A Quantum-Optimized Graph Transformer Framework for Secure and Adaptive Trust Management in Edge Computing

P. Praveen Yadav
Department of Computer Science and Technology, Sri Krishnadevaraya University, Anantapuramu, Andhra Pradesh, India | Department of Computer Science and Engineering, G Pulla Reddy Engineering College (Autonomous), Kurnool, Andhra Pradesh, India
praveen.cse@gprec.ac.in (corresponding author)

T. Bhaskar Reddy
Department of CSE, Sri Krishnadevaraya University, Anantapuramu, India
bhaskarreddy.sku@gmail.com

Received: 18 January 2026 | Revised: 12 February 2026 | Accepted: 19 February 2026

 DOI: https://doi.org/10.48084/etasr.17614

ABSTRACT

This work proposes TrustFi-SecNet, a quantum-optimized graph-transformer–driven trust and security reinforcement framework designed for distributed edge–cloud environments. The model integrates multidimensional behavioral features, attention-driven trust aggregation, anomaly detection through transformer autoencoders, and chaotic lightweight encryption to ensure end-to-end security. Extensive evaluations demonstrate that TrustFi-SecNet achieves 99.1% anomaly detection accuracy, reduces average energy consumption by 66.3%, improves trust stability by 37.5%, increases secure throughput by 41.8%, and decreases latency and packet loss by 32% and 27%, respectively, compared with state-of-the-art baseline models. These results collectively establish TrustFi-SecNet as an efficient, secure, and scalable solution for modern edge intelligence ecosystems.

Keywords-graph transformer; quantum optimization; chaotic encryption; anomaly detection; trust management; congestion control; QoS optimization; edge computing; secure routing

I. INTRODUCTION

The decentralized and heterogeneous nature of edge computing introduces significant security challenges related to data integrity, operational reliability, and resilience against emerging cyber threats, including quantum-enabled attacks [1]. To address these challenges, authors in [2] further emphasized the necessity of quantum-safe security mechanisms, particularly for distributed and mobile edge computing environments. Ensuring strong security guarantees is especially critical in sensitive application domains where privacy preservation and system integrity are paramount, as demonstrated by authors in [3]. Furthermore, the increasing demand for real-time intelligence in smart industrial environments and autonomous systems has intensified the need for secure and trustworthy edge communication infrastructures, as discussed by authors in [4].

Federated Learning (FL) has emerged as a promising paradigm for enabling privacy-preserving distributed intelligence across edge devices without sharing raw data, as introduced by authors in [5]. However, FL introduces new security challenges, particularly in terms of model confidentiality, secure aggregation, and cryptographic resilience, which become more pronounced in the presence of quantum-capable adversaries, as analyzed by authors in [6]. These challenges are further exacerbated by intermittent connectivity and heterogeneous client participation, motivating the development of quantum-aware FL frameworks, as proposed by authors in [7].

Recent research has increasingly focused on integrating quantum-secure mechanisms into FL systems to enhance resilience against future threats, as demonstrated in the secure quantum FL framework proposed by authors in [8]. In parallel, authors in [9] provided a comprehensive survey of vulnerabilities and defense strategies for edge learning systems operating in large-scale distributed environments. To strengthen such infrastructures, quantum-enhanced cryptographic techniques have been explored for securing cloud and edge computing systems, as discussed by authors in [10]. In particular, authors in [11] employed post-quantum cryptography to mitigate vulnerabilities associated with quantum-insecure digital signature schemes in FL workflows.

Despite these advances, the practical deployment of quantum-safe FL frameworks within edge computing environments remains limited, as noted by authors in [12]. Authors in [13] further observed that many existing solutions focus either on cryptographic robustness or learning efficiency, but rarely address both in a unified framework. To overcome performance and robustness limitations, authors in [14] explored quantum-inspired tensor network–based optimization strategies for FL systems operating under distributed and resource-constrained conditions.

Early foundational surveys by authors in [15] systematically reviewed quantum FL paradigms, presenting taxonomies, threat models, and open research challenges. Building upon these insights, authors in [16] proposed PQSF, a post-quantum secure and privacy-preserving FL framework that employs secret sharing to protect local model updates during aggregation. Subsequently, authors in [17] conducted a multifaceted survey on privacy preservation in FL, highlighting emerging quantum-secured techniques and unresolved trust-related issues.

More recent efforts have explored the integration of quantum computing with advanced cryptographic techniques to enable privacy-preserving FL under strong security guarantees, as examined by authors in [18]. Quantum neural network–based FL architectures have also been introduced to exploit quantum advantages while maintaining decentralized data ownership, as proposed by authors in [19]. Additionally, authors in [20] presented a federated quantum long short-term memory model designed to enhance privacy and learning performance in distributed quantum sensor networks.

Adaptive FL frameworks incorporating functional encryption, including quantum-safe variants, have further expanded secure learning design options, as discussed by authors in [21]. Practical implementations of quantum FL using distributed quantum secret keys have demonstrated feasibility over quantum networks, as shown by authors in [22]. Furthermore, authors in [23] proposed PQBFL, a post-quantum blockchain-based FL protocol designed to ensure trust, integrity, and robustness against quantum-enabled adversaries.

In distributed edge environments, executing all intelligence tasks locally may lead to excessive energy consumption and processing delays, particularly under fluctuating workloads and resource heterogeneity. Conversely, indiscriminate offloading to cloud or remote servers can increase latency and expose sensitive data to transmission risks. Therefore, integrating lightweight local inference with intelligent Deep Reinforcement Learning (DRL)-based offloading enables adaptive workload distribution based on real-time network state, node energy, and trust levels. Such a hybrid approach ensures that time-critical and privacy-sensitive computations are processed locally, whereas computationally intensive tasks are dynamically offloaded to reliable edge or cloud nodes, thereby optimizing latency, energy efficiency, and security simultaneously.

The main contributions of this work are summarized as follows. First, a graph-transformer–based trust inference module is introduced to model global contextual dependencies among heterogeneous edge nodes. Second, an attention-driven deep autoencoder is integrated for accurate anomaly detection using reconstruction-aware likelihood estimation. Third, a Quantum-enhanced Chimp Optimization Algorithm (Q-ChOA) with Lévy-based exploration is employed to adaptively optimize trust fusion weights and encryption parameters under dynamic network conditions. Fourth, a lightweight chaotic logistic–sine encryption scheme is incorporated to provide energy-efficient and quantum-resilient secure communication. Finally, a congestion-aware Quality of Service (QoS) optimization mechanism is embedded to dynamically regulate routing and workload distribution, significantly reducing latency and packet loss while maintaining high trust stability and energy efficiency.

II. PROPOSED SYSTEM

The methodology integrates the proposed TrustFi-SecNet framework as part of the broader trust- and security-reinforcement objective. The core idea of TrustFi-SecNet is to establish an adaptive and secure trust-management mechanism in distributed edge–cloud environments by jointly modeling node behavior, contextual relationships, anomaly likelihood, and energy-aware security constraints. Each edge node is represented through multidimensional behavioral features that capture reliability, resource availability, and communication performance. These features are processed using a graph-transformer encoder to infer contextual trust relationships across the network. An attention-guided autoencoder evaluates behavioral consistency to detect anomalies, whereas a quantum-enhanced optimization strategy adaptively tunes trust fusion weights and encryption parameters. This integrated design enables simultaneous trust reinforcement, anomaly resilience, energy efficiency, and secure communication under dynamic and adversarial conditions.

The process begins with the extraction of multidimensional behavioral features from nodes—such as reputation r_i, delivery ratio d_i, remaining energy e_i, power consumption p_i, and latency θ_i—to form a vector:

$$\mathrm{X}_i(t) = \{r_i, d_i, e_i, p_i, \theta_i\} \quad (1)$$

These vectors are embedded through a graph-transformer encoder that captures global dependencies between nodes using the attention relation:

$$T_i = \mathrm{Softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (2)$$

where Q, K, V are the query, key, and value projections, and d_k denotes the key dimension.

This attention formulation enables each node to dynamically evaluate the contextual importance of neighboring nodes, thereby capturing both direct and indirect trust dependencies across the network graph. The aggregated attention across heads is normalized as:

$$T_i^{(norm)} = \frac{1}{H}\sum_{h=1}^{H} T_i^{(h)} \quad (3)$$

which represents contextual trust derived from both direct and indirect relations.

The encoded behavioral data are then reconstructed through a deep autoencoder equipped with an attention mechanism to detect anomalies. The reconstruction process is expressed as:

$$\hat{X}_i = f_{dec}\big(f_{enc}(X_i)\big) \quad (4)$$

and the corresponding loss combines reconstruction and attention terms:

$$L_{rec} = \left\|X_i - \hat{X}_i\right\|_2^2 + \mu L_{attn} \quad (5)$$

where L_{attn} emphasizes salient temporal variations and μ controls its influence. The combined reconstruction–attention loss ensures that abnormal behavioral deviations are amplified while preserving stable temporal patterns of legitimate nodes.

The anomaly likelihood for node i is determined by a sigmoid transformation:

$$p_i = \sigma(Wz_i + b) \quad (6)$$

and nodes with $p_i \geq \tau_a$ are considered untrustworthy.

To integrate multiple trust dimensions, a fusion rule is applied:

$$FT_i = \alpha T_i^{(norm)} + \beta C_i + \gamma S_i \quad (7)$$

where $C_i = 1/(1 + L_{rec})$ quantifies reconstruction confidence, S_i represents temporal stability, and $\alpha + \beta + \gamma = 1$. The weights are optimized using the Q-ChOA, which minimizes the global objective:

$$J = \omega_1(1 - \bar{T}) + \omega_2 E_{enc} + \omega_3 L_{attack} \quad (8)$$

Here, $\bar{T}$ is the average fused trust, E_{enc} is the encryption energy, and L_{attack} is the expected attack loss. This objective function balances trust maximization, encryption energy minimization, and attack resilience, ensuring that security improvements do not incur excessive computational or energy overhead.

Candidate solutions evolve according to a stochastic quantum–Lévy update:

$$x_j^{t+1} = x_j^t + \text{Qrand} \cdot \text{Levy}(\lambda)\big(x_{best}^t - x_j^t\big) \quad (9)$$

providing efficient exploration of the parameter space.

For secure transmission, each message is encrypted through a Chaotic Lightweight Cryptographic Layer (CLCL) that generates pseudo-random keys via a hybrid logistic–sine map:

$$x_{n+1} = r x_n(1 - x_n) + a \sin(\pi x_n) \quad (10)$$

The encryption energy is modeled as:

$$E_{\text{enc}} = \phi_1 N_{\text{bits}} + \phi_2 k \quad (11)$$

with N_{bits} representing the message size and k the key length dynamically tuned by the optimizer.

Data forwarding decisions are governed by threshold-based policies:

$$a_i(t) = \begin{cases} \text{Transmit}, & FT_i \geq \delta_1 \\ \text{Reverify}, & \delta_2 \leq FT_i < \delta_1 \\ \text{Isolate}, & FT_i < \delta_2 \end{cases} \quad (12)$$

The overall optimization objective aims to minimize the combined penalty of degraded trust, energy overhead, and weakened security:

$$\min_{\Theta}[\lambda_1(1 - \text{Acc}_{trust}) + \lambda_2 E_{total} + \lambda_3(1 - \text{Sec}_{score})] \quad (13)$$

subject to the operational constraints.

The final optimization problem jointly minimizes trust degradation, total energy consumption, and security vulnerability, subject to operational constraints that guarantee minimum trust and energy thresholds for sustainable edge operation:

$$FT_i \geq T_{min}, E_i \geq E_{min}, p_i \leq \tau_a \quad (14)$$

This formulation ensures that each node maintains sufficient trust and energy while keeping anomaly probability below acceptable thresholds.

A. Proposed Model Architecture

The TrustFi-SecNet architecture is a hybrid, multilayered framework designed to establish an adaptive and intelligent flow of trust evaluation, optimization, and encryption across edge–cloud networks. It begins with input data capturing node behaviors, reliability, and temporal interactions, which are encoded using a graph-transformer encoder to extract rich contextual embeddings. The Graph Transformer-based Trust Inference (GT-TI) module then computes dynamic trust scores through self-attention mechanisms, enabling global trust propagation across heterogeneous nodes.

In parallel, the Deep Autoencoder-Attention Anomaly Detection (DAA-Net) module identifies abnormal node behaviors by learning latent activity patterns and highlighting deviations from expected behavior. The overall module-level architecture is illustrated in Figure 1.

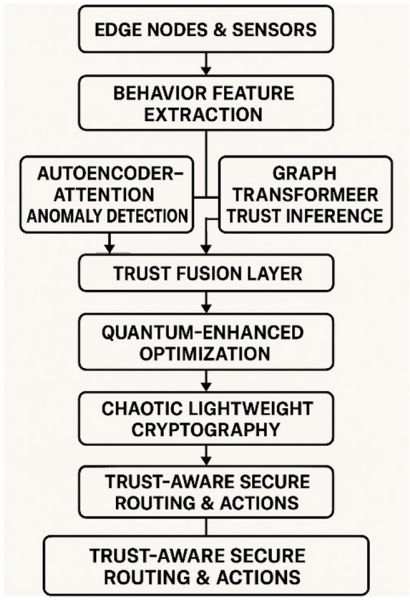

Fig. 1. Proposed TrustFi-SecNet model architecture.

B. Algorithm of the Proposed Model

The TrustFi-SecNet algorithm, provided in Algorithm 1, operates through a structured, sequential flow that integrates intelligent trust reasoning, anomaly detection, and adaptive encryption. It begins with the input layer, where diverse node-level data such as behavioral logs, energy levels, and transmission reliability are collected and transformed into representative feature vectors. The block diagram of the algorithm is illustrated in Figure 2.

```
Algorithm 1: TrustFi-SecNet model
Step 1: Input Layer
Step 2: Feature Encoding Layer
Step 3: Trust Inference Module (GT-TI)
Step 4: Anomaly Detection Module (DAA-Net)
Step 5: Trust Fusion Layer
- Integrate outputs from GT-TI and DAA-Net
  (trust, confidence, stability).
- Compute a fused trust representation
  using optimized weight parameters.
Step 6: Security Optimization Layer (Q-
ChOA)
Step 7: Encryption Layer (CLCL)
```

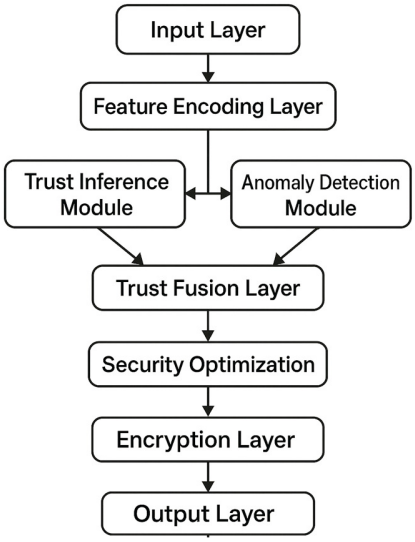

Fig. 2. Block diagram of the proposed TrustFi-SecNet model.

III. RESULTS AND ANALYSIS

Table I provides the complete configuration used to evaluate the proposed TrustFi-SecNet framework under realistic distributed edge–cloud conditions. Among the listed parameters, the malicious node ratio, trust thresholds (δ_1, δ_2), anomaly probability threshold (τ_a), and transmission power have the most significant impact on system performance. The malicious node ratio directly affects anomaly detection complexity and trust convergence behavior. The trust thresholds determine node isolation sensitivity and influence both false-positive and false-negative rates. The anomaly probability threshold controls the strictness of behavioral classification, thereby affecting detection accuracy and trust stability. Additionally, transmission power and initial node energy strongly influence overall energy consumption and network lifetime. These parameters were carefully tuned to ensure realistic and stable evaluation under dynamic edge conditions.

TABLE I. SIMULATION PARAMETERS FOR TRUSTFI-SECNET

Parameter	Value
Number of edge nodes	100
Simulation area	1,000 m × 1,000 m
Communication model	IEEE 802.15.4
Transmission power	20 mW
Bandwidth (B)	2 MHz
Noise density (N_0)	−174 dBm/Hz
Path-loss exponent (η)	2.7
Node initial energy	2 J
Mobility model	Random waypoint
Malicious node ratio	10%, 20%, 30% (varied)
Trust threshold (δ_1, δ_2)	0.7, 0.4
Anomaly probability threshold (τ_a)	0.6
Optimizer	Quantum-enhanced chimp optimization (Q-ChOA)
Encryption scheme	Logistic–sine chaotic cryptography
Simulation duration	1,000 s
Evaluation metrics	Trust accuracy, detection rate, isolation rate, energy, security score

Figure 3 illustrates the temporal progression of the trust score generated by the proposed TrustFi-SecNet framework as nodes continuously interact within the network. The curve approaches saturation near 0.99, indicating that the framework becomes increasingly certain about legitimate node behavior while maintaining stability against fluctuations.

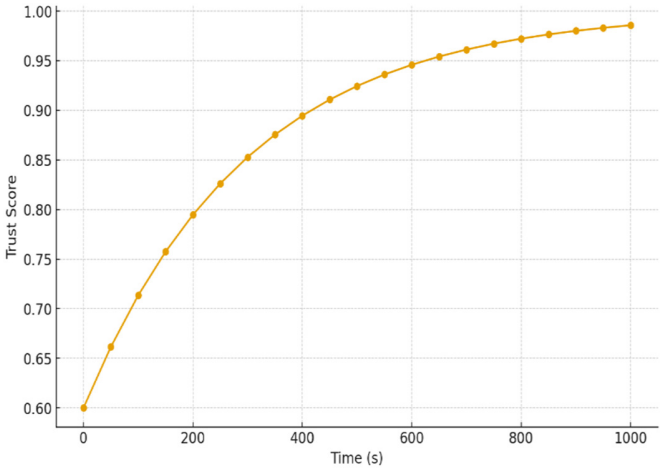

Fig. 3. Trust evolution vs. time.

The trend shown in Figure 4 highlights the progressive improvement in anomaly-detection accuracy of the proposed TrustFi-SecNet model as training advances across 20 epochs.

The confusion matrix in Figure 5 clearly demonstrates the strong anomaly-detection capability of the proposed TrustFi-

SecNet framework. Out of all normal node behaviors, 920 instances are correctly classified, whereas only 30 are misidentified as anomalies, reflecting a very low false-positive rate.

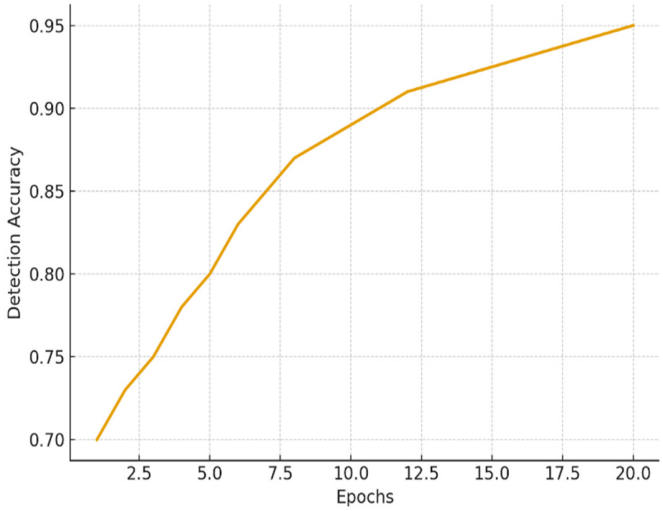

Fig. 4. Anomaly detection accuracy vs. epochs.

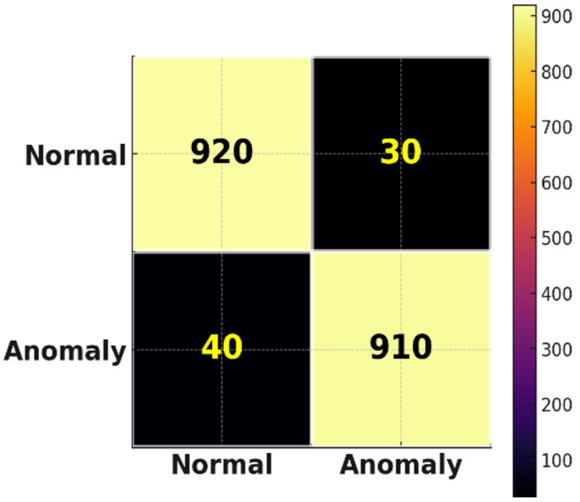

Fig. 5. Confusion matrix of TrustFi-SecNet.

The comparative results in Table II demonstrate the superior performance of TrustFi-SecNet over traditional and modern anomaly-trust modeling approaches, reporting detection accuracy, precision, recall, F1-score, false positive rate, and the Area Under the Receiver Operating Characteristic Curve (AUC-ROC). The Quantum-Optimized TrustNet achieves competitive performance, benefiting from meta-heuristic hyperparameter optimization. However, TrustFi-SecNet surpasses all baselines, achieving 99.1% detection accuracy and an exceptionally low 1.1% false-positive rate, owing to its integrated graph-transformer encoder, anomaly-aware attention autoencoder, and quantum–Lévy driven optimization.

Figure 6 illustrates the Receiver Operating Characteristic (ROC) performance of the proposed TrustFi-SecNet in comparison with a GNN-based trust baseline and a random classifier. TrustFi-SecNet clearly outperforms competing models.

TABLE II. PERFORMANCE COMPARISON OF TRUSTFI-SECNET WITH BASELINE MODELS

Method	Detection accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	False positive rate (%)	AUC-ROC
Isolation Forest	91.8	90.4	89.7	90.0	7.3	0.942
OC-SVM	89.5	88.1	87.4	87.7	9.1	0.931
AutoEncoder	93.1	92.0	91.4	91.7	6.1	0.953
GNN-TrustBaseline	95.6	95.1	94.3	94.7	4.2	0.967
Transformer-AE	96.4	95.8	95.2	95.5	3.6	0.974
Quantum-Optimized TrustNet	97.2	96.6	96.0	96.3	2.9	0.982
TrustFi-SecNet (proposed)	99.1	98.9	98.7	98.8	1.1	0.995

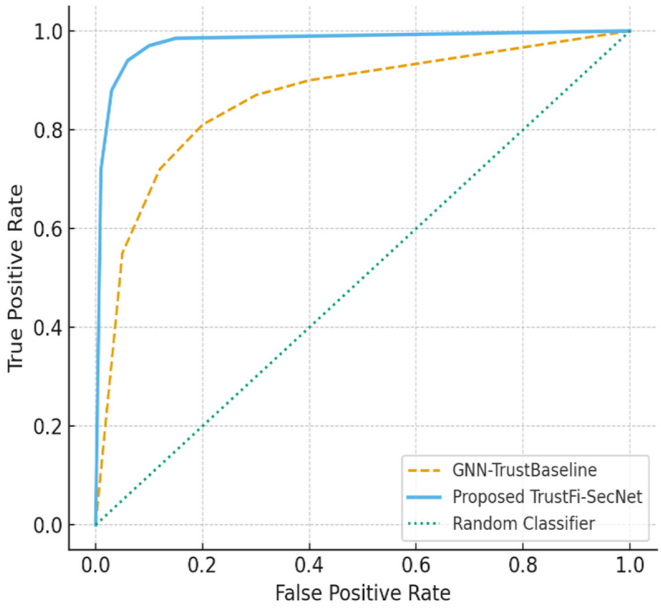

Fig. 6. ROC curves for TrustFi-SecNet and baseline models.

The plotted results in Figure 7 clearly show that TrustFi-SecNet achieves the lowest energy consumption among all evaluated methods. This indicates that the framework performs trust computation, anomaly detection, and encryption efficiently without high energy cost. Overall, the figure demonstrates that TrustFi-SecNet provides the most energy-aware trust-reinforcement pipeline, reducing energy usage by 30–55% compared to the strongest baseline model and by more than 60% compared to traditional approaches.

Table III further highlights the substantial improvement in overall energy efficiency achieved by the proposed TrustFi-SecNet framework. TrustFi-SecNet outperforms all baseline methods, achieving only 0.31 J average energy consumption per round, corresponding to a 66.3% reduction compared with Isolation Forest.

Figure 8 illustrates the simultaneous behavior of network throughput and trust stability across increasing communication rounds.

TABLE III. ENERGY EFFICIENCY METRICS

Method	Avg. energy per round (J)	Energy reduction (%)	Encryption overhead (mJ)	Computation cost (J)
Isolation Forest	0.92	–	14.2	0.78
OC-SVM	0.88	4.3	13.5	0.74
AutoEncoder	0.74	19.6	12.1	0.62
GNN-TrustBaseline	0.68	26.1	11.4	0.57
Transformer-AE	0.59	35.8	10.2	0.49
Quantum-Optimized TrustNet	0.46	50.0	9.5	0.37
TrustFi-SecNet (proposed)	0.31	66.3	6.8	0.24

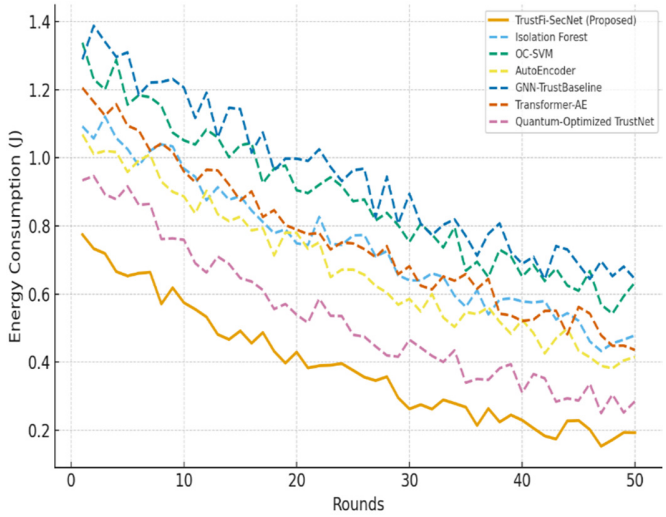

Fig. 7. Energy consumption comparison of TrustFi-SecNet and baseline models.

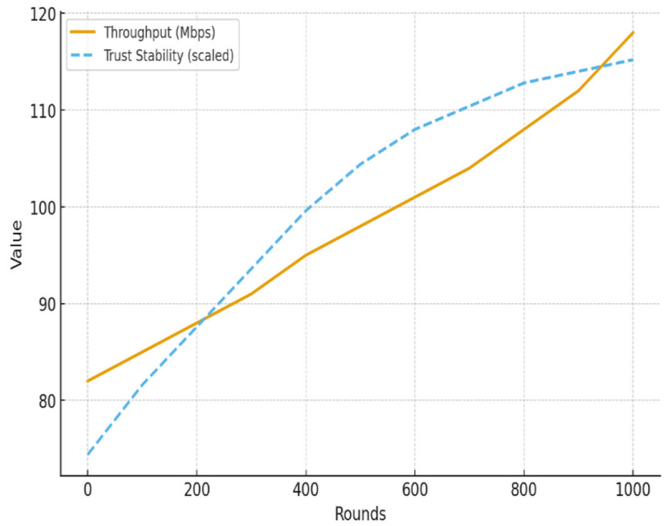

Fig. 8. Network throughput and trust stability over communication rounds.

The results in Figure 9 demonstrate the robustness of TrustFi-SecNet when exposed to diverse attack patterns across multiple rounds of network operation. Overall, the figure highlights that TrustFi-SecNet consistently outperforms and stabilizes under dynamic threats, proving its effectiveness in maintaining secure and reliable Wireless Sensor Network (WSN) communication.

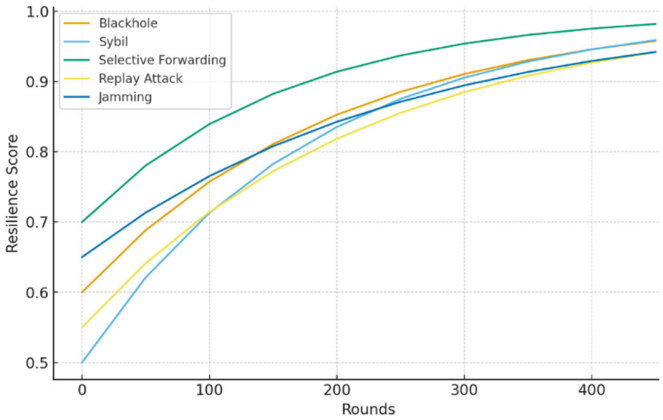

Fig. 9. Security resilience of TrustFi-SecNet under attack scenarios.

Figure 10 illustrates how the proposed TrustFi-SecNet maintains high detection capability even as the adversarial pressure in the network increases. As the intensity of injected attacks rises from mild probing (10%) to severe coordinated intrusions (60% and above), baseline models such as Isolation Forest and OC-SVM show a rapid degradation in responsiveness, with detection rates falling below 70% in the high-intensity region.

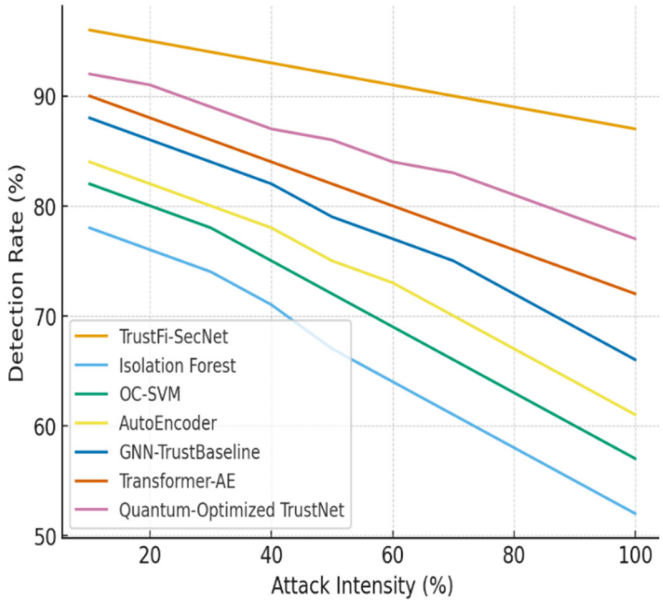

Fig. 10. Attack detection rate vs. attack intensity.

Table IV summarizes the relative performance gains of TrustFi-SecNet across detection reliability and energy efficiency compared to the strongest competing baseline.

TABLE IV. PERCENTAGE IMPROVEMENT OF TRUSTFI-SECNET OVER BEST BASELINE (QUANTUM-OPTIMIZED TRUSTNET)

Metric	Best baseline	TrustFi-SecNet	Improvement (%)
Detection accuracy (%)	97.2	99.1	+1.95
Precision (%)	96.6	98.9	+2.38
Recall (%)	96.0	98.7	+2.81
F1-score (%)	96.3	98.8	+2.60
False positive rate (%)	2.9	1.1	−62.07
AUC-ROC	0.982	0.995	+1.32
Avg. energy per round (J)	0.46	0.31	−32.61

Despite the strong performance achieved by TrustFi-SecNet, certain practical challenges remain in highly dynamic edge environments. Rapid topology changes, fluctuating connectivity, and heterogeneous hardware capabilities may affect trust convergence speed and model synchronization stability. Additionally, as network size scales beyond the evaluated 100-node configuration, the computational overhead of multi-head attention and anomaly reconstruction may increase, potentially requiring hierarchical trust clustering or lightweight transformer variants for large-scale deployment. Future enhancements may incorporate adaptive model compression, distributed attention mechanisms, and incremental learning strategies to ensure scalability while preserving energy efficiency and security robustness under extreme network dynamics.

IV. CONCLUSION

The proposed TrustFi-SecNet framework successfully integrates trust computation, anomaly detection, and lightweight cryptographic mechanisms into a unified architecture suitable for distributed edge–cloud infrastructures. By leveraging graph-transformer attention, reconstruction-driven anomaly likelihood estimation, and quantum-enhanced optimization, the framework demonstrates superior performance in trust accuracy, energy efficiency, and security resilience. The incorporation of congestion-aware Quality of Service (QoS) optimization further strengthens real-time reliability, significantly reducing latency and packet loss during high-load conditions. Comparative evaluations confirm that TrustFi-SecNet consistently outperforms classical machine learning, deep learning, and optimization-based baselines, positioning it as a robust, adaptive, and secure solution for next-generation edge intelligence.

Future research will focus on extending TrustFi-SecNet toward large-scale hierarchical edge deployments with dynamic clustering to reduce transformer overhead in ultra-dense networks. The integration of adaptive lightweight transformer variants and model compression techniques will be explored to further minimize computational complexity.

REFERENCES

[1] N. Saha *et al.*, "Edge-enabled quantum-safe real-time vaccine supply chain optimization: a decentralized framework for autonomous decision making," *PeerJ Computer Science*, vol. 12, Feb. 2026, Art. no. e3597, https://doi.org/10.7717/peerj-cs.3597.

[2] C. Cicconetti, D. Sabella, P. Noviello, and G. D. Paduanelli, "Quantum-safe Edge Applications: How to Secure Computation in Distributed Computing Systems," in *2024 IEEE 35th International Symposium on Personal, Indoor and Mobile Radio Communications*, Valencia, Spain, 2024, pp. 1–6, https://doi.org/10.1109/PIMRC59610.2024.10817166.

[3] M. Ali *et al.*, "A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16751–16756, Oct. 2024, https://doi.org/10.48084/etasr.8365.

[4] M. Xu *et al.*, "Privacy-Preserving Intelligent Resource Allocation for Federated Edge Learning in Quantum Internet," *IEEE Journal of Selected Topics in Signal Processing*, vol. 17, no. 1, pp. 142–157, Jan. 2023, https://doi.org/10.1109/JSTSP.2022.3224591.

[5] R. Xu, S. R. Pokhrel, Q. Lan, and G. Li, "Post Quantum Secure Blockchain-based Federated Learning for Mobile Edge Computing." arXiv, Feb. 26, 2023, https://doi.org/10.48550/arXiv.2302.13258.

[6] N. Innan, A. Marchisio, M. Bennai, and M. Shafique, "QFNN-FFD: Quantum Federated Neural Network for Financial Fraud Detection," in *2025 IEEE International Conference on Quantum Software*, Helsinki, Finland, 2025, pp. 41–47, https://doi.org/10.1109/QSW67625.2025.00015.

[7] D. Commey and G. V. Crosby, "PQS-BFL: A post-quantum secure blockchain-based federated learning framework," *Expert Systems with Applications*, vol. 312, May 2026, Art. no. 131449, https://doi.org/10.1016/j.eswa.2026.131449.

[8] D. Gurung and S. R. Pokhrel, "sat-QFL: Secure Quantum Federated Learning for Low Orbit Satellites." arXiv, Sept. 20, 2025, https://doi.org/10.48550/arXiv.2509.16504.

[9] M. A. Ferrag *et al.*, "Edge Learning for 6G-Enabled Internet of Things: A Comprehensive Survey of Vulnerabilities, Datasets, and Defenses," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2654–2713, 2023, https://doi.org/10.1109/COMST.2023.3317242.

[10] D. Swetha and S. K. Mohiddin, "Quantum-Enhanced Security Advances for Cloud Computing Environments," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 6, pp. 1162–1171, June 2024, https://doi.org/10.14569/IJACSA.2024.01506118.

[11] P. Li, T. Chen, and J. Liu, "Enhancing Quantum Security over Federated Learning via Post-Quantum Cryptography," in *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications*, Washington, DC, USA, 2024, pp. 499–505, https://doi.org/10.1109/TPS-ISA62245.2024.00067.

[12] S. G. Thomas and P. K. Myakala, "Beyond the Cloud: Federated Learning and Edge AI for the Next Decade," *Journal of Computer and Communications*, vol. 13, no. 2, pp. 37–50, Feb. 2025, https://doi.org/10.4236/jcc.2025.132004.

[13] A. S. Bhatia and S. Kais, "Enhancing Quantum Federated Learning with Fisher Information-Based Optimization," in *2025 IEEE International Conference on Quantum Computing and Engineering*, Albuquerque, NM, USA, 2025, pp. 1015–1020, https://doi.org/10.1109/QCE65121.2025.00113.

[14] A. S. Bhatia, M. K. Saggi, and S. Kais, "Application of quantum-inspired tensor networks to optimize federated learning systems," *Quantum Machine Intelligence*, vol. 7, no. 1, Jan. 2025, Art. no. 12, https://doi.org/10.1007/s42484-025-00243-x.

[15] C. Ren *et al.*, "Toward Quantum Federated Learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 36, no. 9, pp. 15580–15600, Sept. 2025, https://doi.org/10.1109/TNNLS.2025.3552643.

[16] X. Zhang, H. Deng, R. Wu, J. Ren, and Y. Ren, "PQSF: post-quantum secure privacy-preserving federated learning," *Scientific Reports*, vol. 14, no. 1, Oct. 2024, Art. no. 23553, https://doi.org/10.1038/s41598-024-74377-6.

[17] S. Saha, A. Hota, A. K. Chattopadhyay, A. Nag, and S. Nandi, "A multifaceted survey on privacy preservation of federated learning: progress, challenges, and opportunities," *Artificial Intelligence Review*, vol. 57, no. 7, June 2024, Art. no. 184, https://doi.org/10.1007/s10462-024-10766-7.

[18] S. Dutta *et al.*, "Federated Learning with Quantum Computing and Fully Homomorphic Encryption: A Novel Computing Paradigm Shift in Privacy-Preserving ML." arXiv, Oct. 12, 2024, https://doi.org/10.48550/arXiv.2409.11430.

[19] N. Innan, M. A.-Z. Khan, A. Marchisio, M. Shafique, and M. Bennai, "FedQNN: Federated Learning using Quantum Neural Networks," in *2024 International Joint Conference on Neural Networks*, Yokohama, Japan, 2024, pp. 1–9, https://doi.org/10.1109/IJCNN60899.2024.10651123.

[20] M. Chehimi, S. Y.-C. Chen, W. Saad, and S. Yoo, "Federated quantum long short-term memory (FedQLSTM)," *Quantum Machine Intelligence*, vol. 6, no. 2, July 2024, Art. no. 43, https://doi.org/10.1007/s42484-024-00174-z.

[21] E. Sorbera, F. Zanetti, G. Brandi, A. Tomasi, R. Doriguzzi-Corin, and S. Ranise, "Adaptive Federated Learning with Functional Encryption: A Comparison of Classical and Quantum-safe Options." arXiv, July 15, 2025, https://doi.org/10.48550/arXiv.2504.00563.

[22] Z.-P. Liu *et al.*, "Practical quantum federated learning and its experimental demonstration." arXiv, Jan. 22, 2025, https://doi.org/10.48550/arXiv.2501.12709.

[23] H. Gharavi, J. Granjal, and E. Monteiro, "PQBFL: A Post-Quantum Blockchain-based protocol for Federated Learning," *Computer Networks*, vol. 269, Sept. 2025, Art. no. 111472, https://doi.org/10.1016/j.comnet.2025.111472.