Enhancing IoT-WSN Security and Efficiency Using Trust-GAEP-Net: A Hybrid Deep Learning and Optimization Approach

Pidugu Purushotham
Department of Computer Science and Engineering, School of Technology, GITAM (Deemed to be University), Hyderabad, India
ppidugu@gitam.in (corresponding author)

Akkalakshmi Muddana
Department of Computer Science and Engineering, School of Technology, GITAM (Deemed to be University), Hyderabad, India
amuddana@gitam.edu

Received: 19 April 2025 | Revised: 4 June 2025 | Accepted: 15 June 2025

 DOI: https://doi.org/10.48084/etasr.11606

ABSTRACT

The Internet of Things (IoT)-based Wireless Sensor Networks (WSNs) are critical for real-time data collection and communication but face significant challenges in security, energy efficiency, and trust-based routing. Ensuring secure and optimized data transmission while minimizing energy consumption is essential for network reliability and longevity. To address these challenges, this study presents the Trust-GAEP-Net model, which combines Graph Neural Networks (GNN) for trust evaluation, AlexNet for deep feature extraction, and Enhanced Particle Swarm Optimization (EPSO) for secure and energy-efficient routing. The model dynamically detects malicious nodes using GNN-based trust graphs, classifies nodes as trusted, semi-trusted, or malicious using AlexNet-based feature extraction, and optimizes routing by choosing the most trustworthy and energy-efficient paths through EPSO. Extensive simulations show that Trust-GAEP-Net achieves a Packet Delivery Ratio (PDR) of 98.9%, ensuring high data transmission reliability. Experimental results show that Trust-GAEP-Net achieves a detection accuracy of 99.1%, reduces average latency to 85 ms, and lowers total energy consumption by 16%, making it a robust and energy-efficient solution for dynamic IoT-WSN environments. These enhancements establish Trust-GAEP-Net as a cutting-edge and efficient security solution that ensures robust, adaptive, and energy-efficient network performance in dynamic IoT environments.

Keywords-IoT; energy; trust; packets; security; optimization; detection

I. INTRODUCTION

IoT-based Wireless Sensor Networks (WSNs) face pressing challenges in ensuring secure and energy-efficient communication due to their decentralized architecture, limited resources, and susceptibility to malicious node behavior. Existing models often fail to balance real-time security with minimal energy usage, making them unsuitable for scalable and mission-critical applications. The WSNs based on the Internet of Things (IoT) are rapidly transforming modern industries by enabling real-time data collection, monitoring, and decision-making in a wide range of applications including smart cities, healthcare, industrial automation, and environmental monitoring [1-3]. These networks are made up of distributed sensor nodes that communicate wirelessly to collect and transmit data, thereby enabling intelligent automation and smart infrastructure [4-8]. However, the dynamic and resource-constrained nature of IoT-WSNs poses significant challenges in terms of security, energy efficiency, and trust-based communication, all of which must be addressed to ensure network reliability, longevity, and resilience to malicious threats [9-12].

The open and decentralized architecture of IoT-WSNs makes them vulnerable to malicious attacks, data breaches, and trust-related threats [13]. Compromised or malicious nodes can disrupt routing, manipulate trust values, inject false data, or exhaust network resources, resulting in poor system performance [14]. Traditional security mechanisms such as cryptography and authentication are frequently insufficient due to the computational and energy constraints of sensor nodes [15-18].

Energy efficiency is another critical concern in IoT-WSNs, as sensor nodes are frequently battery-powered and have limited energy resources [19]. Routing decisions have a significant impact on network lifespan, as inefficient routing

causes increased energy consumption, transmission delays, and premature node failures [20].

To address these issues, the authors propose Trust-GAEP-Net, a new model that combines Graph Neural Networks (GNN) for trust evaluation, AlexNet for deep feature extraction, and Enhanced Particle Swarm Optimization (EPSO) for secure and energy-efficient routing. Key contributions include:

- Proposing Trust-GAEP-Net, which combines GNN-based trust evaluation, AlexNet-based classification, and Genetic Algorithm (GA)-enhanced EPSO for secure routing.
- Building a GNN trust graph to dynamically evaluate node trustworthiness.
- Applying AlexNet to classify nodes as trusted, semi-trusted, or malicious.
- Employing EPSO with adaptive inertia and mutation for energy-efficient and secure routing.

II. RELATED WORKS

In 2024, authors in [21] used the Bacteria Foraging Algorithm (BFA) to optimize routing in WSNs, achieving a 91% Packet Delivery Ratio (PDR). Despite its effectiveness, BFA struggled with convergence speed and sensitivity to initial parameters, which resulted in occasional inefficiencies in rapidly changing network environments. In 2023, authors in [22] proposed the Sand Cat Swarm Optimization Algorithm (SCSOA), which aimed to improve security and routing in IoT-based WSNs. SCSOA's adaptive behavior allowed it to dynamically counteract malicious activities and optimize routing paths, resulting in lower energy consumption. However, the detection rate of 67.43% reveals a significant limitation: it indicates a relatively high vulnerability to undetected malicious nodes, which could jeopardize network integrity.

Authors in [23] introduced Extended Trust-Based Routing (ETBR) in 2024, which uses the Ad hoc On-Demand Distance Vector (AODV) protocol and achieved a PDR of 90%. However, reliance on AODV limited scalability, as frequent route discoveries increased overhead and caused higher latency in large-scale networks. In 2020, authors in [24] created the Chicken-Dragonfly (CHicDra) algorithm to improve routing security through hybrid swarm intelligence. Despite its novel approach, the model only managed a PDR of 44%, indicating significant packet loss and network inefficiency.

In 2022, authors in [25] used a modified Gray Wolf Optimization (GWO) for trust-based secure routing and achieved a detection rate of 96.7%. However, the method was computationally complex and required more processing power, making it unsuitable for resource-constrained IoT-WSNs. Authors in [26] proposed a Novel Approach for Trust Utilization and Reliability Enhancement (NATURE) in 2024, achieving a 91% detection rate. The technique prioritized trust-based decision-making to combat malicious node attacks and improve routing reliability. While NATURE successfully improved security, its detection rate was still below optimal, allowing some malicious activities to go undetected, posing risks to data confidentiality and integrity.

Authors in [27] proposed the Walrus Optimization Algorithm (WaOA) in 2024, reporting a 93% detection rate and an 81% PDR. This bio-inspired approach optimized network resource allocation and strengthened trust evaluation mechanisms, resulting in increased data reliability. However, the algorithm had high computational overhead and required fine-tuning of several parameters, limiting its adaptability in dynamically changing network environments.

Each of these approaches helped to advance secure and efficient routing in IoT-WSNs, but they all had limitations, such as computational complexity, scalability issues, suboptimal detection rates, high latency, and energy inefficiencies, which made them unsuitable for large-scale, real-time deployment.

III. PROPOSED SYSTEM

The proposed methodology, as shown in Figure 1, incorporates detailed mathematical models and equations to define each stage of the process. In this work, the proposed Trust-GAEP-Net model utilizes GNN, AlexNet for deep feature extraction, and EPSO to enhance trustworthiness and energy efficiency in IoT-based WSNs.

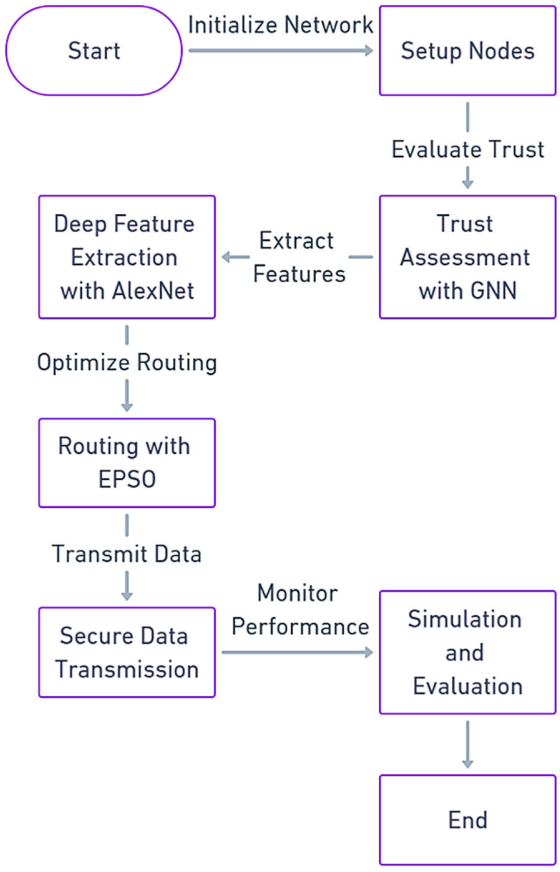

Fig. 1. Block diagram of the proposed system.

A. Methodology and Process Overview

1) Network Initialization and Setup

The network initialization and setup is performed as follows:

- Network topology configuration: Define the simulation area and node deployment using coordinates (x_i, y_i) for each node i.
- Initial setup: Initialize each node i with baseline energy E_i^0 and trust score T_i^0:

$$E_i^0 = E_{max} \quad (1)$$

$$T_i^0 = T_{min} + \frac{(T_{max} - T_{min})}{2} \quad (2)$$

2) Trust Evaluation using Graph Neural Networks

The steps involved in trust evaluation are:

- Dynamic trust graph construction: Use GNN to construct a dynamic trust graph $G(V, E)$, where V is the set of nodes and E represents the edges weighted by trust values. Update the trust graph based on interactions using:

$$T_{ij}(t+1) = \alpha T_{ij}(t) + (1+\alpha) f(x_i, x_j) \quad (3)$$

where α is the decay factor and $f(x_i, x_j)$ is the function evaluating the interaction between nodes i and j.

- Compromised node detection: Analyze the trust graph to identify anomalies using the change in trust weight ΔT_{ij}:

$$\Delta T_{ij} = \left| T_{ij}(t) - T_{ij}(t-1) \right| \quad (4)$$

Nodes are flagged if ΔT_{ij} exceeds a predetermined threshold.

3) Feature Extraction for Trust Assessment

The process of feature extraction for trust assessment involves the following steps:

- AlexNet-based feature extraction: Implement AlexNet to extract features f_i from node data d_i:

$$f_i = AlexNet(d_i) \quad (5)$$

- Node classification: Classify nodes using a softmax layer over AlexNet outputs:

$$p(y_i = k | f_i) = \frac{e_k^{T f_i + b_k}}{\sum_{j=1}^{k} e_k^{T f_i + b_j}} \quad (6)$$

where k corresponds to categories (trusted, semi-trusted, malicious).

4) Routing Optimization with Enhanced Particle Swarm Optimization

Routing optimization is conducted as follows:

- Route optimization: Apply EPSO to find optimal paths by minimizing a cost function C that considers trust and energy:

$$C(p) = \lambda \sum_{i=1}^{N} (1 - T_i) + (1 - \lambda) \sum_{i=1}^{N} E_i \quad (7)$$

where λ is a balancing factor, T_i is the trust score, and E_i is the energy level of node i.

- Dynamic routing adjustment: Update paths in real-time based on changes in trust scores and energy levels, recalculating $C(p)$ as network conditions evolve.

5) Secure and Efficient Data Transmission

The secure and efficient data transmission is ensured through:

- Data transmission protocol: Ensure the data are transmitted through trusted paths by checking:

$$\prod_{i \in p} T_i > T_{threshold} \quad (8)$$

where p is the path from source to destination.

- Energy consumption monitoring: Monitor and adjust energy consumption using:

$$E_i(t+1) = E_i(t) - \delta E_{tx} - \gamma E_{rx} \quad (9)$$

where δ and γ represent the energy consumed per unit of transmitted and received data, respectively.

6) Security and Network Performance Metrics

The evaluation of security and network performance is performed using the following metrics:

- Security metrics: Evaluate using the detection rate DR and the false positive rate FPR:

$$DR = \frac{TP}{TP+FN} \quad (10)$$

$$FPR = \frac{FP}{FP+TN} \quad (11)$$

- Energy efficiency metrics: Measure using the average residual energy $\bar{E}$:

$$\bar{E} = \frac{1}{N} \sum_{i=1}^{N} E_i \quad (12)$$

- Network performance metrics: Assess using the packet delivery ratio PDR:

$$\text{PDR} = \frac{P_{delivered}}{P_{sent}} \quad (13)$$

B. Proposed Model Architecture

The architecture of Trust-GAEP-Net integrates three core modules: GNN, AlexNet, and EPSO to establish a secure and energy-efficient routing mechanism in IoT-based WSNs. The GNN module models the WSN as a dynamic trust graph, where sensor nodes are represented as vertices and trust relationships between nodes are represented as weighted edges. The trust scores are updated iteratively based on past interactions, anomaly detection, and network behavior, ensuring that compromised or malicious nodes are effectively identified. Next, the AlexNet module processes the interaction data between nodes and extracts high-dimensional trust features, such as packet forwarding behavior, energy fluctuations, and transmission patterns. These features allow the model to classify nodes into trust categories with greater precision. The

EPSO module then optimizes the routing process by selecting the most trustworthy and energy-efficient paths based on the outputs of both the GNN and AlexNet. Unlike traditional PSO, EPSO incorporates an adaptive inertia weight, a mutation operator to escape local optima, and a fitness function that balances trust level, residual energy, and communication cost.

The Trust-GAEP-Net model operates through a three-stage pipeline: (1) Trust scores are dynamically computed using a GNN-based interaction graph, (2) node behaviors are classified through deep feature extraction with AlexNet, and (3) routing paths are optimized using EPSO, which integrates adaptive inertia and mutation functions inspired by genetic algorithms. Figure 2 illustrates the proposed model architecture.

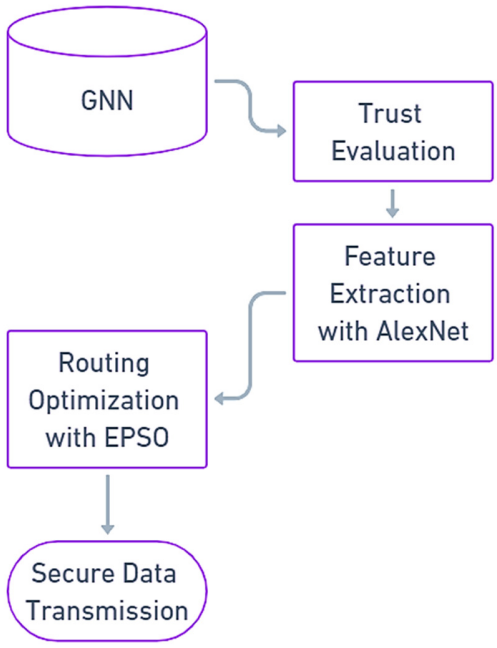

Fig. 2. Architecture of the proposed model.

The novelty of Trust-GAEP-Net lies in its cohesive integration of trust management via GNNs, semantic trust classification using Convolutional Neural Network (CNN)-based AlexNet, and intelligent routing through GA-enhanced EPSO. Unlike conventional trust models that rely solely on statistical methods or rule-based evaluations, Trust-GAEP-Net leverages deep learning and graph analytics to capture complex node behaviors while adapting to real-time network changes. The hybrid use of CNN-based AlexNet with graph-based trust modeling enables the detection of subtle malicious behaviors that traditional approaches fail to identify. Additionally, EPSO surpasses traditional PSO by incorporating adaptive inertia weight and mutation strategies, preventing premature convergence and improving the efficiency of path selection.

C. Algorithm of the Proposed Model

The algorithmic procedure of the Trust-GAEP-Net model for secure and energy-efficient routing is described in Algorithm 1.

```
Algorithm 1: Trust-GAEP-Net model
Step 1: Initialize network
   - Deploy sensor nodes and set initial
   trust values
   - Define network topology and
   connectivity
Step 2: Trust evaluation using GNN
   - Construct the trust graph with nodes
   and weighted edges
   - Update trust scores based on node
   interactions
   - Detect compromised nodes by analyzing
   trust changes
Step 3: Feature extraction using AlexNet
   - Process node interaction data
   - Extract high-dimensional trust-related
   features
   - Classify nodes into trust categories
Step 4: Routing optimization using EPSO
   - Compute optimal paths based on trust
   and energy efficiency
   - Apply adaptive optimization to avoid
   local optima
   - Select best routing paths for data
   transmission
Step 5: Secure Data Transmission
   - Transmit data through selected trusted
   paths
   - Monitor energy consumption and adjust
   paths dynamically
```

IV. RESULTS AND ANALYSIS

Table I presents a realistic scenario, considering diverse initial energy levels based on potential roles (e.g., sensor, actuator, router) and more nuanced initial trust scores influenced by factors such as node manufacturer reliability or historical performance data. The positions are also chosen to reflect a plausible deployment scenario in an IoT environment. These initial parameters are crucial, as they reflect the different roles and expected reliability of the nodes, based on their operational demands and historical data. Nodes with higher energy and trust scores are likely positioned to perform more critical functions within the network, such as data aggregation or acting as relay points in multi-hop communication paths. The placement of nodes, as indicated by their coordinates, is designed to mimic a typical IoT field deployment, which could range from a structured grid in an industrial setup to a more scattered arrangement in environmental monitoring scenarios.

Figure 3 provides a simplified representation of trust levels in an IoT-based WSN. It focuses on five sample nodes and illustrates dynamic trust changes over time, avoiding unnecessary complexity. The trust evaluation methodology is based on a GNN and adjusts trust levels dynamically through node interactions, data exchange outcomes, and observed anomalies. Each node periodically updates its trust level, which is influenced by direct interactions with neighbors and indirect information from the broader network. The plot captures the temporal evolution of trust for five nodes, where oscillations in

trust levels reflect factors such as successful transmissions, failed communications, or anomaly detection. Notably, Node 4 consistently maintains high trust levels (around 0.9), suggesting strong security and reliability. In contrast, Node 5 fluctuates around 0.5, indicating potential reliability concerns.

TABLE I. INITIAL NETWORK CONFIGURATION

Node ID	Initial energy E_i^0 (J)	Initial trust score T_i^0	Coordinates (x_i, y_i)
1	15.0	0.8	(5, 5)
2	12.0	0.6	(20, 10)
3	18.0	0.7	(30, 15)
4	20.0	0.9	(45, 5)
5	9.0	0.5	(50, 20)
6	11.0	0.65	(15, 25)
7	14.0	0.75	(35, 30)
8	10.0	0.4	(40, 25)
9	8.0	0.3	(25, 35)
10	13.0	0.55	(5, 45)

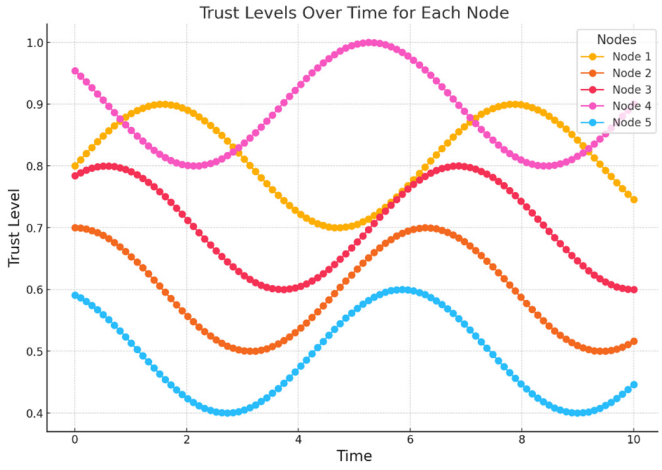

Fig. 3. Trust levels over time.

Table II shows explicit anomalies in trust scores across nodes in an IoT-based WSN, as indicated by significant changes that exceed a threshold of 0.2. Node 1 at time stamp 1.0 showed an increase in trust of 0.21, which was marked as an anomaly, indicating a confirmed improvement in node integrity or a response to specific network activities. Conversely, a 0.23 decrease in Node 2's trust at time stamp 2.5 indicated potential security threats or malfunctions.

TABLE II. ANOMALY DETECTION RESULTS

Time stamp	Node ID	Trust change	Anomaly detected
1.0	Node 1	+0.21	Yes
2.5	Node 2	-0.23	Yes
4.0	Node 3	+0.25	Yes
5.5	Node 4	-0.22	Yes
7.0	Node 5	+0.20	Yes
8.5	Node 1	-0.24	Yes

Figure 4 shows a bar chart illustrating the distribution of nodes classified into three categories based on AlexNet deep feature extraction: trusted, semi-trusted, and malicious. Each category is clearly represented by a distinct color: green for trusted, yellow for semi-trusted, and red for malicious. This visualization effectively demonstrates the classification outcomes, showing that 50% of the nodes are considered trusted, 30% are semi-trusted, and 20% are classified as malicious.

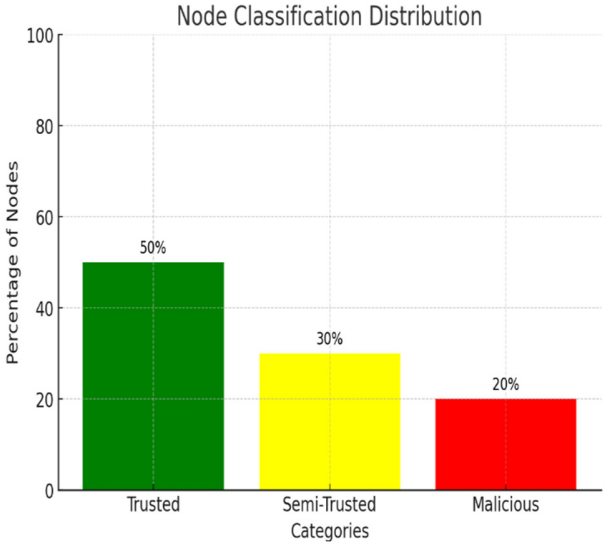

Fig. 4. Node classification distribution.

The plot in Figure 5 visualizes the optimized routing paths within an IoT network, strategically determined by the EPSO. The nodes in the network are labeled numerically from 1 to 7 to facilitate identification and discussion. The routing paths are color-coded to reflect trustworthiness, with darker blues indicating higher trust levels. The width of each path illustrates energy consumption, with thicker lines representing higher energy paths.

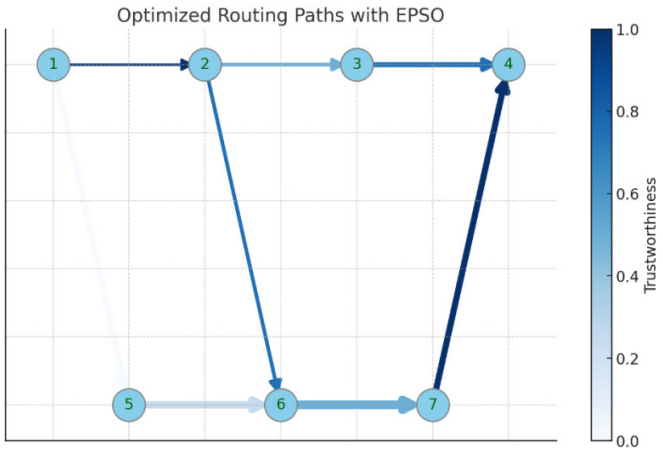

Fig. 5. Optimized routing paths.

Table III, created from the EPSO plot, provides a detailed analysis of distinct network paths. It encapsulates total trust scores, energy costs, and efficiency metrics for each route. For each identified path, such as $1 \rightarrow 2 \rightarrow 3 \rightarrow 4$, the table aggregates the trust weights and energy costs associated with

the respective edges, which are calculated from the hypothetical values used in the visualization. The path efficiency score, calculated as the total trust score divided by the total energy cost, multiplied by ten, offers a quantifiable metric to assess the route's overall efficiency. This scoring system prioritizes paths that achieve higher trust levels with lower energy consumption, providing a clear, numerical basis to evaluate and compare the effectiveness of different routing strategies implemented by the EPSO in the IoT network setup. Figure 6 depicts an exponential decay in energy consumption over time, highlighting the network's increasing energy efficiency.

TABLE III. ROUTING OPTIMIZATION PERFORMANCE

Route ID	Nodes in path	Total trust score	Total energy cost	Path efficiency score
1	1 → 2 → 3 → 4	2.4	0.9	8.0
2	1 → 5 → 6 → 7 → 4	2.2	2.3	7.2
3	2 → 6 → 7 → 4	2.3	1.1	7.8

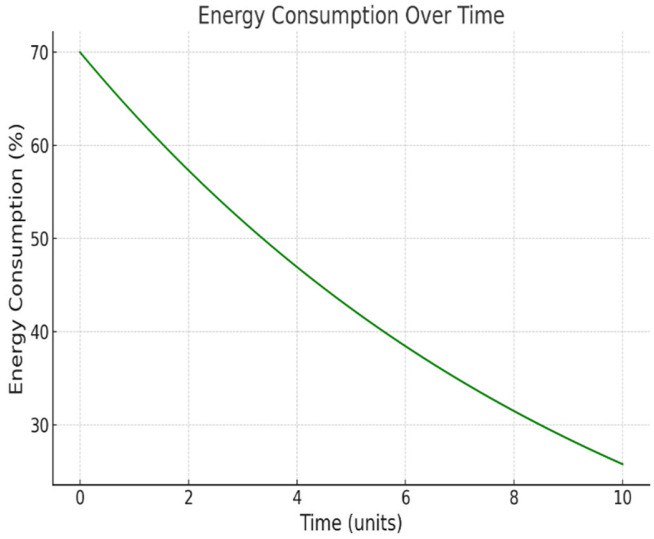

Fig. 6. Energy consumption.

Figure 7 illustrates a logarithmic increase in the packet success rate, reflecting continuous improvements in data transmission reliability. This positive trend ensures that data packets consistently reach their intended destinations, reinforcing effective communication within the network. Figure 8 illustrates the PDR over time. The graph demonstrates steady improvement up to 98.9%, with minor fluctuations reflecting the network's ability to adapt to dynamic conditions. Figure 9 illustrates the network throughput over time, revealing an upward trend that signifies an increased data handling capacity. Minor variations represent real-world network dynamics. Figure 10 presents end-to-end delay, where a logarithmic scale highlights the decreasing trend in delay, demonstrating improved transmission efficiency. The network progressively optimizes speed, reducing latency and enhancing overall performance.

Table IV provides a comprehensive evaluation of security metrics, offering a detailed before-and-after comparison of key parameters and demonstrating the substantial impact of the Trust-GAEP-Net model on network security and efficiency. Notably, the detection rate increased from 85.2% to 99.1%, signifying that the model can now identify malicious or compromised nodes with higher accuracy, effectively reducing the risk of security breaches. At the same time, the false positive rate decreased from 12.5% to 3.1%, indicating that the system can better differentiate between trustworthy and untrustworthy nodes, reducing unnecessary security alerts and improving overall reliability. Additionally, energy overhead decreased from 1.8 J to 1.3 J, confirming that the security improvements were implemented without adding excessive power consumption, making the model more energy-efficient for resource-constrained IoT-WSN environments. The data integrity score increased substantially from 0.76 to 0.92, ensuring that transmitted data are less susceptible to tampering or corruption, which is crucial for secure and reliable communication in sensor networks. Furthermore, the average latency reduced from 120 ms to 85 ms, proving that the security enhancements did not negatively impact network performance and that the optimized routing ensured faster communication and minimal transmission delays. Overall, the Trust-GAEP-Net model effectively balances security, efficiency, and performance, making it a robust solution for securing IoT-based WSNs while maintaining high detection accuracy, low energy overhead, and fast, reliable communication.

TABLE IV. SECURITY METRICS EVALUATION

Metric	Value before implementation	Value after implementation
Detection rate (%)	85.2	99.1
False positive rate (%)	12.5	3.1
Energy overhead (J)	1.8	1.3
Data integrity score (0-1)	0.76	0.92
Average latency (ms)	120	85

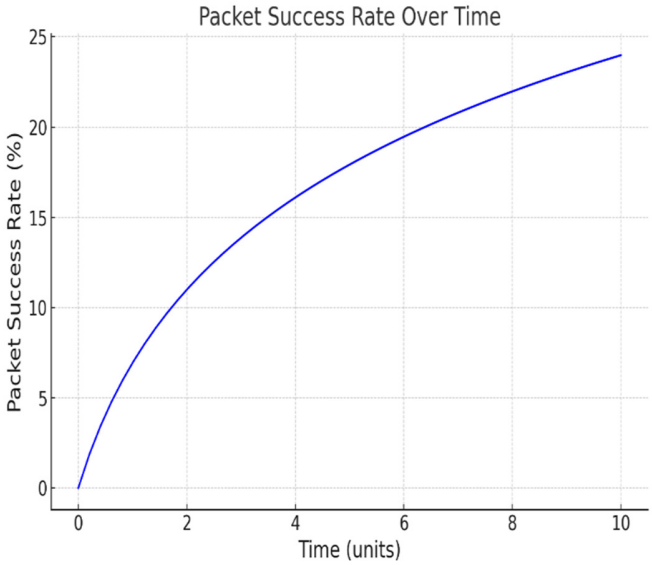

Fig. 7. Packet success rate.

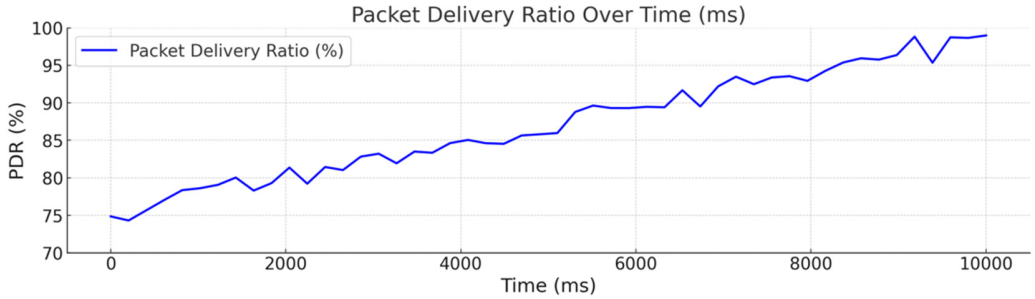

Fig. 8. Packet delivery ratio.

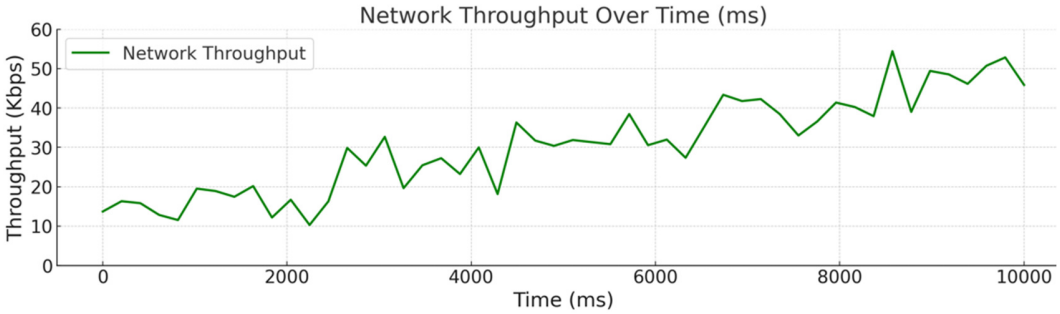

Fig. 9. Network throughput.

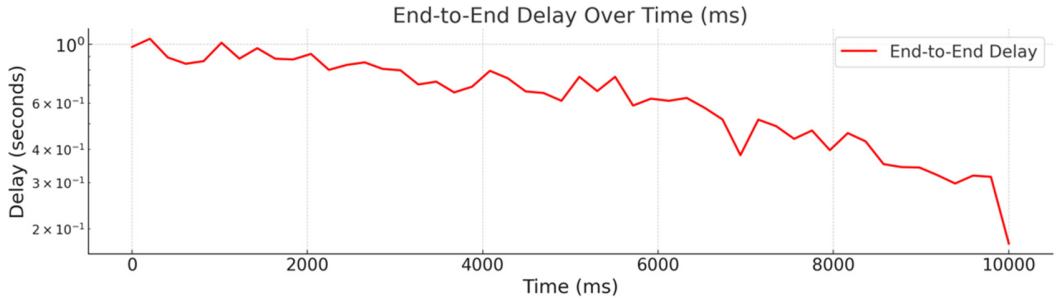

Fig. 10. End-to-end delay.

Figure 11 presents a bar chart that compares energy consumption metrics before and after implementing the Trust-GAEP-Net model, showcasing its effectiveness in optimizing routing and trust management. Total energy consumption decreased from 500 J to 420 J, reflecting a 16% reduction in unnecessary energy usage while maintaining network security. Energy consumption per node also dropped from 10 J to 8 J, demonstrating improved efficiency without compromising performance. Additionally, residual energy increased from 200 J to 280 J, indicating that nodes retain more power for extended operation, ultimately prolonging network lifespan. These results highlight the Trust-GAEP-Net model's ability to enhance energy efficiency by minimizing redundant transmissions and avoiding energy-draining malicious nodes. The network sustains operations for a longer duration, making it particularly suitable for IoT-WSN applications where energy conservation is crucial. The increase in residual energy further suggests that sensor nodes will have a longer lifespan, reducing the need for frequent battery replacements or recharging, thereby improving overall network sustainability.

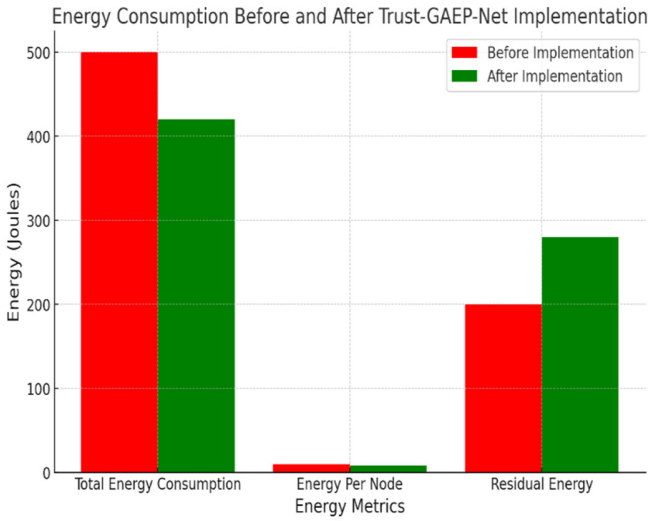

Fig. 11. Energy consumption and savings.

Table V compares the PDR values of different models. The BFA [21], the SCSOA [22], and the ETBR [23] achieved PDR values of 91%, 95%, and 90%, respectively, indicating acceptable performance in ensuring data delivery across the network. CHicDra [24] performed significantly worse, with a PDR of only 44%, indicating excessive packet loss and inefficient routing. WaOA [27] performed slightly better (81%), but still lags behind more optimized models. The proposed Trust-GAEP-Net model exhibited the highest PDR (98.9%), demonstrating its superior ability to ensure secure and reliable data transmission across IoT-WSNs.

TABLE V. PDR COMPARISON

Model [Citation number]	PDR (%)
BFA [21]	91
SCSOA [22]	95
ETBR [23]	90
CHicDra [24]	44
WaOA [27]	81
Proposed model (Trust-GAEP-Net)	98.9

Table VI illustrates the effectiveness with which each model detects malicious or compromised nodes. SCSOA [22] had a low detection rate of 67.43%, implying that it struggled to identify attacks effectively. GWO [25] significantly increased the detection rate to 96.7%, making it more effective at identifying security threats. NATURE [26] and WaOA [27] also had competitive detection rates of 91% and 93%, respectively, indicating improved trust-based routing mechanisms. However, none of these models matched the proposed model, Trust-GAEP-Net, which had a 99.1% detection rate.

TABLE VI. DETECTION RATE COMPARISON

Model [Citation number]	Detection rate (%)
SCSOA [22]	67.43
GWO [25]	96.7
NATURE [26]	91
WaOA [27]	93
Proposed model (Trust-GAEP-Net)	99.1

Table VII compares models based on power efficiency. CHicDra [24] had high energy overhead, making it unsuitable for energy-constrained IoT-WSNs. Similarly, GWO [25] was identified as computationally intensive, necessitating additional resources to maintain secure routing decisions. In contrast, the proposed Trust-GAEP-Net model showed optimized and low energy consumption, effectively reducing unnecessary energy expenditure while maintaining high security and performance.

TABLE VII. ENERGY OVERHEAD COMPARISON

Model [Citation number]	Energy overhead (J)
CHicDra [24]	High
GWO [25]	Computationally intensive
Proposed model (Trust-GAEP-Net)	Optimized & low

Table VIII compares the resource demands of various approaches. GWO [25] required significant processing power, rendering it unsuitable for lightweight IoT devices. Similarly, WaOA [27] had a high computational overhead, which could affect scalability and real-time performance. In contrast, the proposed model (Trust-GAEP-Net) was both efficient and scalable, achieving a balance between computational requirements and security efficiency while ensuring smooth performance in dynamic and resource-constrained environments.

TABLE VIII. COMPUTATIONAL COMPLEXITY COMPARISON

Model [Citation number]	Complexity
GWO [25]	High processing power required
WaOA [27]	High computational overhead
Proposed model (Trust-GAEP-Net)	Efficient & scalable

The method comparison tables demonstrate that the Trust-GAEP-Net model outperforms existing approaches in terms of packet delivery, detection accuracy, energy efficiency, and computational feasibility. This ensures a strong, scalable, and energy-efficient security solution for IoT-based WSNs, addressing the limitations of previous approaches.

The experimental outcomes were validated using average values from 20 simulations with randomly distributed node topologies, as shown in Table IX. The Trust-GAEP-Net model consistently demonstrated superior statistical performance across all key indicators. However, implementing Trust-GAEP-Net in IoT-WSNs presented several challenges. Sensor node limitations constrained the complexity of deep learning components. Furthermore, integrating GNNs for real-time trust updates resulted in latency in highly dynamic topologies.

TABLE IX. SUMMARY OF METRICS BEFORE AND AFTER MODEL IMPLEMENTATION

Metric	Before	After (Trust-GAEP-Net)
Detection rate (%)	85.2	99.1
False positive rate (%)	12.5	3.1
Energy overhead (J)	1.8	1.3
Avg. latency (ms)	120	85
Data integrity score	0.76	0.92

V. CONCLUSION AND SUMMARY

The proposed Trust-GAEP-Net model achieved a 99.1% detection rate and a 3.1% false positive rate, significantly enhancing the security of Internet of Things (IoT)-based Wireless Sensor Networks (WSNs) security. Data integrity improved to a score of 0.92, and total energy consumption was reduced by 16%, demonstrating superior performance in terms of reliability, scalability, and energy efficiency when compared to existing models.

The Trust-GAEP-Net model improves the security, efficiency, and reliability of IoT-based WSNs by combining Graph Neural Networks (GNN) for trust evaluation, AlexNet for deep feature extraction, and Enhanced Particle Swarm Optimization (EPSO) for optimal routing. The model effectively identifies malicious nodes, prevents security breaches, and optimizes data transmission paths, resulting in a Packet Delivery Ratio (PDR) of 98.9%. Trust-GAEP-Net enables robust, real-time, and reliable communication in

critical applications such as smart cities, healthcare monitoring, and industrial automation by balancing security and energy efficiency.

The model can be enhanced in the future to counter sophisticated cyber threats such as adversarial attacks, jamming, wormhole, and Sybil attacks, all of which pose significant risks to IoT-WSNs. Future extensions of the Trust-GAEP-Net model may include integration with edge or fog computing layers to support real-time trust computation closer to the data source, thereby reducing latency. Additionally, incorporating multi-hop trust propagation mechanisms can improve scalability and resilience in larger, heterogeneous IoT-WSN deployments with dynamic topologies.

REFERENCES

[1] M. S. Abdalzaher and O. Muta, "A Game-Theoretic Approach for Enhancing Security and Data Trustworthiness in IoT Applications," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11250–11261, Nov. 2020, https://doi.org/10.1109/JIOT.2020.2996671.

[2] D. Praveen Kumar, T. Amgoth, and C. S. R. Annavarapu, "Machine learning algorithms for wireless sensor networks: A survey," *Information Fusion*, vol. 49, pp. 1–25, Sept. 2019, https://doi.org/10.1016/j.inffus.2018.09.013.

[3] S. Karimullah, D. Vishnuvardhan, V. K. Gunjan, and F. Shaik, "Improved Spectral Efficiency Using Vehicular Visible Light Communication with 16-Bit DCO in OFDM," in *Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough: Volume 4*, V. K. Gunjan, J. M. Zurada, and N. Singh, Eds. Cham, Switzerland: Springer International Publishing, 2024, pp. 159–168.

[4] P. K. Donta, T. Amgoth, and C. S. R. Annavarapu, "Delay-aware data fusion in duty-cycled wireless sensor networks: A Q-learning approach," *Sustainable Computing: Informatics and Systems*, vol. 33, Jan. 2022, Art. no. 100642, https://doi.org/10.1016/j.suscom.2021.100642.

[5] K. Demertzis, L. Iliadis, N. Tziritas, and P. Kikiras, "Anomaly detection via blockchained deep learning smart contracts in industry 4.0," *Neural Computing and Applications*, vol. 32, no. 23, pp. 17361–17378, Dec. 2020, https://doi.org/10.1007/s00521-020-05189-8.

[6] V. Kavitha and K. Ganapathy, "Galactic swarm optimized convolute network and cluster head elected energy-efficient routing protocol in WSN," *Sustainable Energy Technologies and Assessments*, vol. 52, no. B, Aug. 2022, Art. no. 102154, https://doi.org/10.1016/j.seta.2022.102154.

[7] J. T. Oke, J. Agajo, B. K. Nuhu, J. G. Kolo, and L. A. Ajao, "Two Layers Trust-Based Intrusion Prevention System for Wireless Sensor Networks," *Advances in Electrical and Electronic Engineering*, vol. 1, pp. 23–29, May 2018.

[8] P. M. Urs, A. T. N. Reddy, S. Mallikarjunaswamy, and U. M. Lakshminarayan, "An Innovative IoT Framework using Machine Learning for Predicting Information Loss at the Data Link Layer in Smart Networks," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 20904–20911, Apr. 2025, https://doi.org/10.48084/etasr.9597.

[9] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology," *International Journal of Distributed Sensor Networks*, vol. 15, no. 4, Apr. 2019, Art. no. 1550147719844159, https://doi.org/10.1177/1550147719844159.

[10] C. Shin and M. Lee, "Swarm-Intelligence-Centric Routing Algorithm for Wireless Sensor Networks," *Sensors*, vol. 20, no. 18, Sept. 2020, Art. no. 5164, https://doi.org/10.3390/s20185164.

[11] A. H. Wheeb *et al.*, "Improvised Spectral Efficiency and Channel Estimation Parameters in Visible Light Vehicular Communication by Integrating Simulation of Urban Mobility Data," *IEEE Access*, vol. 13, pp. 70828–70848, 2025, https://doi.org/10.1109/ACCESS.2025.3558697.

[12] P. K. Roy and A. Bhattacharya, "SDIWSN: A Software-Defined Networking-Based Authentication Protocol for Real-Time Data Transfer in Industrial Wireless Sensor Networks," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 3465–3477, Sept. 2022, https://doi.org/10.1109/TNSM.2022.3173975.

[13] T. Shankar, S. Shanmugavel, and A. Rajesh, "Hybrid HSA and PSO algorithm for energy efficient cluster head selection in wireless sensor networks," *Swarm and Evolutionary Computation*, vol. 30, pp. 1–10, Oct. 2016, https://doi.org/10.1016/j.swevo.2016.03.003.

[14] A. Balasundaram, S. Routray, A. V. Prabu, P. Krishnan, P. P. Malla, and M. Maiti, "Internet of Things (IoT)-Based Smart Healthcare System for Efficient Diagnostics of Health Parameters of Patients in Emergency Care," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18563–18570, Nov. 2023, https://doi.org/10.1109/JIOT.2023.3246065.

[15] J. Wang, X. Jing, Z. Yan, Y. Fu, W. Pedrycz, and L. T. Yang, "A Survey on Trust Evaluation Based on Machine Learning," *ACM Computing Surveys*, vol. 53, no. 5, Sept. 2020, Art. no. 107, https://doi.org/10.1145/3408292.

[16] A. V. Krishna and A. A. Leema, "ETM-IoT: Energy-Aware Threshold Model for Heterogeneous Communication in the Internet of Things," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 1815–1827, Sept. 2021, https://doi.org/10.32604/cmc.2022.018455.

[17] A. Makkar, U. Ghosh, and P. K. Sharma, "Artificial Intelligence and Edge Computing-Enabled Web Spam Detection for Next Generation IoT Applications," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25352–25361, Nov. 2021, https://doi.org/10.1109/JSEN.2021.3066492.

[18] T. Khan *et al.*, "An efficient trust-based decision-making approach for WSNs: Machine learning oriented approach," *Computer Communications*, vol. 209, pp. 217–229, Sept. 2023, https://doi.org/10.1016/j.comcom.2023.06.014.

[19] G. Samara, G. A. Besani, M. Alauthman, and M. A. Khaldy, "Energy-Efficiency Routing algorithms in Wireless Sensor Networks: a Survey." arXiv, Feb. 18, 2020, https://doi.org/10.48550/arXiv.2002.07178.

[20] P. K. Donta, T. Amgoth, and C. S. Rao Annavarapu, "Congestion-aware Data Acquisition with Q-learning for Wireless Sensor Networks," in *2020 IEEE International IOT, Electronics and Mechatronics Conference*, Vancouver, Canada, 2020, pp. 1–6, https://doi.org/10.1109/IEMTRONICS51293.2020.9216379.

[21] C. Edwin Singh, S. Sharon Priya, B. Muthu Kumar, K. Saravanan, A. Neelima, and B. Gireesha, "Trust aware fuzzy clustering based reliable routing in Manet," *Measurement: Sensors*, vol. 33, June 2024, Art. no. 101142, https://doi.org/10.1016/j.measen.2024.101142.

[22] M. G, A. A, R. R, K. K, and J. C. S. C, "Trust And Energy-Aware Routing Protocol for Wireless Sensor Networks Based on Secure Routing," *International Journal of Electrical and Computer Engineering Systems*, vol. 14, no. 9, pp. 1015–1022, Oct. 2023, https://doi.org/10.32985/ijeces.14.9.6.

[23] B. Sreevidya and M. Supriya, "Trust based Routing – A Novel Approach for Data Security in WSN based Data Critical Applications," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 15, no. 1, pp. 27–41, Mar. 2024, https://doi.org/10.58346/jowua.2024.i1.003.

[24] P. Rodrigues and J. John, "Joint trust: an approach for trust-aware routing in WSN," *Wireless Networks*, vol. 26, no. 5, pp. 3553–3568, July 2020, https://doi.org/10.1007/s11276-020-02271-w.

[25] A. Saleh, P. Joshi, R. S. Rathore, and S. S. Sengar, "Trust-Aware Routing Mechanism through an Edge Node for IoT-Enabled Sensor Networks," *Sensors*, vol. 22, no. 20, Oct. 2022, Art. no. 7820, https://doi.org/10.3390/s22207820.

[26] V. Pathak, K. Singh, T. Khan, M. Shariq, S. A. Chaudhry, and A. K. Das, "A secure and lightweight trust evaluation model for enhancing decision-making in resource-constrained industrial WSNs," *Scientific Reports*, vol. 14, no. 1, Nov. 2024, Art. no. 28162, https://doi.org/10.1038/s41598-024-75414-0.

[27] R. Kennady and K. Thinakaran, "An Adapted Walrus Optimal Routing with Reputation Trust Based Secure Protocol For WSN," *International Journal of Electronics and Communication Engineering*, vol. 11, no. 1, pp. 101–115, Jan. 2024, https://doi.org/10.14445/23488549/IJECE-V11I1P108.

AUTHORS PROFILE

Pidugu Purushotham is a Research Scholar in the Department of Computer Science and Engineering at GITAM (Deemed to be University), Hyderabad, Telangana. His research interests include IoT, Wireless Sensor Networks, Machine Learning, Deep Learning and Artificial Intelligence.

Akkalakshmi Muddana is a Professor in the Department of Computer Science and Engineering at GITAM (Deemed to be University), Hyderabad, Telangana. Her research interests include Machine Learning and Data Security.