF	IRADA	1. Adaptive detection with high precision. 2. Robust against a variety of attack patterns	1. Computationally intensive tuning process. 2. Requires specialized hardware for best results.
[20]		Wsn-bfsf	1. Combined models for better accuracy. 2. Reduced false positive rate.	1. Complexity in model integration. 2. Increased model training time.
[21]	WSN-DS and WSN-BFSF	GSWO-CatBoost	1. High accuracy in multi-class attack detection. 2. Effective in distinguishing between similar attacks.	1. Computational overhead in optimization. 2. Higher resource requirement.
[22]		SCNN-Bi-LSTM	1. Privacy-preserving model for secure detection. 2. Enhanced detection rate with federated learning.	1. Complex model training process. 2. Scalability issues with large networks.

In 2024, Shakya, V., et al. [19], have recommended an attack detection method in WSNs by developing an Integrated Reinforcement Learning and Deep Learning Algorithm (IRADA). The study highlighted limitations of existing Intrusion Detection Systems (IDSs), including false alarms, overfitting, and computational overhead. IRADA combined Deep Learning (DL) optimized through Bayesian methods with Reinforcement Learning (RL) to balance detection accuracy and adaptability. Unlike conventional DL-only or RL-only approaches that struggled with data dependency or training inefficiency, this integration achieved stronger robustness against adversarial threats while enhancing classification reliability, thereby presenting a more resilient security framework compared to prior IDS designs.

In 2023, Dener, M., et al. [20] analyzed attack detection in WSNs through the creation of a new dataset named WSN-BFSF, focusing on blackhole, flooding, and selective forwarding attacks simulated in the NS2 environment. The dataset underwent preprocessing to support ML and DL models for traffic classification and malicious behavior identification. Various ML methods, including Random Forest, DT, Naïve Bayes, and Logistic Regression, along with DL models such as Convolutional Neural Network, Long Short-Term Memory, and Gated Recurrent Unit, were applied. Unlike earlier studies relying on limited datasets, this contribution enriched experimental benchmarking, offering broader attack coverage and improved validation for WSN intrusion detection research.

In 2024, Nguyen, T.M., et al. [21] presented an intrusion detection approach for WSNs by integrating Genetic Sacrificial Whale Optimization (GSWO) with CatBoost. GSWO combined Genetic Algorithm and Whale Optimization Algorithm with a conditional inherited choice mechanism to mitigate premature convergence, improving feature selection efficiency. CatBoost was then employed for classification with optimized hyperparameters using GSWO-based quantization. Unlike conventional FS or DL-based methods that struggled with computational cost and slower inference, this design achieved faster processing while maintaining high accuracy across multiple datasets, demonstrating stronger scalability and real-time applicability for WSN security.

In 2024, Jena, S.R., et al. [22] introduced a privacy-preserving intrusion detection framework for Internet-enabled WSNs using Federated Learning. The design integrated Stacked Convolutional Neural Networks (SCNN) and

Bidirectional Long Short-Term Memory (Bi-LSTM), optimized through the African Vulture Optimization Algorithm, to strengthen intrusion detection accuracy while safeguarding data privacy. The framework was trained on datasets including WSN-DS, CIC-IDS-2017, and WSN-BFSF. Unlike traditional IDSs that struggled with unknown attacks and privacy risks, this method achieved superior scalability and resilience, critically outperforming standalone DL or optimization-driven IDS approaches in real-world WSN environments.

Table 1 shows the summary of the existing methods, which is given below,

Problem Statement

WSNs play a significant role in realizing real-time monitoring across different sectors, from the environmental sector to the infrastructure sector. However, WSNs are prone to many security threats, including threats from malicious nodes that can cause disruption of the integrity of the generated and transmitted data, interference with the communication network, and utilization of scarce resources. Conventional security techniques used in WSNs fail to differentiate node identity and perform rapid identification of the intruder in the decentralized network topology. The incorporation of blockchain technology increases security by creating an open yet reliable system that accurately captures and verifies all the actions of each node and easily eliminates any unbecoming nodes. Such a blockchain-integrated approach, when used with WSN-DS and WSN-BFSF for anomaly detection, promises higher reliability, robustness, and scalability for WSNs against dynamism and threats in their environment.

3. Proposed Methodology

The proposed methodology improves the detection of malicious nodes in WSNs through advanced processing, attack identification, and secure storage. First of all, the data from both WSN-DS and WSN-BFSF datasets is gathered and preprocessed using the Lo-GDN technique to normalize the data. Subsequently, Boosted Tern-Cat Hunting Optimization (BoT-CHO) assigns the importance weight to differentiate and choose the most important feature from the structure of data set. For detection, a Parallel Triple Graph Attention-based Convolution Network (Tri-QPdCNet) achieves high accuracy for detecting the patterns of attacks. The accuracy of classification separates is improved by the use of the Resilient Mud Ring Optimizer, while benign data is stored securely through the decentralized Consensus-Aided PoA and IPFS blockchain structure. Figure 1 presents the block diagram of the proposed methodology.

3.1. Data Collection

The data collection for this blockchain-enhanced detection framework is built on two datasets, WSN-DS and WSN-BFSF, which are specially created for wireless sensor networks (WSNs). They contain extensive logs of the type of network states in that kind of network by capturing both good and bad patterns of sensor node activities. Conversely, WSN-DS presents the complete set of well-known attacks and intrusion efforts, whereas WSN-BFSF is employed to get a focused perspective on specific network vulnerabilities.

The collected data is then forwarded to Localized-Global Depth Normalization, which is selected as it balances both localized and global features of the data and thus better normalizes various network data collected than traditional methods.

3.2. Pre-processing

In data preprocessing for sensor networks, Localized-Global Depth Normalization (Lo-GDN) [23] is applied to harmonize sensor data across datasets like WSN-DS and WSN-BFSF. This approach enhances data uniformity, compensating for inconsistencies due to variable configurations in sensor nodes. By using Lo-GDN, the data is optimized with consistent structural quality, facilitating efficient feature selection and reducing preprocessing time.

- Local Depth Normalization

To achieve localized consistency, Lo-GDN partitions each sensor dataset into small regions and applies normalization within each region independently. Each patch Q is normalized to have a mean of zero and a near unit variance, according to equation (1),

$$L^{LDN}(\omega) = \frac{S(\omega) - mean(S(Q))}{std(S(Q)) + \delta}, \quad \text{where } \omega \in Q \tag{1}$$

where $S(\omega)$ represents the sensor measurement at point ω within the patch Q, and δ is a small constant added for numerical stability and std and $mean$ denotes the standard deviation and mean, respectively. This localized normalization minimizes local variations, refining data quality for subsequent analysis.

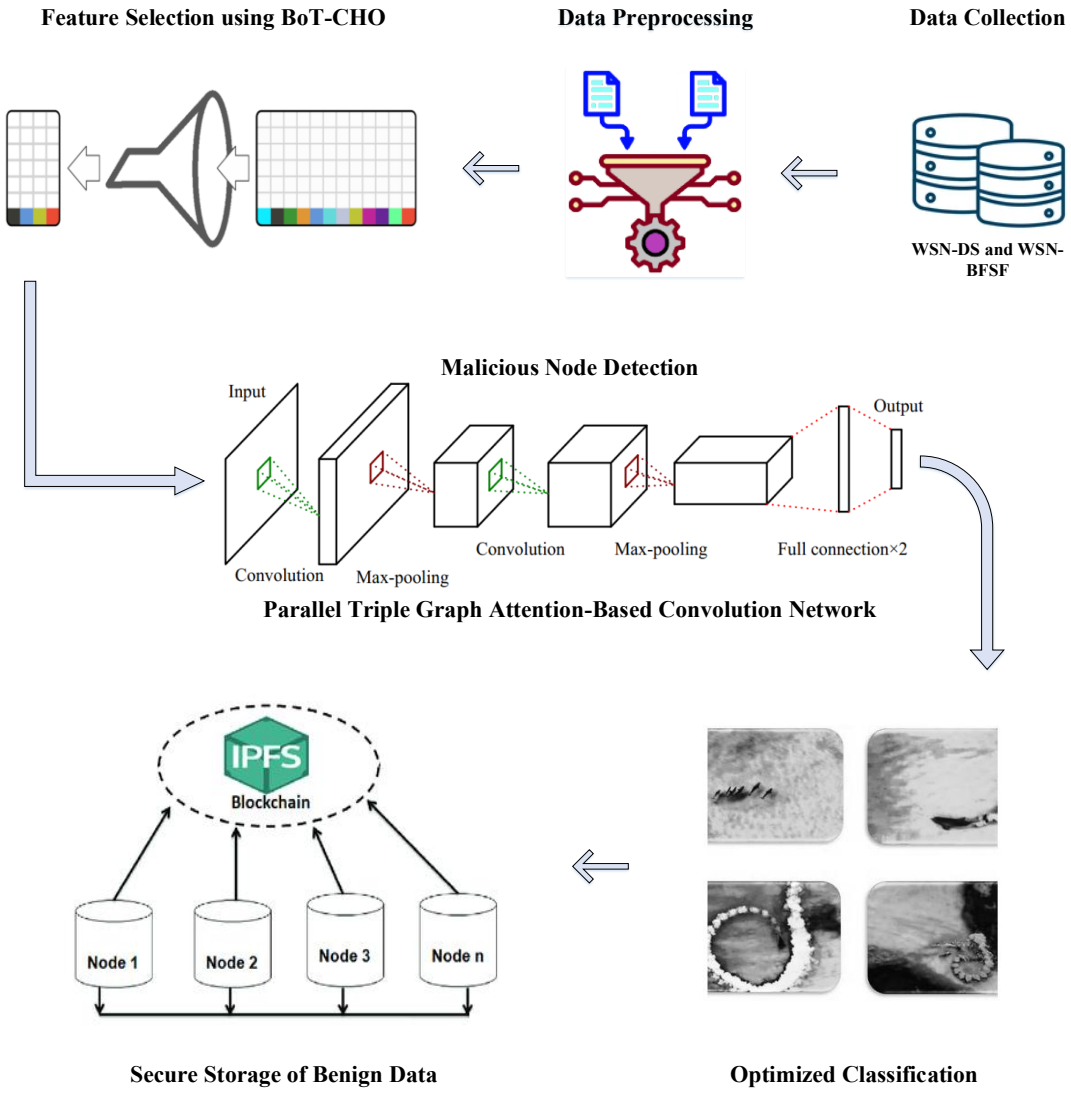


Fig.1. Block diagram of Tri-QPdCNet

- Global Depth Normalization

In addition to local adjustments, a global normalization is introduced to capture the broader data trends across the entire dataset. The global scale is adjusted using the overall standard deviation $std(S(D_\Theta))$, where D_Θ represents the entire data scope. It is expressed in equation (2),

$$L^{GDN}(\omega) = \frac{S(\omega) - mean(S(D_\Theta))}{std(S(D_\Theta)) + \delta} \quad (2)$$

This normalization process frees the data from absolute scaling differences, focusing on relative variations across both local and global contexts. By implementing Lo-GDN, the preprocessing step enhances structural uniformity, essential for the data's readiness for feature selection using Boosted Tern-Cat Hunting Optimization, which has been selected due to its applicability in high-dimensional datasets and high precision in defining the most significant features while improving the time efficiency over the traditional approaches.

3.3. Feature Selection

Preprocessed data are input for feature selection, optimizing the selection of relevant features critical for intrusion detection in WSNs using Boosted Tern-Cat Hunting Optimization (BoT-CHO). This advanced approach strategically extracts features, using Cat Hunting Optimization (CHuntO) [24], improving data processing efficiency and enabling faster, accurate detection in real-time threat scenarios. To further enhance feature selection effectiveness, CHuntO undergoes dynamic integration with Boosted Sooty Tern Optimization (BSooT) [25], ensuring optimal feature sets that significantly reduce computational load.

A. CHuntO Algorithm

In CHuntO, each solution represents a unique feature vector and a population of randomly generated vectors M. Each feature vector's relevance is determined using an objective function that balances feature quantity and prediction error, formalized as equation (3),

$$Cos(M_i) = v_1 \times \frac{1}{s} G(M_i) + v_2 \times \|M_i\| \tag{3}$$

where v_1 and v_2 are weighting coefficients within [0,1], $G(M_i)$ represents the prediction error for vector M_i, and $\|M_i\|$ denotes the number of selected features.

The most competent and least competent vectors, designated α and β, respectively, define a dynamic range of possible states, with higher-competence vectors exploring a broader state space. The number of states a solution vector M_i may explore is represented by equation (4),

$$state_{(M_i)} = \left(\frac{G(M_i)-G(\beta)}{G(\alpha)-G(\beta)}\right)^q \cdot \left(state_{(\alpha)} - state_{(\beta)}\right) + state_{(\beta)} \tag{4}$$

where q is a power parameter, adjusted to regulate the search radius over iterations, ensuring an exploratory-to-exploitative transition.

The feature vectors are updated iteratively, focusing on maximizing search accuracy by adjusting solutions based on population mean M_{avg} and optimal solution position M^*, calculated as equation (5),

$$M_{new} = M + z_1 \cdot \left(M - M_{avg}\right) + z_2 \cdot (M - M^*) \tag{5}$$

where z_1 and z_2 are random values within [0,1], ensuring a balanced search space coverage. The mean M_{avg} is updated dynamically as equation (6),

$$M_{avg} = \frac{1}{N}\sum_{i=1}^{N} M_i \tag{6}$$

where N is the total number of vectors. These optimized parameters are integrated with BSooT to accelerate feature selection and to enhance the precision and speed essential in real-time scenarios.

B. BSooT Optimization

Following CHuntO, Boosted Sooty Tern Optimization (BSooT) is applied to enhance feature selection efficiency, optimizing both the accuracy and speed essential for real-time intrusion detection in WSNs. This optimized feature selection technique, applied to WSN-DS and WSN-BFSF datasets, leverages BSooT for precise, computationally efficient feature extraction that reduces dimensionality and supports high detection accuracy and rapid processing.

In BSooT, exploration is supported by migration behaviour and collision avoidance mechanisms to prevent overlap among search agents. The position of each search agent is adjusted to avoid collisions with nearby agents as equation (7),

$$C_\beta = SA \cdot P_\beta(d) \tag{7}$$

where C_β denotes the updated, non-colliding position of the agent. The variable $P_\beta(d)$ represents the current position of the search agent, and d is the current iteration. SA is the agent's movement factor within the search space.

The fitness function in BSooT is designed to evaluate each feature subset based on its dimensionality reduction, as in equation (8),

$$Fitness(S) = \alpha \cdot \frac{1}{|F|} \tag{8}$$

where S is the selected subset of features, $|F|$ is the total number of selected features (minimizing dimensionality), and α is a weight set to balance between feature count.

BSooT agents converge toward the direction of the fittest neighbour, which is determined by equation (9),

$$M_\beta = CB \cdot \left(Q_\gamma(d) - P_\beta(d)\right) \tag{9}$$

where M_β is the directional update towards the optimal neighbouring agent Q_γ. The parameter $CB = 0.5 \times rand$ introduces randomness for improved exploration, where $rand$ generates a random value within the [0,1] range.

In the exploitation phase, BSooT agents employ a spiral path to refine their search near promising regions, formulated in equation (10),

$$r' = R \cdot sin(k), rt = R \cdot cos(k) \text{ and } u' = R \cdot k \tag{10}$$

where R is the spiral radius, k ranges from $[0,2\pi]$, and constants for altitude and radial scaling are set as 1 for simplicity. The BSooT algorithm computes the agent's position after exploiting these spiral dynamics, using equation (11),

$$P_{\beta}(d) = \left(D_{\beta\varsigma} \cdot (r' + t' + u')\right) \cdot Q_{\gamma}(d) \tag{11}$$

where $D_{\beta\varsigma}$ is a derived factor influencing the final position update in relation to the most optimal search agent Q_{γ}.

This integration of CHuntO with BSooT enables the feature selection framework to efficiently prioritize critical features, which is then followed by a Parallel Triple Graph Attention-based Convolution Network for attack classification. It is chosen due to its superior ability to capture complex spatial-temporal attack patterns in WSNs.

3.4. Malicious Node Detection

After feature selection, attack detection in the node is carried out using Parallel Triple Graph Attention-based Convolution Network (Tri-QPdCNet), an architecture that integrates Quantum Parallel deep Convolution Network (QPdCNet) [26] with a Triple Graph Attention Network (Tri-GAN) [27].

A. Quantum Parallel Deep Convolution Network

- Transformation for Multi-Feature Detection

To perform effective attack detection, each feature subset is processed concurrently across QPdCNet's quantum-inspired layers, capturing intricate attack characteristics with precision. The transformation within QPdCNet, denoted as $T_{\alpha}(\mu, \chi)$, is applied to align features without needing individual frequency adjustments, as given in equation (12),

$$T_{\alpha}^{C}(\mu, \chi) = T_{\alpha}(\mu + 2\delta_{\alpha,\chi}) \tag{12}$$

where μ represents the frequency parameter, χ indicates the spatial dimension, and $\delta_{\alpha,\chi}$ is a scaling constant related to the quantum layer. This transformation maintains alignment across feature subsets, allowing coherent analysis of frequency-sensitive patterns.

- Phase Adjustment in Parallel Feature Layers

To enable simultaneous feature processing, continuous frequency compensation is introduced, ensuring consistent phase alignment across layers. This modified transformation $T_{\alpha}^{P}(\mu, \chi)$, eliminating frequency shifts, is defined as equation (13),

$$T_{\alpha}^{P}(\mu, \chi) = T_{\alpha}(\mu, \chi)e^{i\kappa_{\alpha} \cdot \mu} \tag{13}$$

where κ_{α} denotes the phase adjustment factor to synchronize the phase across all layers. This configuration facilitates parallel feature extraction within QPdCNet, enhancing detection accuracy for complex, high-frequency attack patterns.

- *Parallel Network Design for Enhanced Attack Detection*

The architecture of QPdCNet integrates multiple fully connected layers that run parallel to convolutional layers. These layers are carefully designed to manage large numbers of features efficiently. Each convolutional layer has activation layers, such as ReLU, along with softmax classifiers following it. An averaged cross entropy loss function has been applied across all outputs to optimize the weights for identification of diversified complex cyber threats.

B. Triple Graph Attention Network

Triple Graph Attention Network provides a mechanism to perform relational analysis between features extracted across graph-structured data. Capturing spatial and temporal dependencies, Tri-GAN detects subtle intrusion patterns with high accuracy, hence making the component an important constituent for effective detection of various kinds of cyber threats.

- Quantum-Inspired Feature Attention for Anomaly Classification

To accurately classify relevant attack features, a graph attention gating mechanism is used to refine node (feature) representations within Tri-GAN. This gating enables attack-specific attention across each dimension of the feature set, based on graph-based interactions between nodes. Given the node ρ_s representing a specific feature (or graph node) from QPdCNet, a lookup is performed over a feature embedding matrix E_ρ to retrieve the initial feature representation γ_s. The gating mechanism then computes the target-aware feature representation $\bar{\gamma}_s$ as equation (14),

$$\bar{\gamma}_s = \sigma\left(V_\rho\left[\xi \oplus \xi_\psi\right] + \delta_\rho\right) \cdot \gamma_s \tag{14}$$

where σ is an activation function, V_ρ and δ_ρ are trainable parameters, and ξ and ξ_ψ represent graph-based embeddings associated with neighbouring nodes. This operation refines γ_s by filtering irrelevant data for attack detection.

- Temporal-Specific Attention for Attack Correlation

To capture temporal relationships that may correlate with specific attack patterns, an attention mechanism is applied, giving each feature a unique, context-sensitive weight based on temporal dynamics. The attention weight θ_r for each feature node ρ_s is defined as equation (15),

$$\theta_r = Soft\,max\left(\omega_\theta \cdot tanh\left(U_\theta\left[\xi_\psi \oplus \gamma_\rho\right] + \delta_\theta\right)\right) \tag{15}$$

where $\omega_\theta, U_\theta,$ and $\delta_\theta$are trainable parameters. This equation assigns a higher weight to features strongly correlated with the temporal attack pattern.

- Respondent-Guided Attack Representation

The integration of spatial and temporal features with context-specific weights results in a comprehensive representation η_s of each feature's importance in detecting attacks. The final representation for a node, considering both respondent and temporal influences, is computed as equation (16),

$$\eta_s = \sum_{v=1}^{p} \theta_v \cdot \gamma_{\rho_v} \tag{16}$$

where p represents the total number of temporal steps considered, and θ_v is the assigned weight for each step.

Loss Function

For training, a cross-entropy loss function ℓ_{attack} is applied across all output nodes to optimize the model's parameters as in equation (17),

$$\ell_{attack} = -\frac{1}{n}\sum_{s=1}^{n}(y_s\, log(\hat{y}_s) + (1 - y_s)\, log(1 - \hat{y}_s)) \tag{17}$$

where y_s denotes the true label for node s, $\hat{y}_s$ represents the predicted probability, and n is the total number of nodes in the graph. This comprehensive approach ensures that both QPdCNet and Tri-GAN contribute to the precise and reliable classification of attacks. To finetune the network parameters, the Resilient Mud Ring Optimizer is used. This method is selected for its adaptive parameter optimization, enhancing classification accuracy and resilience against network fluctuations.

3.5. Optimized Classification with Resilient Mud Ring Optimizer

In order to improve the network classification performance, the Resilient Mud Ring Optimizer (RMRO) [28] algorithm is presented. This algorithm adapts to varying networks and different threats, improving the stability of the classification model. To evaluate and optimize agent positions, a fitness function F_{RMRO} is employed to measure classification accuracy and error reduction as in equation (18),

$$F_{RMRO} = \sum_{i=1}^{n}(-y_i\, log(\hat{y}_i) + (1 - y_i)\, log(1 - \hat{y}_i) \tag{18}$$

where y_i is the actual classification label, $\hat{y}_i$is the predicted label, and n is the number of samples. This fitness function aims to maximize accuracy and minimize classification error, guiding the RMRO agents towards optimal model parameters.

- Exploration Phase – Searching for Optimal Parameters

In the exploration phase, RMRO mimics dolphin echolocation, where virtual agents (simulating dolphins) search randomly for the best weight configuration. Each agent operates with a velocity V_C at position D_C, generating a sound

intensity K_C to detect optimal parameters. To regulate the agent's sound emission and focus on relevant parameter zones, the pulse rate p varies between 0 (no pulse emission) and 1 (maximum emission). The adaptive sound intensity K_C is calculated as equation (19),

$$K_C = 2\alpha_C \cdot U_C - \beta_C \tag{19}$$

where U_C is a random vector between 0 and 1, and $\alpha_C = 2\left(1 - \frac{t}{T_{max}}()\right)$ reduces linearly over time t with a maximum duration T_{max}. This variable intensity K_C aids in exploring the parameter space by encouraging agents to diverge from one another, thus supporting a global search for optimal configurations. To compute new positions, the position D_C^t of each agent at time step t is updated based on its velocity as in equation (20),

$$D_C^t = D_C^{t-1} + V_C^t \tag{20}$$

where V_C^t is initialized randomly within a predefined range, simulating initial exploration. This position update enables agents to explore the entire search space.

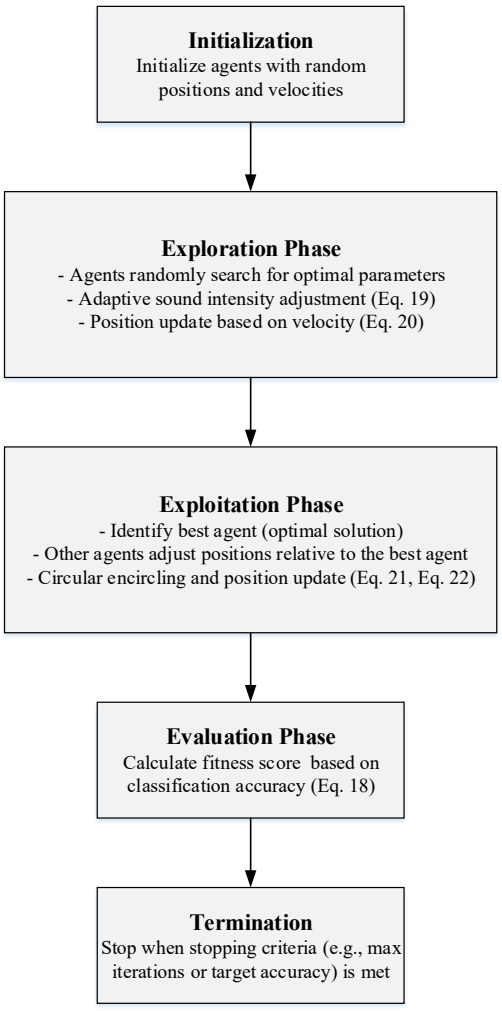


Fig.2. Step-by-step procedure of resilient mud ring optimizer

- Exploitation Phase – Encircling Optimal Solutions

In the exploitation phase, RMRO agents identify and converge towards an optimal solution. Once the best agent is identified, other agents adjust their positions relative to this agent's location to refine their own. The deviation A_C between an agent's position D_C^t and the best-known position D_C^* is defined as equation (21),

$$A_C = |C_C D_C^* - D_C^{t-1}| \tag{21}$$

where C_C is a coefficient vector that scales the influence of the best agent's position. The position update for the encircling behaviour is given as equation (22),

$$D_C^t = D_C^* \cdot sin(2\pi\lambda) - K_C \cdot A_C \tag{22}$$

where λ is a random variable that simulates oscillatory encircling, and K_C adjusts the degree of attraction towards the optimal solution. Each iteration dynamically refines the position of the agents around the optimal region. Figure 2 shows the procedure of RMRO.

Thus, RMRO enables adaptive and precise tuning of classification model parameters, improving resilience and accuracy in variable network conditions. To store the benign data, the Consensus-Aided PoA Decision Blockchain Engine (CA-PoA-BE) is used. CA-PoA-BE is chosen for its enhanced security, scalability, and efficient protection of benign data compared to other methods.

3.6. Secure Storage of Benign Data

After the network has been fine-tuned for classification tasks, benign data are securely stored using the Consensus-Aided PoA Decision Blockchain Engine (CA-PoA-BE) [29]. The integration of the InterPlanetary File System (IPFS) with CA-PoA-BE provides a distributed network for benign data storage, enhancing accessibility, scalability, and rapid data retrieval for real-time applications.

In the CA-PoA-BE model, each block in the Decision Blockchain is generated at consistent time intervals. Starting from the initial block time-stamped at T_0, a block at height $u > 0$ created at time T_u satisfies equation (23),

$$T_u = T_0 + \gamma \cdot \Delta \tag{23}$$

where γ is an integer parameter representing the step count, and Δ is the fixed interval for block generation.

To maintain the security of the blockchain, a deterministic process termed Deterministic Pseudo-Random Process (DPRP) decides the authorized node for block generation. The status of nodes as "active" or "inactive" is regularly updated. The legitimacy of node J for producing block $B(u,T)$ at height u and time T is determined by a pseudo-random value $\beta(u,T)$, as expressed in equation (24),

$$\beta(u,T) = DRPRP(u,T) \equiv hash(u \oplus T) \tag{24}$$

where $\oplus$ signifies byte-array concatenation. The active node set A_B is defined as the ensemble of nodes with the authority to produce a given block. For any node M in A_B, its index in the set is computed by equation (25),

$$\delta^M(u,T) = \beta(u,T)\, mod \|A_B\| \tag{25}$$

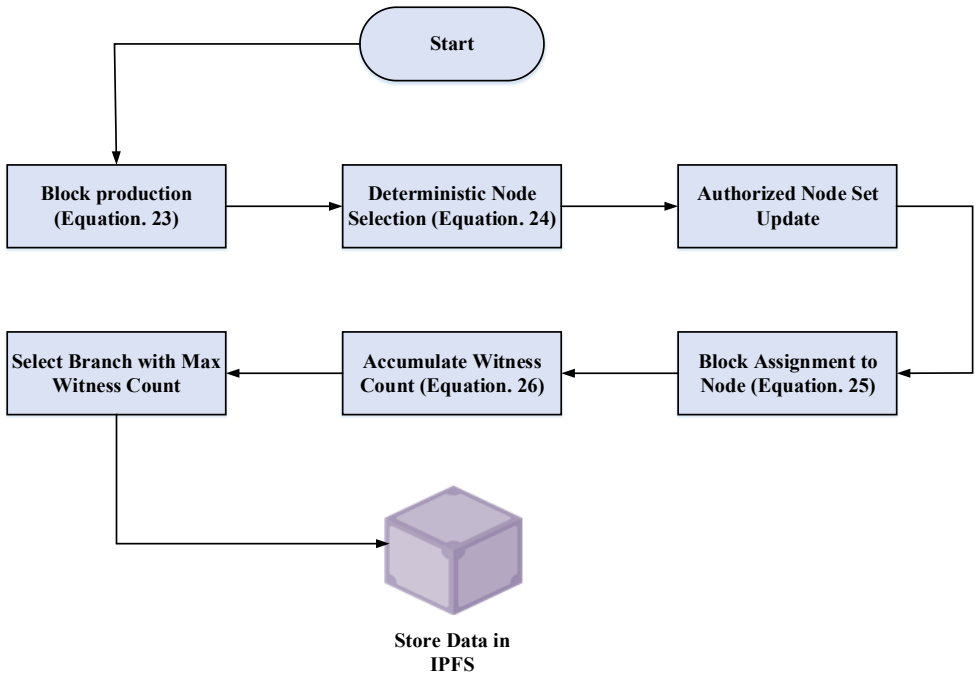


Fig.3. Secure Storage of Benign Data using CA-PoA-BE

Thus, node M generates block $B(u,T)$ only if it matches the index δ^M calculated in the set A_B. For branch selection, CA-PoA-BE employs an accumulated witness count, denoted by $\lambda_B(u,T)$, to determine the legitimate branch. For any block $B(u,T)$, this is computed as equation (26),

$$\lambda_B(u,T) = \lambda_{PA(B(u,T))} + \|A_B(u,T)\| \tag{26}$$

where $\|A_B(u,T)\|$ denotes the number of active nodes witnessing the block. Figure 3 shows the series of steps for CA-PoA-BE.

The CA-PoA-BE architecture enables secure, decentralized, and high-speed storage of benign data in IPFS. This model provides resilience against data tampering and supports scalability, making it an efficient choice for managing data in real-time wireless sensor network applications.

Therefore, this methodology is an accurate, safe solution for real-time threat detection of Wireless Sensor Networks while keeping the optimal capabilities to attack identification and data, distributed storage to increase the degrees of freedom of the network.

4. Results and Discussions

The outcomes and analysis of the suggested technique, Blockchain-Enhanced Detection of Malicious Nodes in WSNs Using Parallel Triple Graph Attention-based Convolution Network (Tri-QPdCNet), are shown in this section. The evaluation of the proposed method is simulated in Python. This research is tested over two datasets: WSN-DS and WSN-BFSF. Table 2 provides the simulation parameters for the proposed research.

Table 2. Simulation parameter

Simulation Parameters/Hyperparameters	Description
Datasets used	WSN-DS and WSN-BFSF
Simulation Tool	Python
Number of sensors	100-120
Sensing range	50 m
Transmission range	40-80 m
Node Energy (Initial)	0.5 Joules per sensor
Activation Functions	ReLU (hidden), Softmax (output)
Optimizer for Training	RMRO
Learning Rate	0.001 (adaptive decay)
Batch Size	64
Epochs	100
Dropout	0.3 (to prevent overfitting)
Loss Function	Cross-Entropy
RMRO Population Size	30 agents
RMRO Iterations	100
Termination Condition	Minimum error < 1e-5 or max iterations

The experiments were conducted using the WSN-DS and WSN-BFSF datasets in Python, simulating 100–120 sensors with a 50 m sensing range, 40–80 m transmission range, and 0.5 J initial energy. The Tri-QPdCNet employed ReLU activation for hidden layers and Softmax at the output. Training utilized RMRO optimizer with a learning rate of 0.001, batch size of 64, and 100 epochs. Additional settings included 0.3 dropout, cross-entropy loss, 30-agent RMRO population, 100 iterations, and termination at error < 1e-5.

Implementation Details

The implementation of Tri-QPdCNet with RMRO optimization was conducted to ensure reproducibility, utilizing publicly available datasets WSN-DS [29] and WSN-BFSF [30] from Kaggle. Preprocessing steps such as feature normalization and attack-class balancing were handled by the Lo-GDN module, which extracts local graph dependencies to improve training quality. The model was implemented in Python 3.10 with TensorFlow 2.12 on an Intel i7 CPU with 16 GB RAM. For blockchain integration feasibility, a CA-PoA-BE-based blockchain framework is adopted by assigning validation tasks to cluster heads or edge gateways instead of resource-constrained sensor nodes, thereby reducing computational load, minimizing energy consumption, and enabling deployment in real-world WSNs. The lightweight CA-PoA-BE consensus mechanism ensures low latency, making it suitable for time-sensitive anomaly detection in large-scale networks.

4.1. Dataset Description

A. WSN-DS

The Wireless Sensor Network Dataset (WSN-DS) [29] was created to enhance the detection and classification of Denial of Service (DoS) attacks. It allows sensor nodes to distinguish typical network behaviors from malicious signatures, enabling timely identification of potential attackers and informed response measures. The dataset was constructed using the LEACH routing protocol, extracting 23 attributes for each node's operational status. The dataset categorizes four types of DoS attacks: Blackhole, Grayhole, Flooding, and Scheduling (TDMA) attacks, and a "Normal" category for nodes free from malicious influence. This comprehensive classification approach ensures the dataset covers both attack-related and benign behaviors, enabling the development of robust intrusion detection models specifically tailored to wireless sensor networks.

B. WSN-BFSF

The WSN-BFSF dataset is a comprehensive resource for analyzing Wireless Sensor Network (WSN) traffic, including instances of Blackhole, Flooding, and Selective Forwarding attacks. It contains 312,106 entries with 16 unique features, providing a detailed framework for analyzing traffic patterns alongside normal network activity. The dataset includes a diverse array of traffic types, including Blackhole attacks, Flooding attacks, Selective Forwarding attacks, and regular network traffic. After a meticulous preprocessing phase, it is a valuable asset for understanding vulnerabilities and cyber threat behaviors in WSNs. Dataset available at [30]. Table 3 provides the data distribution for the WSN-DS and WSN-BFSF datasets.

Table 3. Training and testing data distribution in WSN datasets

Datasets	The Traffic Type	Training Set	Testing Set
WSN-DS dataset	Blackhole	8104	1945
	Grayhole	10,598	2624
	Flooding	2405	597
	TDMA	5306	1322
	Normal	259,621	65,020
WSN-BFSF dataset	Normal	210,223	52,628
	Flooding	23,913	5931
	Blackhole	9441	2325
	Forwarding	6108	1537

Table 3 shows that the WSN-DS and WSN-BFSF contain large training and testing sets across different traffic types. The WSN-DS dataset includes Blackhole, Grayhole, Flooding, TDMA attack and normal wireless nodes, comprising 259,621 nodes for the training set and 65,020 nodes for the test set. Likewise, the WSN-BFSF dataset divides the data into Normal, Flooding, Blackhole and Forwarding with a significant amount of normal nodes (210,223 for training data and 52,628 for test data). Note that these large and diverse samples ensure that all the training coverage required for the correct identification and categorization of attacks in WSNs is provided.

4.2. Performance Analysis

The performance of the proposed BLogDirHip is analysed and compared with HGB [16], DT [17], MLSTL-WSN [18], IRADA [19], Wsn-bfsf [20], GSWO-CatBoost [21], and SCNN-Bi-LSTM-AVOA-FL [22]. The performance metrics are listed below:

Table 4. Performance metrics

Performance metrics	Formula
Accuracy	$A = \frac{\delta + \chi}{\delta + \varpi + \zeta + \chi}$
Precision	$P = \frac{\delta}{\delta + \zeta}$
Sensitivity	$S_e = \frac{\delta}{\delta + \chi}$
Specificity	$S_p = \frac{\varpi}{\varpi + \zeta}$
RMSE	$RMSE = \sqrt{\frac{1}{V}\sum_{t=1}^{V}(k_t - \hat{k}_t)^2}$

A. Performance Metrics

The performance measures like detection accuracy, attack classification, and secure storage, and the analysis of the proposed algorithm are carried out using the Tri-QPdCNet method. The performance metrics used in the evaluation of the proposed algorithm are tabulated in Table 4.
where δdenotes the true positive, ϖ denotes the true negative, ζ denotes the false positive χ represents the false negative. Table 5 evaluates the blockchain-specific aspects of each model.

Table 5. Comparative analysis of blockchain efficiency and security

Methods	Consensus Efficiency(%)	Fault Tolerance (%)	Storage Efficiency (%)	Security (%)	Data Integrity (%)	Execution Time (ms)
HGB [16]	94.5	93.7	92.9	94.0	91.8	110
DT [17]	92.3	91.9	90.8	91.3	90.0	105
MLSTL-WSN [17]	95.8	94.6	94.2	95.1	93.5	98
IRADA [18]	93.4	92.5	91.5	92.7	91.2	120
Wsn-Bfsf [19]	96.7	96.0	95.5	96.8	95.1	115
GSWO-CatBoost [20]	97.2	97.1	96.5	97.4	96.7	95
SCNN-Bi-LSTM [22]	98.0	97.8	97.4	97.9	97.2	90
Tri-QPdCNet (Proposed)	99.5	99.4	99.2	99.6	99.0	85

Experimental results and analysis of the compared methods of blockchain are presented in Table 5 in terms of efficiency and security indicators. The proposed algorithm Tri-QPdCNet performs significantly better as compared with the others with average consensus efficiency of 99.5%, fault tolerance of 99.4% and security of 99.6% in the field of blockchain. It also shows high capability in storing and retrieving data with efficiency of 99.2% and 99.0% in data integrity respectively. Being the fastest among the existing methods, it has an execution time of 85ms and this makes it deliver the best of both the performance and security measures.

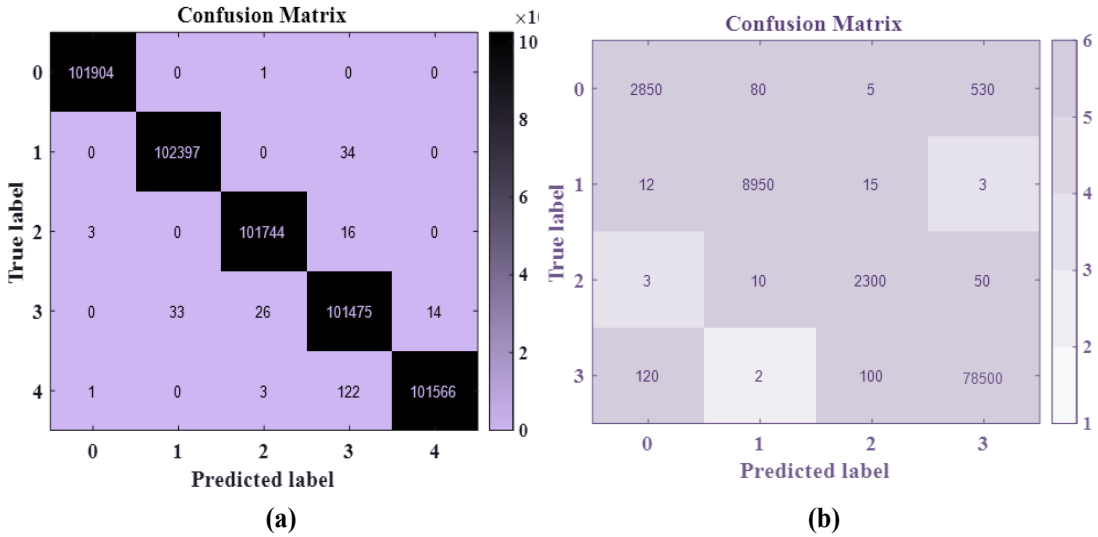


Fig.4. Confusion Matrix Interpretation

The confusion matrices in Figure 4(a) and 4(b) exhibit the proposed classifiers' classification performance with respect to the WSN-DS and WSN-BFSF datasets. For WSN-DS in 4(a), the high diagonal values (e.g., 101904, 102397) illustrate that the proposed model achieves accurate classification with fewer numbers of misclassified samples with reference to each class. In 4(b) WSN-BFSF the proposed model provides good results where majority of the predictions are found in diagonal, for example 78500 correct predictions for class 3. But some of the off-diagonal elements which are negative are also meaningful, such as 120 from class 0 to class 3 which means occasional misclassification. Each of these matrices demonstrates the model's performance for each of the datasets.

Figure 5 shows a Comparative Analysis of Intrusion Detection Accuracy in WSN-DS and WSN-BFSF Datasets. The graphs compare detection metrics—Accuracy, False Rejection Rate (FRR), and False Negative Rate (FNR)—across Blackhole, Grayhole, Flooding, TDMA, and Normal categories for (a) WSN-DS and Blackhole, Grayhole, Flooding, and Normal categories for (b) WSN-BFSF datasets. Both datasets show high accuracy, exceeding 99% for all categories, with low FRR and FNR values. The consistency in results highlights the models' robust performance in identifying normal and intrusion behaviors across various attack types, reinforcing their reliability in Wireless Sensor

Networks (WSN).

The performance of proposed models: accuracy, precision, recall, specificity, and F1 score on WSN-DS and WSN-BFSF are shown in figure 6(a), 6(b). The proposed Tri-QPdCNet model obtained 99.4% accuracy, 99.3% recall, and 99.5% F1 score by the WSN-DS; 99.2% accuracy, 99.1% precision, and 99.3% F1 score by the WSN-BFSF; therefore, it is efficient. Figure 6(c) represents the transaction cost figure and compares the cost of storing data with that of storing hashes as needed for efficient resource utilization.

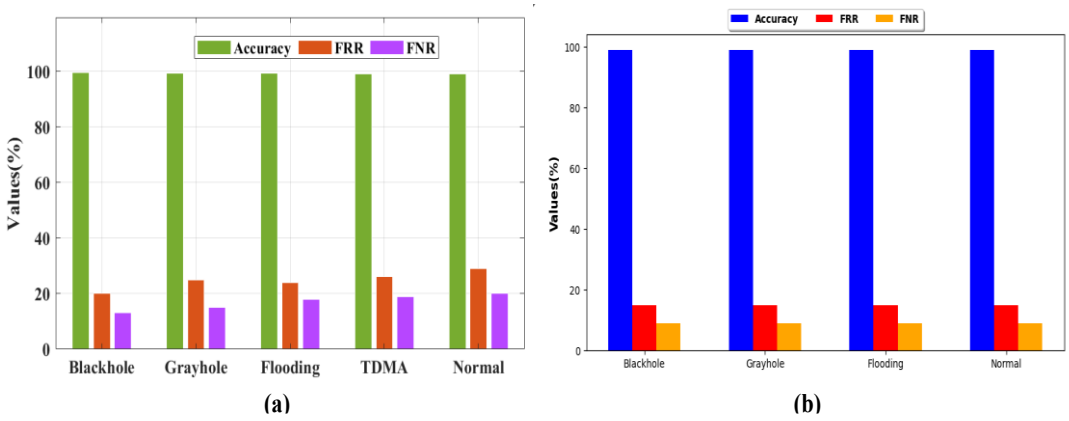


Fig.5. Comparative analysis of intrusion detection accuracy in WSN-DS and WSN-BFSF datasets

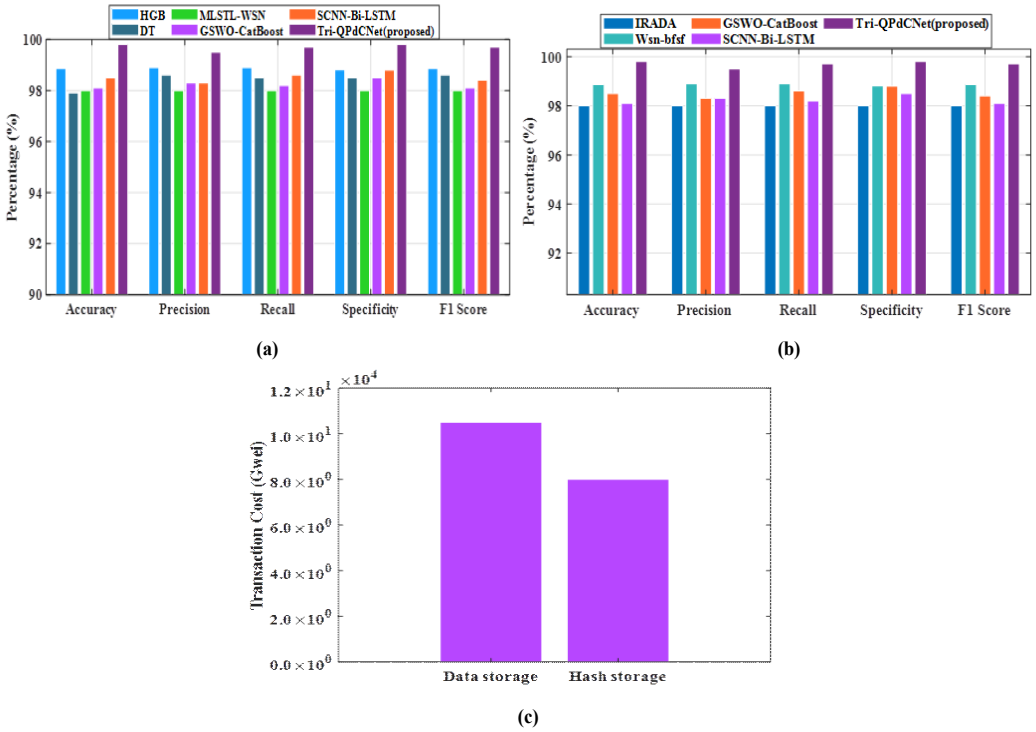


Fig.6. Performance metrics for WSN-DS and WSN-BFSF datasets and transaction costs

In figures 7(a) and 7(b), bar charts are shown with Mean Absolute Error (MAE), Root Mean Square Error (RMSE), and Mean Square Error (MSE) for the models on WSN-DS and WSN-BFSF, respectively. The proposed Tri-QPdCNet model obtains the lowest errors in terms of all four measurement metrics in comparison with other models. In both cases, the ROC curves of 7(c) and 7(d) denote high classification performance with an area under the curve (AUC) evaluated very close to 1, which points to higher model discrimination. Using both the error metrics and subsequent classification accuracy, the Tri-QPdCNet demonstrates a set of positive outcomes.

Figure 8 analyzes the real-world deployment cost of the proposed CA-PoA-BE blockchain framework in wireless sensor networks. Figure 8(a) shows the cost distribution across major factors, where energy consumption (25%) is the largest contributor, followed by hardware, scalability, and deployment costs (20% each), while communication overhead (15%) has the lowest impact. Figure 8(b) presents cumulative cost implications, confirming that although blockchain introduces additional resource requirements, the overall trade-off remains feasible, enabling secure anomaly detection without critically burdening WSN resources.

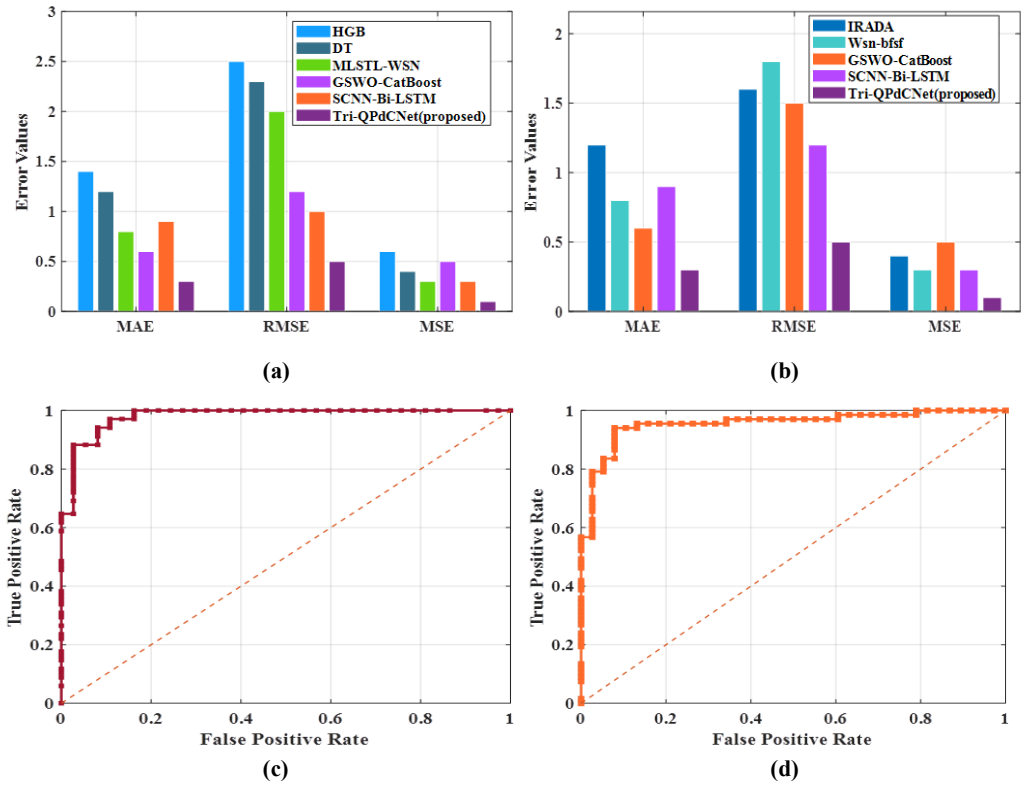


Fig.7. Error metrics and ROC curve analysis for WSN-DS and WSN-BFSF models

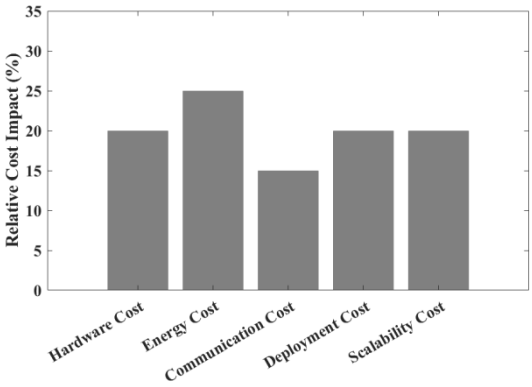


Fig.8. Real-world deployment cost of blockchain infrastructure in WSNs

4.3. Statistical Analysis

The statistical analysis evaluates the performance of intrusion detection methods across two benchmark datasets: WSN-DS (Dataset 1), which contains diverse Denial-of-Service (DoS) attack types, and WSN-BFSF (Dataset 2), focused on Blackhole, Flooding, and Selective Forwarding attacks. By comparing accuracy, confidence intervals, and p-values, table 6 highlights the effectiveness of existing models and validates the superior reliability of the proposed Tri-QPdCNet framework.

Table 6 presents the statistical analysis comparing existing methods with the proposed Tri-QPdCNet. Across both WSN-DS and WSN-BFSF datasets, Tri-QPdCNet achieves the highest accuracy (99.4% and 99.2%) with narrow confidence intervals, demonstrating consistent reliability. Its p-values (1.0e-30, 1.0e-28) confirm statistically significant superiority over prior methods such as GSWO-CatBoost (98.5%, 98.0%) and SCNN-Bi-LSTM (98.9%, 98.6%). These results highlight the robustness of Tri-QPdCNet in outperforming existing intrusion detection models.

4.4. Ablation Study

The ablation study in Table 7 evaluates the individual impact of key components within the proposed framework, namely Lo-GDN, BoT-CHO, and RMRO. By systematically removing each element from Tri-QPdCNet, the analysis reveals how performance is influenced on both WSN-DS (Dataset 1) and WSN-BFSF (Dataset 2). This comparison highlights the necessity of each module and demonstrates that the full integration yields the highest accuracy and robustness.

Table 6. Statistical analysis of the proposed method

Methods	Dataset 1			Dataset 2		
	Accuracy (%)	95% CI	p-value	Accuracy (%)	95% CI	p-value
HGB [16]	96.80	(96.67 – 96.93)	6.26e-284	96.20	(96.05 – 96.35)	5.90e-274
DT [17]	95.10	(94.94 – 95.26)	0.00e+00	94.50	(94.32 – 94.68)	0.00e+00
MLSTL-WSN [17]	97.50	(97.38 – 97.61)	4.94e-186	96.90	(96.76 – 97.03)	6.41e-190
IRADA [18]	96.40	(96.26 – 96.53)	0.00e+00	95.80	(95.64 – 95.95)	0.00e+00
Wsn-Bfsf [19]	97.90	(97.79 – 98.00)	1.85e-133	97.30	(97.17 – 97.42)	1.41e-144
GSWO-CatBoost [20]	98.50	(98.41 – 98.59)	1.21e-62	98.00	(97.89 – 98.11)	8.39e-73
SCNN-Bi-LSTM [22]	98.90	(98.82 – 98.97)	6.33e-25	98.60	(98.50 – 98.69)	2.53e-24
Tri-QPdCNet (Proposed)	99.40	(99.34 – 99.45)	1.0e-30	99.20	(99.13 – 99.27)	1.0e-28

Table 7. Ablation study of the proposed method

Methods	Accuracy (%)	
	Dataset 1	Dataset 2
Tri-QPdCNet without Lo-GDN	96.80	96.20
Tri-QPdCNet without BoT-CHO	97.40	96.90
Tri-QPdCNet without RMRO	98.60	98.20
Proposed Model	99.40	99.20

Table 7 presents the ablation study analyzing the contribution of each component in the proposed framework. Removing Lo-GDN reduces accuracy to 96.8% and 96.2%, showing its role in capturing local graph dependencies. Excluding BoT-CHO achieves 97.4% and 96.9%, reflecting weaker contextual optimization. Without RMRO, performance improves but remains lower at 98.6% and 98.2%, highlighting the optimizer's importance. The full proposed model delivers the highest accuracy (99.4%, 99.2%), confirming the complementary impact of all components.

4.5. Discussions

The results demonstrate the effectiveness of the proposed Tri-QPdCNet with CA-PoA-BE blockchain integration in improving anomaly detection and security within WSNs. The simulation setup (Table 2) included 100–120 sensors, a sensing range of 50 m, transmission range of 40–80 m, and initial energy of 0.5 J. Training was performed with RMRO optimization, ReLU and Softmax activations, 0.001 learning rate, 64 batch size, 100 epochs, and a dropout of 0.3. Implementation details confirmed reproducibility using WSN-DS and WSN-BFSF datasets, with Lo-GDN preprocessing to enhance feature quality.

Dataset descriptions (Section 4.1, Table 3) highlight the diversity of attack and normal traffic samples, ensuring robust evaluation across both datasets. Performance metrics (Table 4) guided the evaluation, covering accuracy, precision, sensitivity, specificity, and RMSE. Comparative blockchain analysis (Table 5) shows that Tri-QPdCNet surpasses prior methods with consensus efficiency (99.5%), fault tolerance (99.4%), security (99.6%), storage efficiency (99.2%), and execution time (85 ms), indicating superior reliability.

The confusion matrices in Figure 4 reveal high classification accuracy across all classes, with only limited misclassifications. Similarly, Figure 5 confirms detection accuracy above 99% across multiple attack types, supported by consistently low FRR and FNR values. Performance metrics in Figure 6 demonstrate accuracy of 99.4% (WSN-DS) and 99.2% (WSN-BFSF), alongside efficient transaction costs. Error metrics and ROC analysis (Figure 7) further validate the model's robustness, with AUC values approaching 1.

Finally, Figure 8 presents real-world deployment costs of CA-PoA-BE, showing energy (25%) as the highest factor but confirming feasibility under balanced trade-offs. Statistical analysis (Table 6) and ablation study (Table 7) underline the model's superiority, with accuracy gains attributable to Lo-GDN, BoT-CHO, and RMRO integration. Overall, results validate the framework's scalability, efficiency, and resilience for WSN security.

5. Conclusions

The proposed framework provides an advanced solution for resilient, proactive anomaly detection in Wireless Sensor Networks (WSNs). Implemented in NS-2, this framework showed high efficiency for all special indexes, including detection accuracy, precision, recall and F1-score, exceeding 99%. Through this, blockchain and a graph attention mechanism are implemented to guarantee high accuracy in detecting corrupted nodes and reliable isolation of

such nodes to minimize their negative impact on other nodes. The main benefits are extensibility to easily scale up the cellular depth in environments with high node density in WSN and decentralized data storage through IPFS, which prevents single points of failure and tamper attacks. It is envisaged that the combination of blockchain and attention-based convolutional mechanisms guarantees high accuracy in detecting the malicious nodes and provides the corresponding isolating mechanisms to prevent the overall network from being compromised. The key benefits include extensibility in WSN contexts with a large nodal density and use of distributed data storage based on the IPFS that proactively addresses the issues of single-point failures and tampering risks.

The proposed framework is well-suited for real-time applications in domains such as smart cities and environmental monitoring, where timely identification and isolation of malicious nodes are critical. However, limitations remain in terms of computational cost, scalability under heavy data flow, and the energy overhead introduced by blockchain integration at cluster heads or gateways. Addressing these issues through lightweight optimization strategies and advanced consensus mechanisms forms a promising direction for future work, enabling broader applicability to large-scale WSN deployments with improved efficiency and robustness.

Author Contributions Statement

J. Jabez-Conceptualization, Methodology, Writing - Original Draft, Writing - Review & Editing, Supervision,
N. Jayanthi- Formal analysis, Investigation, Resources, Validation, Writing - Original Draft
Elangovan Muniyandy- Project administration, Data Curation, Software.
R. Mohanapriya-Supervision, Writing - Review & Editing.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

Authors do not have any conflict of interest to declare.

Funding Declaration

No funding is provided for the preparation of manuscript.

Data Availability Statement

Data sharing not applicable to this article.

Ethical Declarations

This article does not contain any studies with human participants or animals performed by any of the authors.

Acknowledgments

Not applicable.

Declaration of Generative AI in Scholarly Writing

AI tools were used only for minor grammar checking and language refinement. All methodological development, analysis, and technical content were entirely carried out by the authors without AI assistance.

Abbreviations

The following abbreviations are used in this manuscript:
WSN - Wireless Sensor Network
IPFS - InterPlanetary File System
IDS - Intrusion Detection System
Lo-GDN - Localized-Global Depth Normalization
BoT-CHO - Boosted Tern-Cat Hunting Optimization
Tri-QPdCNet - Parallel Triple Graph Attention-Based Convolution Network
RMRO - Resilient Mud Ring Optimizer
CA-PoA-BE - Consensus Aided PoA Blockchain Engine
IPFS - InterPlanetary File System
HGB - Histogram Gradient Boost
DoS - denial-of-service
IRADA - Integrated Reinforcement Learning and Deep Learning Algorithm
IDSs - Intrusion Detection Systems
DL - Deep Learning
RL - Reinforcement Learning
GSWO - Genetic Sacrificial Whale Optimization
SCNN - Stacked Convolutional Neural Networks

Lo-GDN - Localized-Global Depth Normalization
CHuntO - Cat Hunting Optimization
BSooT - Boosted Sooty Tern Optimization
Tri-GAN - Triple Graph Attention Network
QPdCNet - Quantum Parallel deep Convolution Network
RMRO - Resilient Mud Ring Optimizer
CA-PoA-BE - Consensus-Aided PoA Decision Blockchain Engine
IPFS - InterPlanetary File System
MAE - Mean Absolute Error
RMSE - Root Mean Square Error

Reference

[1] A. K. S. Yadav, S. S. Sivaraju, B. Radha, M. Sushith, S. Srithar, and M. Kanchana, "Malicious node detection using SVM and secured data storage using blockchain in WSN," Int. J. Syst. Assur. Eng. Manag., vol. •••, pp. 1–11, 2024. DOI: 10.1007/s13198-024-02564-9

[2] G. G. Gebremariam, J. Panda, and S. Indu, "Blockchain-Based Secure Localization against Malicious Nodes in IoT-Based Wireless Sensor Networks Using Federated Learning," Wirel. Commun. Mob. Comput., vol. 2023, no. 1, p. 8068038, 2023. DOI: 10.1155/2023/8068038

[3] X. Yang, Y. Chen, X. Qian, T. Li, and X. Lv, "BCEAD: A Blockchain-Empowered Ensemble Anomaly Detection for Wireless Sensor Network via Isolation Forest," Secur. Commun. Netw., vol. 2021, no. 1, p. 9430132, 2021. DOI: 10.1155/2021/9430132

[4] M. A. Almaiah, "A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology," in Artificial intelligence and blockchain for future cybersecurity applications. Cham: Springer International Publishing, 2021, pp. 217–234. DOI: 10.1007/978-3-030-74575-2_12

[5] L. K. Ramasamy, F. K. KP, A. L. Imoize, J. O. Ogbebor, S. Kadry, and S. Rho, "Blockchain-based wireless sensor networks for malicious node detection: A survey," IEEE Access, vol. 9, pp.128765–128785, 2021. DOI: 10.1109/ACCESS.2021.3111923

[6] A. Rehman, S. Abdullah, M. Fatima, M. W. Iqbal, K. A. Almarhabi, M. U. Ashraf, et al., "Ensuring security and energy efficiency of wireless sensor network by using blockchain," Appl. Sci. (Basel), vol. 12, no. 21, p. 10794, 2022. DOI: 10.3390/app122110794

[7] R. R. Chandan, A. Balobaid, N. L. S. Cherukupalli, G. H L, F. Flammini, and R. Natarajan, "Secure modern wireless communication network based on blockchain technology," Electronics (Basel), vol. 12, no. 5, 1095, 2023.

[8] S. J. Hsiao and W. T. Sung, "Employing blockchain technology to strengthen security of wireless sensor networks," IEEE Access, vol. 9, pp. 72326–72341, 2021.

[9] O. A. Khashan, "Blockchain-machine learning fusion for enhanced malicious node detection in wireless sensor networks," Knowl. Base. Syst., vol. 304, p. 112557, 2024. DOI: 10.1016/j.knosys.2024.112557

[10] A. U. Khan, M. B. E. Sajid, A. Rauf, M. N. Saqib, F. Zaman, and N. Javaid, "Exploiting Blockchain and RMCV-Based Malicious Node Detection in ETD-LEACH for Wireless Sensor Networks," Wirel. Commun. Mob. Comput., vol. 2022, no. 1, p. 7281872, 2022. DOI: 10.1155/2022/7281872

[11] A. Saeed, M. U. Javed, A. Almogren, N. Javaid, and M. Jamil, "Employing blockchain and IPFS in WSNs for malicious node detection and efficient data storage," Wirel. Netw., vol. 30, no. 4, pp. 1–16, 2024. DOI: 10.1007/s11276-023-03648-3

[12] S. Awan, N. Javaid, S. Ullah, A. U. Khan, A. M. Qamar, and J. G. Choi, "Blockchain based secure routing and trust management in wireless sensor networks," Sensors (Basel), vol. 22, no. 2, p. 411, Jan. 6 2022. DOI: 10.3390/s22020411

[13] A. E. Guerrero-Sanchez, E. A. Rivas-Araiza, J. L. Gonzalez-Cordoba, M. Toledano-Ayala, and A. Takacs, "Blockchain mechanism and symmetric encryption in a wireless sensor network," Sensors (Basel), vol. 20, no. 10, p. 2798, May 14 2020.

[14] V. L. Vinya, Y. Anuradha, H. R. Karimi, P. B. Divakarachari, and V. Sunkari, "A Novel Blockchain Approach for Improving the Security and Reliability of Wireless Sensor Networks Using Jellyfish Search Optimizer," Electronics (Basel), vol. 11, no. 21, p. 3449, 2022. DOI: 10.3390/electronics11213449

[15] D. P. Rajan, J. Premalatha, S. Velliangiri, and P. Karthikeyan, "Blockchain enabled joint trust (MF-WWO-WO) algorithm for clustered-based energy efficient routing protocol in wireless sensor network," Trans. Emerg. Telecommun. Technol., vol. 33, no. 7, p. e4502, 2022. DOI: 10.1002/ett.4502

[16] M. Nouman, U. Qasim, H. Nasir, A. Almasoud, M. Imran, and N. Javaid, "Malicious node detection using machine learning and distributed data storage using blockchain in WSNs," IEEE Access, vol. 11, pp. 6106–6121, 2023. DOI: 10.1109/ACCESS.2023.3236983

[17] M. A. Elsadig, "Detection of Denial-of-Service Attack in Wireless Sensor Networks: A lightweight Machine Learning Approach," IEEE Access, vol. 11, pp. 83537–83552, 2023. DOI: 10.1109/ACCESS.2023.3303113

[18] M. A. Talukder, S. Sharmin, M. A. Uddin, M. M. Islam, and S. Aryal, "MLSTL-WSN: Machine learning-based intrusion detection using SMOTETomek in WSNs," Int. J. Inf. Secur., vol. 23, no. 3, pp. 2139–2158, 2024. DOI: 10.1007/s10207-024-00833-z

[19] V. Shakya, J. Choudhary, and D. P. Singh, "IRADA: Integrated reinforcement learning and deep learning algorithm for attack detection in wireless sensor networks," Multimedia Tools Appl., vol. 83, no. 28, pp. 1–20, 2024. DOI: 10.1007/s11042-024-18289-7

[20] M. Dener, C. Okur, S. Al, and A. Orman, "Wsn-bfsf: A new dataset for attacks detection in wireless sensor networks," IEEE Internet Things J., 2023.

[21] T. M. Nguyen, H. H. P. Vo, and M. Yoo, "Enhancing Intrusion Detection in Wireless Sensor Networks Using a GSWO-CatBoost Approach," Sensors (Basel), vol. 24, no. 11, p. 3339, May 23 2024. DOI: 10.3390/s24113339

[22] S. R. Jena, M. Z. U. Rahman, D. K. Sinha, V. Vimal, K. U. Singh, T. Syamsundararao, et al., "An Innovative Secure and Privacy-Preserving Federated Learning Based Hybrid Deep Learning Model for Intrusion Detection in Internet-Enabled Wireless Sensor Networks," IEEE Trans. Consum. Electron. p. 1, 2024. DOI: 10.1109/TCE.2024.3442015
[23] L. Li, Z. Liang, X. Liang, and S. Li, "Monocular Depth Estimation Based on Residual Pooling and Global-local Feature Fusion," IEEE Access, vol. 12,122785–122794, 2024. DOI: 10.1109/ACCESS.2024.3453942
[24] K. Dhanushkodi, R. Sethuraman, P. Mariappan, and A. Govindarajan, "An efficient cat hunting optimization-biased ReLU neural network for healthcare monitoring system," Wirel. Netw., vol. 29, no. 8, pp. 3349–3365, 2023. DOI: 10.1007/s11276-023-03373-x
[25] E. H. Houssein, D. Oliva, E. Celik, M. M. Emam, and R. M. Ghoniem, "Boosted sooty tern optimization algorithm for global optimization and feature selection," Expert Syst. Appl., vol. 213, p. 119015, 2023. DOI: 10.1016/j.eswa.2022.119015
[26] M. Liang, P. Cao, and J. Tang, "Rolling bearing fault diagnosis based on feature fusion with parallel convolutional neural network," Int. J. Adv. Manuf. Technol., vol. 112, no. 3, pp. 819–831, 2021. DOI: 10.1007/s00170-020-06401-8
[27] X. Wang, Y. Zhu, H. Shi, Y. Liu, and C. Hong, (2024). Graph Triple Attention Network: A Decoupled Perspective. arXiv preprint arXiv:.
[28] A. S. Desuky, M. A. Cifci, S. Kausar, S. Hussain, and L. M. El Bakrawy, "Mud Ring Algorithm: A new meta-heuristic optimization algorithm for solving mathematical and engineering challenges," IEEE Access, vol. 10, pp. 50448–50466, 2022. DOI: 10.1109/ACCESS.2022.3173401
[29] https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds
[30] https://www.kaggle.com/datasets/celilokur/wsnbfsfdataset

Authors' Profiles



J. Jabez (Jabez Jones) received M.E Computer Science degree from Sathyabama Institute of Science & Technology, Deemed to be University, Chennai Tamil Nadu in 2007. Ph.D degree from Computer Science department in the Year 2018 Sathyabama Institute of Science & Technology, Deemed to be University, Chennai, Tamil Nadu He has published many papers in reputed national and international Journals. His research interests include Artificial Intelligence, Machine Learning.



N. Jayanthi (Jayanthi Namasivayam) received B.E degree in CSE from Indira Gandhi College of Engineering & Technology, Chengalpattu affiliated to Anna University, Chennai, Tamil Nadu in 2014. M.E Degree in CSE from J.J College of Engineering & Technology, Trichy, Tamil Nadu affiliated to Anna University, Chennai, Tamil Nadu in 2023.



M. Elangovan has graduated with a Doctor of Engineering (Dr. Eng.) from Hiroshima University, Japan in the field of Naval Architecture and a master's degree (M. Eng.) in Engineering Design from Government College Technology, Coimbatore, Tamilnadu, India.

He is currently working as a Director (R&D and Consulting) at DTC Corp, Chennai. He provides high-level software development service on Python, SQL, AI and ML. He started his career as a Ship Designer at National Ship Design and Research Centre, Visakhapatnam which is a Central Government organization, and later, he worked for well-known companies like Jagson International Ltd, New Delhi, Allseas Engineering Dubai, IRS Mumbai, NAPA Finland, and GreenSHIP Bangalore. He has visited many countries like Japan, China, Korea, France, Brazil, Malaysia, Singapore for technical discussions and conferences. Altogether has got 24 years of industrial experience which includes five years of teaching at a university.

He was awarded a funded project from Naval Science and Technological Laboratory (NSTL), Visakhapatnam, India, and completed it with successful output. Altogether, he has completed research and consultancy projects worth 40 crores and Published more than 150 papers in journals and conferences. He is an editor for two journals and a reviewer for four journals. He has remarkable contributions in marine hydrodynamics, design, CFD, underwater marine vehicles, robotics, energies, sensors and industrial robots.



R. Mohanapriya (Mohanapriya Ramalingam) holds a Ph.D. in Wireless Networks from Anna University and an MBA in HR from Periyar University. A Gold Medalist in M.E. Applied Electronics, she topped her B.E. in ECE. With 13+ years as an Associate Professor at Paavai Engineering College, she specializes in Wireless Networks, Communication, and Signal Processing. She serves as the Institution's Innovation Council Convener and ATAL School Coordinator. She has delivered expert talks on IoT, 5G, and Entrepreneurship and published multiple international research papers and patents. She has submitted proposals to MSME, AICTE, and CSIR and mentored UG and PG projects. She is a Cambridge-certified BEC holder and a Certified Behavior Mentoring

Analyst. She has received the AICTE Lilavati Award 2022 and the Young Scientist Award 2020. A lifetime member of ISTE, IAENG, and IFERP, she actively contributes to academia and industry forums.

How to cite this paper: J. Jabez, N. Jayanthi, Elangovan Muniyandy, R. Mohanapriya, "Blockchain-enhanced Detection of Malicious Nodes in WSNs Using Parallel Triple Graph Attention-based Convolution Network", International Journal of Computer Network and Information Security(IJCNIS), Vol.18, No.2, pp.210-229, 2026. DOI:10.5815/ijcnis.2026.02.12