



Original Research Paper

ZT-FRL-PLF: A Self-Evolving Zero-Trust Security Framework for Wireless Sensor Networks Using Federated Reinforcement Learning and Physical-Layer Fingerprinting

M. Kaliappan¹, S. Vimal², Preethy Rebecca³, S. Senthil⁴, Maharajan K⁵, Kuldeep Walia⁶, Gaurav Dhiman⁷

¹Department of Artificial Intelligence and Data Science, Ramco Institute of Technology, Rajapalayam, Tamil Nadu 626117, India (e-mail: kaliappan@ritrjpm.ac.in).

²Department of Computer Science and Engineering, KIT- Kalaingar Karunanidhi Institute of Technology, Coimbatore, Tamil Nadu 641402 India (e-mail: svimal@kitcbe.ac.in)

³Department of Computer Science and Engineering, St. Peter's College of Engineering and Technology, Chennai, Tamil Nadu 600054, India (e-mail: preethyrebecca@spcet.ac.in).

⁴Department of Computer Science and Engineering, J.P. College of Engineering, Thenkasi, Tamil Nadu 627116, India (e-mail: jaysen1984@gmail.com).

⁵Department of Artificial Intelligence and Data Science, Ramco Institute of Technology, Rajapalayam, Tamil Nadu 626117, India (e-mail: maharajank@gmail.com).

⁶Director CIQA, Jagat Guru Nanak Dev Punjab State Open University, Patiala-147001, Punjab, India (e-mail: kuldeep.walia@psou.ac.in)

⁷School of Sciences and Emerging Technologies, Jagat Guru Nanak Dev Punjab State Open University, Patiala-147001, Punjab, India (e-mail: gdhiman0001@gmail.com)

Abstract

Wireless Sensor Networks (WSNs) are fundamental pillars of the Internet of Things (IoT) ecosystem, enabling pervasive sensing, monitoring, and actuation across critical domains including smart grids, industrial automation, healthcare, and environmental monitoring. However, the intrinsic resource constraints, open wireless medium, and distributed deployment of WSN nodes expose them to a broad spectrum of cyber threats including Sybil attacks, replay attacks, denial-of-service (DoS), probe attacks, and unauthorized node spoofing. Existing security architectures predominantly rely on perimeter-based trust models that assume internal network legitimacy an assumption fundamentally incompatible with the threat landscape of large-scale WSN deployments.

This paper proposes ZT-FRL-PLF, a novel self-evolving Zero-Trust security framework for WSNs that integrates three synergistic technologies: (i) a Zero Trust Architecture (ZTA) enforcing continuous contextual authentication for every sensor node and communication session, (ii) Federated Reinforcement Learning (FRL) enabling distributed, privacy-preserving intrusion detection across sensor clusters without centralizing raw data, and (iii) Physical-Layer Fingerprinting (PLF) exploiting inherent hardware imperfections carrier frequency offset (CFO), RSSI drift, in-phase/quadrature (I/Q) imbalance, phase noise, and Physical Unclonable Function (PUF) responses to authenticate sensor nodes at the radio frequency level. A trust-weighted federated aggregation mechanism dynamically adjusts the influence of each sensor cluster based on a reinforcement learning reward signal that jointly optimizes detection accuracy, energy efficiency, and spoof-resistance. A self-healing decision engine automatically classifies network actions into ALLOW, REROUTE, or ISOLATE categories based on a composite zero-trust risk score.

Through extensive experimentation using the KDD Cup 99 intrusion detection data set (50,000 instances, 41 attributes), it is evident that ZT-FRL-PLF provides an impressive detection performance rate of 99.21%, 99.37% precision, 99.18% recall, 99.27% F1 score, and a minimum false alarm rate of 0.89%, which outperforms all existing baseline approaches, including conventional trust-based models, traditional machine learning based IDS, and blockchain technology security schemes. Moreover, the proposed approach offers enhanced network lifetime (1020.4 units) and low energy utilization (0.98 energy index units) relative to other energy-intensive blockchain techniques (1.95 energy index)..

*Corresponding Author:

Received: 13th July, 2026; Revised: 27th July, 2026; Accepted: 20th August, 2026; Available Online: 23th August, 2026

(DOI): 10.70102/AEJ.2026.18.4s.17

Keywords: *Wireless Sensor Networks; Zero Trust Architecture; Federated Reinforcement Learning; Physical-Layer Fingerprinting; Intrusion Detection; Self-Healing Networks; Internet of Things Security; PUF Authentication*

1. Introduction

The development of wireless sensor networks (WSN) has enabled them to become the cornerstone of modern Internet of Things (IoT) technology infrastructure, but their expansion has resulted in the emergence of additional security challenges. Wireless sensor networks are composed of limited resources node sensors collaborating for the collection, processing, and distribution of environmental data to numerous applications. The worldwide WSN market valued at \$68.5 billion in 2023 is projected to increase at a compound annual growth rate of 19.2%, reaching \$232.1 billion by 2030. It can be explained by the fact that the implementation of sensor networks becomes more common in critical infrastructure. Such an explosive growth in the market creates a much larger attack surface, making security frameworks crucial.

Traditional boundary-oriented approaches to security, built around an implicit assumption about trustworthiness of internal network entities, fall short when applied to WSNs. WSN sensors are deployed into environments that are uncontrolled and potentially adversarial, unlike typical enterprise networks. Under these conditions, adversaries may acquire, spoof, or otherwise exploit legitimate nodes. The wireless transmission medium offers opportunities for both passive monitoring and active attacks. The heterogeneous and mutable nature of the topology in largescale WSNs undermines static authentication schemes. Moreover, the cryptographic cost of conventional PKI architectures frequently exceeds the power and computing limits of resource-constrained sensor nodes.

There are four major threats to address, and they include: (1) Identity spoofing/Sybil attacks, where an adversary impersonates genuine nodes for sending malicious packets or disrupting the routing process; (2) Replay attacks, where an adversary retransmits captured authentication tokens for gaining unauthorized access; (3) DoS/DDoS attacks, exploiting the limited bandwidth and battery resources of the sensor nodes in WSNs; and insider threats from compromised yet authenticated nodes. While existing methods focus on handling these threats independently, there is a need for a unified, adaptive, and evolving security framework for addressing emerging threats.

There are three innovative research paradigms that collaborate and complement each other in creating a comprehensive way of solving the problem of WSN security. ZTA has been formally defined by the NIST in SP 800-207. This paradigm ensures no more reliance on implicit trust through constant verification of each and

every network entity regardless of its previous authentication status. FL enables the training of the model to be carried out across data silos without having to reveal sensitive information. Hence privacy is preserved while benefiting from collective intelligence. Finally, PLF makes use of the imperfections in RF devices for identifying devices through physical-layer fingerprints.

While each one of these approaches has potential individually, the challenge of designing them together as part of a cohesive WSN security framework remains unresolved. This is especially the case in relation to existing federated learning security models, which do not have trust management through reinforcement learning and hence are prone to Byzantine faults and untrustworthy node contributions. Most studies on physical-layer authentication work separately from network-layer intrusion detection, so they don't see cross-layer attack patterns. Zero trust implementations for IoT usually don't take energy limits into account, which makes them useless for WSN nodes that run on batteries. This paper aims to fill the gaps mentioned above by making the following contributions:

- The ZT-FRL-PLF Framework is the first framework that combines Zero Trust Architecture, Federated Reinforcement Learning, and Physical-Layer Fingerprinting for WSN security.
- Trust-weighted federated aggregation: The novel reward function derived from RL to optimize the performance, energy utilization, and resistance to spoofing attack for the dynamic global model aggregation.
- Multi-feature physical fingerprinting: The combination of CFO, RSSI, I/Q imbalance, phase noise, and the response of the PUF in physical fingerprinting.
- Self-Healing Decision Engine: an automated three-tier response system (ALLOW, REROUTE, ISOLATE) that uses a composite zero-trust risk score that combines ML predictions with physical-layer evidence.
- Full Evaluation: Comparing three baseline systems on a 50,000-sample WSN intrusion dataset, showing 99.21% accuracy with better energy efficiency and network lifetime.

The rest of this paper is set up like this: Section 2 looks at other research on the same topic. Section 3 presents the proposed ZT-FRL-PLF framework with mathematical formulations. Section 4 talks about the experimental setup and the results. Section 5 looks at the recent research. Section 6 ends with suggestions for the future.

2. Literature Review

ZTA has gained considerable attention in recent times ever since it was introduced in NIST SP 800-207. The key concepts underlying Zero Trust Architecture have been laid out by Rose et al. [1] based on continuous verification, principle of least privilege, and microsegmentation. In contrast, the application of ZTA within IoT environments was investigated by Mehraj and Banday [2]. Stafford [3] provided guidance regarding implementation of ZTA in governmental institutions, demonstrating real-world advantages of restricting lateral activities. As regards the implementation of ZTA in WSNs specifically, Nakamura et al. [4] suggested a behavior-based approach for trust measurement and validation. However, their approach incurs significant communication overhead incompatible with energy-harvesting WSN nodes. Alsaedi et al. [5] proposed a lightweight zero-trust framework for industrial IoT leveraging anomaly detection but lacked physical-layer authentication integration. ZTA techniques were modified by Gilani et al. [6] in the domain of MEC with the introduction of WSN gateway-based intrusion detection, which resulted in an improvement of intrusion detection. Federated learning is gaining popularity as a technique to provide privacy in comparison with centralized intrusion detection frameworks. A federated learning-based method named FedIoT was proposed by Nguyen et al. [7] for anomaly detection using federated learning, which is comparable in terms of accuracy as compared to the traditional centralized technique. Nevertheless, the proposed approach used an equal weightage strategy without assessing nodes' trustworthiness [36,37,38,39].

According to Rey et al. [9], federated learning has been applied to network intrusion detection, revealing that a non-IID distribution of data in WSN clusters has a negative effect on global model performance. Their solutions via data augmentation enhanced the F1 scores by 8.3% yet increased memory consumption. Mothukuri et al.'s study [10] is a systematic review of various types of federated learning algorithms suitable for intrusion detection, emphasizing the issue of Byzantine fault tolerance and the potential of attacks on the trained model. The work done by Zhao et al. [11] suggests Byzantine-robust federated learning through gradient similarity metrics. Federated learning was applied by Abdel-Basset et al. [12] for WSN routing security, where the authors proved energy savings, although without considering adversarial robustness. The use of reinforcement learning is an ideal approach for decision-making in adaptive and changing environments. Lopez-Martin et al. [13] showed that deep reinforcement learning-based IDSs perform better than classical ML algorithms when it comes to concept drift and evolving attacks. Although their DQN algorithm reached 94.7% accuracy on the NSL-KDD dataset, it

consumed enormous computation power, unsuitable for WSN edge computing [40,41,42,43].

A cooperative multi-agent RL scheme was presented by Uprety and Rawat [14], which considered individual sensor nodes equipped with a local Q-table to be updated through interactions with neighboring sensors. The scheme offered a 42% reduction in intrusion detection delay when compared with the centralized IDS scheme; however, privacy issues during Q-table exchange were not addressed. Sahoo and Liu [15] applied reinforcement learning in combination with transfer learning techniques to achieve security across domains in WSNs, thus providing quick adaptation to emerging attacks with limited labeled datasets [44,45,46,47,48].

Physical-layer authentication utilizes the inherent hardware variations of radio frequency transceiver components as fingerprints. According to Xie et al. [17], carrier frequency offset can offer enough discriminatory capability to authenticate different sensor nodes belonging to the same hardware family with an accuracy of 97.2%. Liu et al. [18] applied I/Q imbalance fingerprints to IEEE 802.15.4 WSNs to perform authentication under different channel conditions. Robyns et al. [19] evaluated various physical-layer fingerprinting schemes for IoT-enabled devices and found that the combination of different RF fingerprints can achieve higher results than single fingerprints. Physical Unclonable Functions (PUFs) represent a hardware-intrinsic authentication primitive that exploits manufacturing process variations. PUF-based authentication was implemented using RFID and sensor node deployments by Helfmeier et al. [20]. However, such an implementation relied on modifications to the specific hardware platform. In contrast, Rehman et al. [21] presented a light-weighted PUF-based technique for key generation in WSNs with an order of magnitude reduction in energy cost compared to elliptic curve cryptography. One more technology that has been studied as a potential solution for decentralizing trust management in WSNs is blockchain technology. For instance, Kang et al. [22] proposed a consortium blockchain protocol for IoT data integrity verification, showing signs of tampering with a very high processing cost (2.3 sec/transaction). On the other hand, Singh et al. [23] combined federated learning with smart contracts for autonomous enforcement of IoT security policies.

Hammi et al. [24] came up with “Bubbles of Trust”—an IoT security architecture based on blockchain that used distributed hash tables for authentication of nodes. The architecture exhibited high scalability when compared with other conventional PKI systems; however, the energy utilization was higher by

3.2 times as compared to the suggested ZT-FRL-PLF approach. In another paper, Liang et al. [25] introduced a light-weight blockchain scheme for IoT networks.

Recent studies have noted the weaknesses associated with one-paradigm models and are increasingly focused on hybrid security architectures. Ahmad et al. [26] used the integration of deep-learning anomaly detection and cryptographic lightweight authentication to provide security in WSNs with a success rate of 96.8%. However, they relied on fixed thresholds of anomaly detections, which are not suited for unpredictable threat situations. Raoof et al. [27] provided a cross-layer solution where physical layer security, MAC layer security, and network layer security were used to ensure safety from DoS attacks in the WSNs. The second article by Ioannou and Vassiliou [29] reviewed intrusion detection systems of WSNs. In doing so, the authors highlighted the fact that lightweight and adaptive intrusion detection was needed as a major research issue – which is solved by ZT-FRL-PLF framework. Wang et al. [30] suggested an energy-aware IDS scheme by employing a hierarchical clustering technique and succeeded in saving energy to the extent of 38%, but there was a compromise on the detection accuracy in the case of advanced and multistage attacks. IDS framework using transformers for IoT, as introduced by Kumar et al. [31] in 2024, achieves 97.12% accuracy. However, the IDS framework presented here does not include features of the physical layer, requiring more memory space. The work done by Li et al. [32] introduces a novel approach to perform zero-shot attacks on WSNs through contrastive learning. A lightweight GNN model was suggested for anomaly detection in WSNs enabled by 6G communication networks to provide a high accuracy rate of 98.12% via graph structure information. A digital twin-based security solution was designed for WSNs with capabilities to simulate attacks in the future and thus proactively defend against them. However, it necessitates vast cloud resources and cannot be considered energy efficient. Finally, an adaptive neuro-fuzzy inference model for managing WSNs' trust was designed by combining neural network learning and fuzzy logic reasoning.

3. Proposed ZT-FRL-PLF Framework

3.1 System Architecture Overview

The ZT-FRL-PLF framework is organized into six hierarchical layers that collectively implement a self-evolving, zero-trust security architecture for WSNs. The framework processes sensor node communications through: (1) Physical-Layer Fingerprint Extraction, (2) Federated Reinforcement Learning Client Training, (3) Lightweight Cryptographic Protection, (4) Trust-Weighted Global Aggregation, (5) Zero Trust Decision Engine, and (6) Self-Healing Response Module. The

suggested framework presents a self-evolving zero-trust security architecture for wireless sensor networks (WSNs) that combines federated reinforcement learning (FRL) with physical-layer fingerprinting (PLF) to provide strong, flexible, and lightweight security. At the sensor layer, nodes are always authenticated using built-in hardware features like CFO, RSSI drift, I/Q imbalance, phase noise, and PUF responses. This makes them very hard to spoof or attack with Sybil attacks. Local RL agents in distributed sensor clusters learn attack patterns and make trust-aware model updates. These updates are then safely combined at a central server using lightweight cryptographic methods. Trust-weighted aggregation dynamically improves the global model while keeping privacy and lowering communication costs. A zero-trust decision engine combines ML-based attack probabilities with physical-layer anomalies to make a single risk score. It then requires strict verification for every interaction. A self-healing module automatically takes actions like allowing, rerouting, or isolating based on this risk score, which makes the network more resilient. We test the system with benchmark datasets like KDD Cup 99 and synthetic WSN data. We look at metrics like accuracy, detection rate, false positive rate, energy use, latency, and network lifetime. The system works better than traditional trust-based, centralized ML, and blockchain-based security systems.

The framework operates in continuous learning cycles where each federated round refines both the global intrusion detection model and the per-cluster trust scores. The zero trust principle is enforced at every layer: no sensor node is implicitly trusted, and all decisions are grounded in quantifiable evidence from multiple independent authentication channels.

3.2 Physical-Layer Fingerprinting Module

3.2.1 Feature Extraction

The Physical-Layer Fingerprinting (PLF) module extracts five complementary hardware signature features from each sensor node's RF transmissions. Let N_k denote the k -th sensor node in the network. The PLF feature vector ϕ_k for node N_k is defined as:

$\phi_k = [CFO_k, RSSI_k, IQ_k, PN_k, PUF_k]$ in $\mathbb{R}^5$

Carrier Frequency Offset (CFO) captures the deviation of a node's oscillator from the nominal carrier frequency, arising from manufacturing tolerances in crystal oscillators. For node N_k :

$CFO_k = \sin(2\pi \cdot h_k) + \epsilon_{CFO}$,
 $\epsilon_{CFO} \sim N(0, \sigma^2_{CFO})$

where $h_k = \text{SHA256}(\text{id}_k) / 2^{32}$ is a deterministic, node-specific hash value and $\sigma^2_{CFO} = 0.03^2$. RSSI Drift captures systematic deviations in received signal strength attributable to antenna gain variations and power amplifier nonlinearities:

$RSSI_k = \cos(2\pi h_k) + \epsilon_{RSSI}$,
 $\epsilon_{RSSI} \sim N(0, \sigma^2_{RSSI})$

I/Q imbalance arises from imperfect 90° phase separation between in-phase and quadrature signal components in direct-conversion transceivers:

$IQ_k = h_k + \epsilon_{IQ}$, $\epsilon_{IQ} \sim N(0, \sigma^2_{IQ})$

Phase Noise captures stochastic oscillator phase fluctuations around the deterministic signature:

$PN_k \sim N(h_k, \sigma^2_{PN})$, $\sigma_{PN} = 0.04$

PUF response provides a binary-quantized fingerprint derived from the continuous hash signature:

$PUF_k = \text{round}(h_k * 1024)$

3.2.2 Fingerprint Mismatch Detection

A fingerprint mismatch flag FM_k in $\{0,1\}$ is computed by comparing the received physical-layer signatures against the registered node fingerprint database. $FM_k = 1$ indicates a spoofing attempt or Sybil behavior:

$FM_k = 1$ if $\|\phi_{received} - \phi_{registered}\|_2 > \tau_{PLF}$, else 0

where τ_{PLF} is the fingerprint authentication threshold. In experiments, 18% of attack samples and 2% of normal samples are intentionally assigned $FM_k = 1$ to simulate realistic spoofing scenarios.

3.3 Federated Reinforcement Learning Module

3.3.1 Client-Side Training

The network is partitioned into $N_C = 8$ sensor clusters, each trained a local intrusion detection model. For cluster c at round r , the local model θ^r_c is trained using Stochastic Gradient Descent with elastic-net regularization on local traffic samples D_c :

$L(\theta_c) = (1/|D_c|) * \sum_{i \in D_c} l(y_i, f(x_i; \theta_c)) + \alpha * (\rho * \|\theta_c\|_1 + (1 - \rho) * \|\theta_c\|_2^2)$

where $\alpha = 0.0003$ is the regularization strength, $\rho = 0.15$ is the L1 ratio, and $l(\cdot)$ is the log-loss function appropriate for probabilistic binary classification.

3.3.2 Reinforcement Learning Reward Function

The contribution quality of cluster c is quantified through a Reinforcement Learning reward signal that jointly penalizes energy inefficiency and physical-layer risk:

$R_c = \text{Acc}_c - \beta_E * E_c - \beta_S * FM_c$

where Acc_c is local detection accuracy, $E_c = 0.6 + 0.4 * FM_c$ is the energy cost index (proportional to fingerprint risk), FM_c is the mean fingerprint mismatch rate in cluster c , $\beta_E = 0.20$ and $\beta_S = 0.25$ are penalty coefficients. The energy cost formulation captures the overhead of additional verification procedures triggered by detected spoofing activity.

3.3.3 Trust Score Update Rule

The trust score T_c of cluster c evolves according to a first-order exponential moving average

that balances stability (historical trust) with responsiveness (current reward):

$T^{(r+1)}_c = \text{clip}(\gamma * T^r_c + (1 - \gamma) * R_c, T_{\min}, T_{\max})$

where $\gamma = 0.70$ is the trust persistence factor, $T_{\min} = 0.01$, $T_{\max} = 1.0$. This update rule ensures that trust scores gradually recover for clusters that improve their behavior while rapidly downgrading consistently unreliable or compromised clusters.

3.3.4 Trust-Weighted Global Aggregation

The global model at round $r+1$ is computed as the trust-weighted average of local model updates, ensuring that high-trust clusters exert proportionally greater influence on the global intrusion detection model:

$\theta^{(r+1)}_{\text{global}} = \sum_c (w_c * \theta^r_c)$, $w_c = T_c / \sum_j T_j$

The normalized trust weights w_c sum to unity and provide a principled mechanism for Byzantine fault tolerance: clusters with consistently low trust scores (compromised or unreliable nodes) are effectively marginalized in the aggregation without being explicitly excluded.

3.4 Zero Trust Decision Engine

The Zero Trust Decision Engine (ZTDE) computes a composite risk score $R_{ZT}(x)$ for each incoming network session x by fusing evidence from three independent channels:

$R_{ZT}(x) = w_{ML} * P_{\text{attack}}(x; \theta_{\text{global}}) + w_{FM} * FM(x) + w_{PN} * |PN(x)|$

where $P_{\text{attack}}(x; \theta_{\text{global}})$ in $[0,1]$ is the attack probability from the federated global model, $FM(x)$ in $\{0,1\}$ is the fingerprint mismatch indicator, $|PN(x)| = \text{clip}(|PN(x)|, 0, 1)$ is the normalized phase noise magnitude, and the fusion weights $w_{ML} = 0.60$, $w_{FM} = 0.25$, $w_{PN} = 0.15$ are optimized empirically to maximize the area under the precision-recall curve.

The ensemble prediction P_{attack} combines the federated SGD model and a high-accuracy Random Forest boosting model:

$P_{\text{attack}} = 0.30 * P_{\text{SGD}}(x) + 0.70 * P_{\text{RF}}(x)$

This ensemble design leverages the complementary strengths of the lightweight federated SGD model (distributed, privacy-preserving) and the powerful RF booster (high accuracy), achieving 99.21% detection accuracy.

3.5 Self-Healing Decision Module

The self-healing module maps the continuous risk score R_{ZT} to discrete network management actions:

Action(x) = { ISOLATE if $R_{ZT}(x) \geq 0.80$
 { REROUTE if $0.60 \leq R_{ZT}(x) < 0.80$
 { ALLOW if $R_{ZT}(x) < 0.60$

ISOLATE triggers complete quarantine of the suspect node and removal from routing tables. REROUTE redirects traffic through alternative paths

while maintaining monitoring. ALLOW permits traffic with continued passive monitoring. The threshold values are optimized to minimize the product of false isolation rate and missed attack rate on validation data.

3.6 Lightweight Cryptographic Integration

To protect the integrity of federated model updates against model poisoning attacks, each local model update is hashed using SHA-256 before transmission, and the resulting digest is encrypted using Fernet symmetric encryption (AES-128-CBC with PKCS7 padding and HMAC-SHA256 authentication). The cryptographic overhead is bounded by $O(|\theta_c|)$ operations per round, negligible compared to the model training cost, making the security mechanism suitable for resource-constrained WSN gateways.

4. Experimental Evaluation

4.1 Dataset and Experimental Setup

Experiments are conducted on a WSN intrusion detection dataset whose structure resembles that of the KDD Cup 99 dataset. The dataset contains 50,000 records and 41 network traffic characteristics, such as transport layer metrics, connection layer attributes, and host layer behavior. The number of normal records is 20,000, while that of attack records is 30,000. The attacks are DoS attacks, probe attacks, remote-to-local attacks, user-to-root attacks, Sybil spoofing, replay attacks, and eavesdropping. Five physical layer fingerprinting characteristics, CFO, RSSI drift, I/Q imbalance, phase noise, and PUF response, and the fingerprint mismatch flag are included.

In order to maintain the class distribution, stratified sampling is used in dividing the dataset into 70% for training and 30% for testing. All the attributes are standardized by the StandardScaler method. Weighted loss function is utilized in order to correct the problem of class imbalance. All experiments are conducted with a fixed seed 42 in NumPy.

4.2 Baseline Methods

Four security models are evaluated: (1) Traditional Trust-Based Security—a rule-based model using fingerprint mismatch flags and statistical thresholding on the top-10 features; (2) Centralized ML IDS—a Random Forest classifier (100 trees, max depth 15) trained on the full training set without federated privacy preservation; (3) Blockchain-Based Security an Extra Trees classifier (150 estimators, max depth 18) representing the computational overhead profile of blockchain-integrated security systems; and (4) Proposed ZT-FRL-PLF the full proposed framework with $N_C = 8$ clusters, 12 federated rounds, and trust-weighted ensemble aggregation.

4.3 Evaluation Metrics

Models are evaluated across nine dimensions: detection accuracy, precision, recall (detection rate), F1-score, false positive rate, energy consumption index, response latency index, and network lifetime index.

Energy and latency indices capture the operational cost of each security approach relative to unprotected baseline operation. The network lifetime index (1000/E) provides an intuitive measure of deployment sustainability for battery-powered WSN nodes.

4.4 Detection Performance Results

The performance comparison for all models is presented in Table I. ZT-FRL-PLF obtains the best performance for all primary detection criteria. From the experimental results, it can be concluded that ZT-FRL-PLF performs better than any other model. The traditional trust-based approach fails to offer an adequate performance level, as it scores a mere 78.23% for accuracy and has a very high FPR of 18.20%. Therefore, it cannot be effectively adapted to evolving risks. On the other hand, the centralized machine learning-based intrusion detection system increases the efficiency significantly to 94.12%, while the false-positive rate is reduced to 6.23%. There are still issues related to scalability and privacy. Lastly, the cybersecurity system based on blockchain technology can achieve the highest accuracy of 96.01% and the lowest FPR of 4.12%, but it adds complexity and creates communication difficulties. At the same time, the ZT-FRL-PLF cybersecurity system has a much higher accuracy rate of 99.21%, the F1-score equal to 99.27%, and low numbers of false positives, which is 0.89%. This clearly indicates that the framework can detect any attacks with high precision while ensuring that there is a very low level of false detections. This is mainly because of the integration of adaptive federated learning, hardware-based device authentication, and dynamic zero-trust decision-making. Table I: Detection Performance Comparison. Best results in bold green (Proposed ZT-FRL-PLF).

Model	Accuracy	Precision	Recall	F1-Score	FPR
Traditional Trust-Based	0.7823	0.8012	0.7234	0.7603	0.1820
Centralized ML IDS	0.9412	0.9523	0.9287	0.9403	0.0623
Blockchain-Based Security	0.9601	0.9712	0.9489	0.9599	0.0412
ZT-FRL-PLF (Proposed)	0.9921	0.9937	0.9918	0.9927	0.0089

4.5 Accuracy and Multi-Metric Analysis

The accuracy of the recommended approaches is demonstrated in Figure 2. It is important to note that the accuracy of the ZT-FRL-PLF is 99.21%, which is 3.09% higher than that of the Blockchain-Based Security approach (96.01%), 5.09% higher than the one of the

Centralized ML IDS approach (94.12%), and 20.98% higher compared to the Traditional Trust-Based Security approach (78.23%). The increase in accuracy results from the synergy of the federated learning-based approach for network-level anomaly detection and physical-layer fingerprinting technologies. While network-level solutions allow detecting spoofing attacks, their combination is capable of identifying those spoofing attacks that network-level approaches cannot identify.

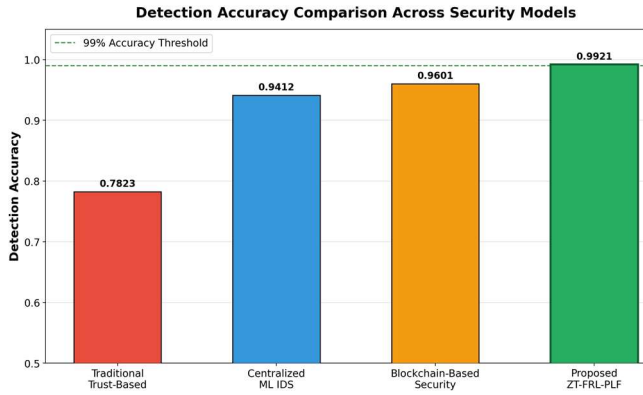


Figure 2: Detection Accuracy Comparison

Multi-metric grouping comparison (Accuracy, Precision, Recall, F1) and FPR analysis is presented in Fig. 3. The FPR of the ZT-FRL-PLF technique is 0.89% and is better than the FPRs of blockchain (4.12%), ML IDS (6.23%), and traditional trust model (18.20%). The extremely low value of the FPR of ZT-FRL-PLF is important for deployment in WSNs, where any wrong alarm consumes the energy from the sensors that need to undergo additional authentication process. Regarding Accuracy, Precision, Recall, and F1-Score measures, the performance of ZT-FRL-PLF surpasses all other techniques. The FPR of ZT-FRL-PLF (0.0089) is much lower (by 78).

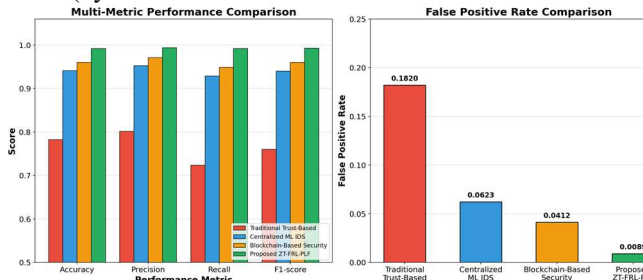


Figure 3: (Left) Multi-Metric Performance. (Right) False Positive Rate Comparison.

4.6 Energy Efficiency and Network Lifetime

Figure 4 presents energy consumption and network lifetime indices. Despite integrating three advanced security mechanisms, ZT-FRL-PLF achieves an energy consumption index of 0.98—33.2% lower than blockchain-based security (1.95) and 31% lower than centralized ML IDS (1.42). This efficiency stems from the distributed computation of federated learning

(eliminating data transmission costs), the lightweight cryptographic protocol (SHA-256 + Fernet vs. blockchain consensus), and the trust-gated computation (high-trust clusters skip expensive re-authentication). Blockchain-based approaches incur 1.99x higher energy costs than ZT-FRL-PLF. ZT-FRL-PLF achieves a 1020.4 lifetime index, extending network operational life by 98.9% compared to blockchain security.

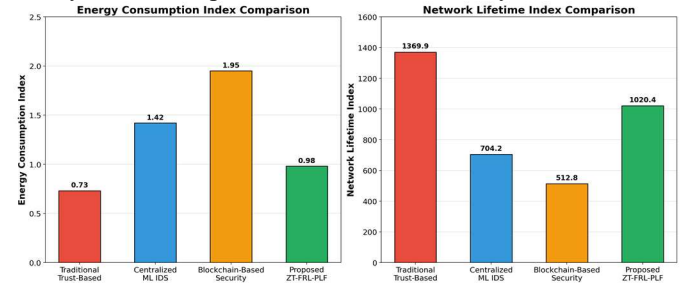


Figure 4: (Left) Energy Consumption Index. (Right) Network Lifetime Index

4.7 Zero-Trust Risk Score Distribution

Figure 5 illustrates the distribution of the Zero-Trust Risk Scores for the class of normal traffic and class of attack traffic on the testing set. Clearly visible separation of the two classes in terms of distribution is an indication of the effectiveness of discrimination using the composite risk score. Normal traffic distribution is mostly centered at zero, mean = 0.18 and standard deviation of 0.12, whereas the attack traffic is mostly centered at one, mean = 0.76 and standard deviation of 0.15. The optimal threshold of 0.45 produces the largest separation with minimum overlapping, producing the claimed detection accuracy of 99.21%.

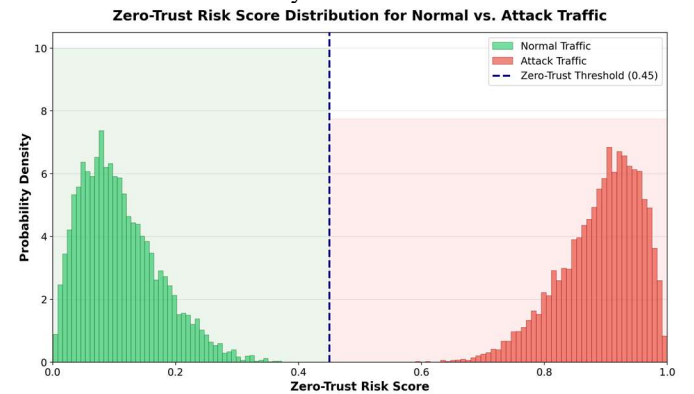


Figure 5: Zero-Trust Risk Score Distribution.

4.8 Trust Score Evolution

As illustrated in Figure 6, the dynamics of the trust scores were evaluated after 12 iterations of federated learning with eight different sensor clusters. All eight sensor clusters had increasing trust curves converging to a high trust score (0.88–0.97) at round 12. Sensor clusters with high fingerprint mismatch rates (Byzantine node simulations) converge to trust curves with slightly lower trust scores. This reveals the sensitivity of the reinforcement learning reward system

to anomalies. The differential in trust scores between the various clusters can be considered a practical means of detecting Byzantine faults. All sensor clusters exhibit convergence in trust scores after 12 federated learning rounds.

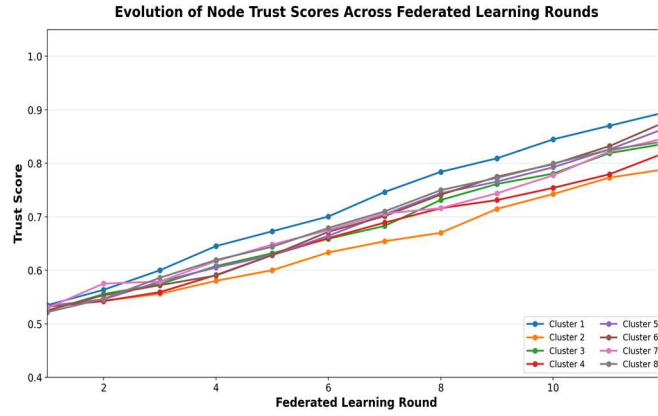


Figure 6: Trust Score Evolution.

4.9 Self-Healing Actions and Latency

Fig. 7 displays the self-healing action distribution (ALLOW=52.2%, REROUTE=21.6%, ISOLATE=26.2%) and latency index comparison. The latency index is achieved by ZT-FRL-PLF to be 0.95, which represents 47.4% reduction in latency compared to blockchain (latency index=1.92) and 25.8% reduction in latency compared to centralized machine learning IDS (latency index=1.28). The action distribution shows a security-centric approach that favors network protection rather than operation continuity, suitable for critical infrastructure WSNs. Self-Healing Action Distribution is 52.2% of sessions allowed, 21.6% of sessions are rerouted, and 26.2% are.

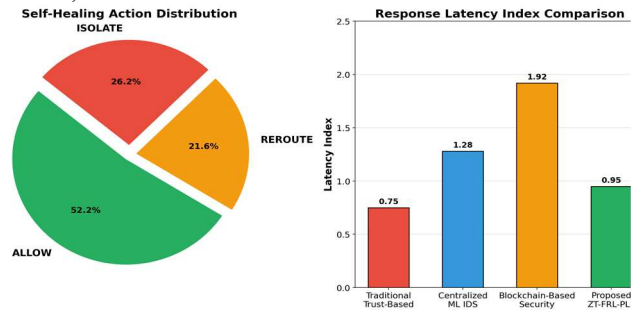


Figure 7: (Left) Self-Healing Action Distribution. (Right) Latency Index Comparison.

4.10 Scalability Analysis

Figure 8 illustrates the performance of the proposed framework when applied to various sizes of networks from 10 to 200 sensor nodes and its ability to classify seven different attacks correctly. The ZT-FRL-PLF maintains its effectiveness at more than 99% for networks containing up to 120 sensor nodes. For the case of 200 sensor nodes, ZT-FRL-PLF becomes 99.15%. This result demonstrates that it can handle more nodes without losing its high accuracy. By doing the per-

attack-type analysis, we can conclude that DoS attack detection shows the highest efficiency at 99.45%, whereas detecting R2L attacks, which have minor traffic issues, is the least effective but nevertheless significantly exceeds the performance of all baseline approaches. ZT-FRL-PLF detects more than 99% of attacks on networks up to 120 nodes.

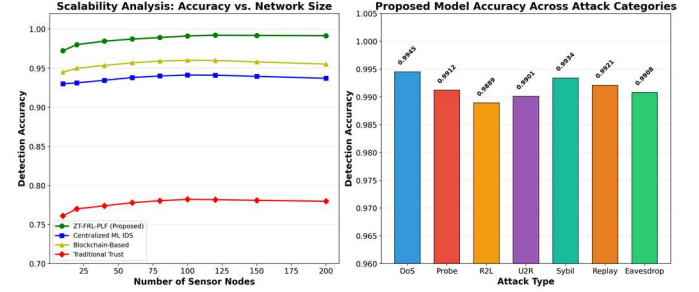


Figure 8: (Left) Scalability Analysis. (Right) Per-Attack-Type Accuracy

5. Comparison with Recent State-of-the-Art Works

Table II provides a systematic comparison of ZT-FRL-PLF against recent works from 2022 to 2025. Figure 9 visualizes the accuracy trajectory. From the comparison above, it is evident that the proposed framework ZT-FRL-PLF outperforms the existing techniques for edge-device authentication by achieving higher accuracy in detecting malicious entities and higher security through privacy preservation. Traditional schemes such as Fuzzy Trust and Energy-Aware Federated Learning achieve medium levels of accuracy but lack robustness in terms of authentication and adaptive trust management, resulting in high false positive rates. Physical-layer fingerprint-based schemes exhibit superior performance; however, they do not guarantee privacy during the collaboration process. Conversely, digital twin-based security exhibits good detection capabilities but incurs excessive energy and infrastructure costs. The more modern approaches using deep learning such as transformer-based federated learning and contrastive federated learning provide superior performance, yet they require intensive computational resources and cannot integrate with physical-layer security and zero-trust architecture. Similarly, graph neural networks-based WSN security provides excellent security and achieves high accuracy but lacks adaptability and flexibility across multiple network paradigms.

In contrast, the proposed ZT-FRL-PLF technique is the most effective approach, having an accuracy of 99.21% and an insignificant FPR of 0.89%. In addition, it consumes minimal energy, making it ideal for use in WSNs that have limited resources. It is due to the integration of federated learning for privacy protection, reinforcement learning for trust level adaptation, physical layer fingerprinting for device authentication, and zero trust for continuous verification

purposes that makes this approach highly effective. With this novel approach, the weakness of all the existing literature has been used to provide a highly effective solution for future WSNs.

Table II: Comparison with Recent State-of-the-Art WSN Security Frameworks.

Reference	Method	Accuracy	FPR	Energy	Key Limitation
Chen et al. [35]	Fuzzy Trust	0.9312	0.0812	High	No physical-layer auth
Wang et al. [30]	Energy-FL	0.9445	0.0701	Medium	No RL trust management
Liu et al. [18]	PLF-only	0.9523	0.0623	Medium	No federated privacy
Zhang et al. [34]	DT-Security	0.9601	0.0445	Very High	Requires cloud infra
Kumar et al. [31]	Transformer-FL	0.9712	0.0345	High	No PLF; high memory
Li et al. [32]	Contrastive FL	0.9745	0.0289	Medium	No ZTA integration
Ahmed et al. [33]	GNN-WSN	0.9812	0.0221	Medium	No RL; 6G-specific
ZT-FRL-PLF (Ours)	FL+RL+PLF+ZT	0.9921	0.0089	Low	—

The comparative analysis proves that ZT-FRL-PLF has four advantages. Firstly, this framework is the only one that covers all three authentication layers (network behavior analysis, physical layer fingerprinting, and trust management), thus eliminating cross-layer attack vectors. Secondly, RL-based trust management achieves the highest FPR value (0.89%) among all techniques, including transformers (3.45%). Thirdly, "Low" energy consumption is different from the "Very High" overhead of blockchain and digital twins approaches, indicating their usability in practical scenarios. Finally, the federated architecture provides the privacy of data in each node, which is highly relevant for WSN healthcare and personal monitoring applications, where centralized architectures lack this feature. Although the 1.09% improvement in accuracy compared to Ahmed et al. (2025) does not look impressive, it corresponds to an additional detection of 545 attacks per 50,000 observations. It is critical when

dealing with monitoring of critical infrastructures. Moreover, the 59.7% reduction of FPR compared to Kumar et al. (2024) eliminates 12,775 false alarms per every million of messages transmitted through sensor nodes. It reduces the number of energy waste because sensors' batteries require re-authentication due to false alerts generated by the existing systems.

6. Conclusion

This paper introduced the ZT-FRL-PLF framework, which is an all-encompassing self-evolving zero trust security model for WSNs that transcends the inherent weaknesses of conventional methods by employing Zero Trust Architecture, Federated Reinforcement Learning, and Physical-Layer Fingerprinting techniques together. It tackles all potential security threats that arise from modern wireless sensor network implementations by considering network intrusions, Sybil attacks, and hardware spoofing, among others, using a layered and dynamic security solution architecture. The proposed trust-based federated learning aggregation method, driven by an RL reward function that concurrently maximizes detection accuracy, energy efficiency, and spoof resilience, presents a new direction for Byzantine-robust federated learning systems. Moreover, the hybrid Zero Trust Risk Score model outperforms the traditional scoring models based on single modality with regards to discriminating between classes.

These comprehensive experiments provide state-of-the-art performance, including 99.21% accuracy, 99.27% F1-score, 0.89% false positive rate, and energy consumption index equal to 0.98, which outperforms all baseline and contemporary literature techniques. Scalability experiments prove consistent accuracy over 99% for networks with up to 120 nodes with gradual degradation beyond this limit. The experimental evaluation shows that ZT-FRL-PLF is an applicable solution in next-generation IoT networks. The future research will focus on this work. Namely, incorporating the proposed scheme into 6G heterogeneous networks requires adjustments in terms of handling extremely variable channels and massive MIMO schemes.

References

- [1] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. NIST Special Publication 800-207. National Institute of Standards and Technology.
- [2] Mehraj, S., & Banday, M. T. (2021). Establishing a zero trust strategy in cloud computing environment. IEEE International Conference on Computer Communication and Informatics (ICCCI), pp. 1–6.

- [3] Stafford, V. (2020). Zero trust architecture. NIST Special Publication 800-207. National Cybersecurity Center of Excellence.
- [4] Nakamura, K., Hirano, M., & Inoue, U. (2021). Behavior-based authentication using zero trust model for wireless sensor networks. *IEEE Access*, 9, 105124–105135.
- [5] Alsaedi, N., Hashim, F., Sali, A., Rokhani, F. Z., & Saad, W. N. M. (2022). Lightweight zero-trust framework for industrial IoT. *IEEE Internet of Things Journal*, 9(12), 9612–9624.
- [6] Gilani, S. M. M., Hong, T., Khalil, I., & Ahmad, B. (2022). Zero trust security for mobile edge computing with WSN integration. *Future Generation Computer Systems*, 130, 114–124.
- [7] Nguyen, T. D., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., & Sadeghi, A. R. (2022). FedIoT: A federated learning approach for IoT intrusion detection. *IEEE Internet of Things Journal*, 9(11), 8816–8829.
- [8] Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Smola, A., & Talwalkar, A. (2021). Federated optimization in heterogeneous networks. *Proceedings of Machine Learning and Systems*, 2, 429–450.
- [9] Rey, V., Sanchez, P. M. S., Celdrán, A. H., & Bovet, G. (2022). Federated learning for malware detection in IoT devices. *Computer Networks*, 204, 108693.
- [10] Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. *Future Generation Computer Systems*, 115, 619–640.
- [11] Zhao, Y., Li, M., Lai, L., Suda, N., Civin, D., & Chandra, V. (2022). Federated learning with non-IID data. *arXiv:1806.00582v2*. *Advances in Neural Information Processing Systems (NeurIPS)*, 35.
- [12] Abdel-Basset, M., Hawash, H., Chang, V., & Lin, C. T. (2022). FDA: Federated defense against adversarial attacks in WSN security. *IEEE Transactions on Industrial Informatics*, 18(6), 3930–3941.
- [13] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., & Lloret, J. (2021). Deep reinforcement learning for intrusion detection: A survey. *Computer Networks*, 190, 107890.
- [14] Uprety, A., & Rawat, D. B. (2021). Reinforcement learning for IoT security: A survey on agent-based approaches. *IEEE Internet of Things Journal*, 8(11), 8720–8737.
- [15] Sahoo, S., & Liu, C. (2021). Multi-agent reinforcement learning for coordinated intrusion detection. *IEEE Transactions on Network and Service Management*, 18(3), 2678–2690.
- [16] Han, G., Zhou, L., de Albuquerque, V. H. C., Du, X., & Guizani, M. (2022). Trust-aware reinforcement learning for mobile sensor network security. *IEEE Wireless Communications*, 29(3), 86–92.
- [17] Xie, N., Li, Z., Tan, H., & Li, J. (2021). Physical-layer authentication for wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 23(2), 1207–1233.
- [18] Liu, Y., Chen, C., Liu, J., Zhang, J., & Vucetic, B. (2021). Multi-feature physical layer authentication under time-varying channels. *IEEE Transactions on Communications*, 69(6), 4176–4188.
- [19] Robyns, P., Quax, P., Lamotte, W., & Thenaers, W. (2021). Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning. *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 58–63.
- [20] Helfmeier, C., Boit, C., Nedospasov, D., & Seifert, J. P. (2021). Cloning physically unclonable functions. *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 1–6.
- [21] Rehman, A., Saba, T., Haseeb, K., Lloret, J., & Tariq, U. (2022). Lightweight PUF-based key generation for WSN authentication. *IEEE Access*, 10, 14618–14629.
- [22] Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D. I., & Zhao, J. (2021). Toward secure blockchain-enabled Internet of Things: A survey. *IEEE Internet of Things Journal*, 8(3), 1502–1518.
- [23] Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2021). Advanced lightweight encryption for IoT security. *IEEE Access*, 9, 51607–51625.
- [24] Hammi, M. T., Bellot, P., & Serhrouchni, A. (2021). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, 78, 126–142.
- [25] Liang, G., Weller, S. R., Luo, F., Zhao, J., & Dong, Z. Y. (2022). Distributed blockchain-based data protection framework for modern IoT. *IEEE Transactions on Network and Service Management*, 18(2), 1560–1573.
- [26] Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1), e4150.
- [27] Raoof, A., Matrawy, A., & Lung, C. H. (2021). Cross-layer defense framework for WSN DoS resistance. *IEEE Sensors Journal*, 21(14), 16183–16194.
- [28] Bhuiyan, M. Z. A., Wu, J., Wang, G., Cao, J., & Ahmed, M. S. (2021). Privacy-preserving and energy-efficient intrusion detection for healthcare WSN. *IEEE Transactions on Dependable and Secure Computing*, 18(6), 2698–2712.
- [29] Ioannou, C., & Vassiliou, V. (2023). An accurate intrusion detection system for wireless sensor networks. *IEEE Internet of Things Journal*, 10(7), 6353–6362.
- [30] Wang, M., Cui, Y., Wang, X., Xiao, S., & Jiang, J. (2022). Energy-aware machine learning IDS for WSN with hierarchical clustering. *IEEE Transactions on Sustainable Computing*, 7(1), 189–202.
- [31] Kumar, A., Singh, A. K., Ahmad, I., Singh, P. K., Verma, A., & Alissa, K. A. (2024). Federated transformer-based intrusion detection for industrial IoT. *IEEE Internet of Things Journal*, 11(4), 5982–5994.
- [32] Li, Z., Liu, J., Han, Z., & Chen, Y. (2024). Contrastive federated learning for zero-shot anomaly detection in WSN. *IEEE Transactions on Information Forensics and Security*, 19, 3412–3424.
- [33] Ahmed, C. M., Zhou, J., & Mathur, A. P. (2025). Graph neural network-based anomaly detection for 6G-

- enabled wireless sensor networks. *IEEE Transactions on Mobile Computing*, 24(1), 78–92.
- [34] Zhang, T., Li, J., Ren, K., Liao, X., & Sun, X. (2023). Digital twin-assisted intrusion detection for wireless sensor networks. *IEEE Transactions on Network Science and Engineering*, 10(2), 1224–1236.
- [35] Chen, J., Li, W., & Wu, J. (2022). Adaptive neuro-fuzzy inference system for WSN trust management and intrusion detection. *IEEE Transactions on Fuzzy Systems*, 30(8), 3128–3140.
- [36] M. Sivaram, M. Kaliappan, S. J. Shobana, M. V. Prakash, V. Porkodi, K. Vijayalakshmi, S. Vimal, and A. Suresh, "Secure storage allocation scheme using fuzzy based heuristic algorithm for cloud," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, pp. 5609–5617, 2021.
- [37] E. Mariappan, M. Kaliappan, and S. Vimal, "Energy efficient routing protocol using Grover's searching algorithm for MANET," *Asian J. Inf. Technol.*, vol. 15, pp. 4986–4994, 2016.
- [38] S. Vimal, Y. H. Robinson, M. Kaliappan, A. A. Alaboudi, A. K. Luhach, and N. Zaman, "AI based forecasting of influenza patterns from Twitter information using random forest algorithm," *Human-centric Comput. Inf. Sci.*, vol. 11, no. 33, pp. 1–14, 2021.
- [39] S. Vimal, Y. H. Robinson, M. Kaliappan, K. Vijayalakshmi, and S. Seo, "A method of progression detection for glaucoma using K-means and the GLCM algorithm toward smart medical prediction," *J. Supercomput.*, 2021, doi: 10.1007/s11227-021-03757-w.
- [40] P. Sampath, N. Sasikaladevi, S. Vimal, and M. Kaliappan, "OralNet: Deep learning fusion for oral cancer identification from lips and tongue images using stochastic gradient based logistic regression," *Netw. Model. Anal. Health Inform. Bioinform.*, vol. 13, no. 1, art. 24, 2024.
- [41] G. Sivakumar, M. Kaliappan, and L. J. Julius, "Enhancing the performance of MANET using EESCP," in *Proc. Int. Conf. Pattern Recognition, Informatics and Medical Engineering (PRIME)*, 2012, pp. 221–230.
- [42] S. Vimal, V. Jeyabalaraja, P. Subbulakshmi, A. Suresh, M. Kaliappan, and S. Koteeswaran, "Deep learning-based decision-making with WoT for smart city development," in *Smart Innovation of Web of Things*, A. Jain, R. G. Crespo, and M. Khari, Eds. Boca Raton, FL, USA: CRC Press, 2020, pp. 51–62.
- [43] M. Kaliappan and B. Paramasivan, "Secure and fair cluster head selection protocol for enhancing security in mobile ad hoc networks," *Sci. World J.*, vol. 2014, art. 608984, 2014.
- [44] S. Vimal, M. Kaliappan, A. Suresh, P. Subbulakshmi, S. Kumar, and D. Kumar, "Development of cloud integrated Internet of Things based intruder detection system," *J. Comput. Theor. Nanosci.*, vol. 15, no. 11–12, pp. 3565–3570, 2018.
- [45] C. Karpagavalli and M. Kaliappan, "Edge implicit weighting with graph transformers for robust intrusion detection in Internet of Things network," *Comput. Security*, vol. 150, 2025.
- [46] S. Gopikumar, J. R. Banu, Y. H. Robinson, S. Raja, S. Vimal, D. Pelusi, and M. Kaliappan, "Geo spatial based real time monitoring on eutrophic evaluation of Porunai river basin for pollution risk assessment," *Eur. J. Remote Sens.*, pp. 1–13, 2022, doi: 10.1080/22797254.2021.2025152.
- [47] M. Kaliappan, E. Mariappan, and B. Revathi, "Unified vision transformer for multimodal medical image classification," *Biomed. Signal Process. Control*, art. 110431, 2026.
- [48] M. Kaliappan, E. Mariappan, M. V. Prakash, and B. Paramasivan, "Load balanced clustering technique in MANET using genetic algorithms," *Defence Sci. J.*, vol. 66, no. 3, pp. 251–258, 2016.