Computer Modeling in Engineering & Sciences

Tech Science Press

https://doi.org/10.32604/cmes.2026.080134

ARTICLE

FedGNN: Federated Graph Neural Networks for Privacy-Preserving Cyber-Resilient Energy Optimization in IoT-Based Smart Grids

Alanoud Al Mazroa[1], Fahad Masood[2], Bakri Hussain Awaji[3], Mohammad Alhefdi[4], Abeer Aljohani[5] and Jawad Ahmad[6,*]

[1]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia
[2]Department of Computer Science, CECOS University of IT and Emerging Sciences, Peshawar, Pakistan
[3]Department of Computer Science, Collage of Computer Science and Information Systems, Najran University, Najran, Saudi Arabia
[4]Computer Engineering Department, King Khalid University, Abha, Saudi Arabia
[5]Department of Computer Science and Informatics, Applied College, Taibah University, Madinah, Saudi Arabia
[6]Cybersecurity Center, Prince Mohammad Bin Fahd University, Alkhobar, Saudi Arabia

*Corresponding Author: Jawad Ahmad. Email: jahmad@pmu.edu.sa

Received: 03 February 2026; Accepted: 21 April 2026; Published: 27 May 2026

ABSTRACT: The rapid integration of Internet of Things (IoT) devices and distributed energy resources into smart grids has improved monitoring, control, and energy efficiency. However, it also exposes the grid to cyberattacks and privacy risks, as increased connectivity and data exchange can significantly disrupt energy management and system stability. Studies focused on centralized cybersecurity mechanisms that lacked scalability and did not emphasize the inherent graph structure of power networks. This study proposes a privacy-preserving and cyber-resilient energy-optimization framework, *FedGNN*, for IoT-enabled smart grids that jointly integrates federated learning, graph neural network-based trust inference, and trust-aware energy dispatch. The framework dynamically learns node-level trust scores from multi-feature measurements, including load, voltage, frequency, renewable generation, and battery storage, and incorporates them into real-time energy optimization. Results demonstrate that the proposed approach improves system resilience up to 12%, mitigates the impact of compromised nodes, and maintains operational reliability, while preserving the privacy of distributed data. A comparative analysis with baseline methods shows the proposed framework's superior performance in energy deviation, resilience, and trust-aware decision-making. The results highlight the potential of integrating AI-driven trust mechanisms with federated learning for secure and efficient energy management in future IoT-enabled smart grids.

KEYWORDS: Cyber security; energy optimization; graph neural networks; IoT; smart grids

1 Introduction

Sensors and edge Internet of Things (IoT) devices play an important role in data collection, processing, and system control [1,2]. The interconnected nature of these devices creates multiple entry points, increasing the risk of significant cybersecurity exposures [3]. Rising energy demand and technological integration have increased the complexity of modern smart grids, necessitating advanced security strategies [4]. Cyberattacks can result in falsified data, measurement tampering, and even system failures [5,6].

Privacy-preserving energy prediction and control have been focused on using various machine learning (ML) techniques. Federated learning (FL) is a recent, innovative ML approach that performs predictive

analysis in a privacy-preserving manner [7,8]. The main focus of FL is on data privacy and decentralized model training [9]. The model is trained by sharing only local model updates, without sharing device data with the central server. ML-based techniques are well-suited to identifying cyberattacks on energy devices, abnormal energy consumption, and malfunctioning devices. Given the nature of interconnected devices in IoT-based smart grids, it is appropriate to use a graph for the representation of devices' spatial relationships [10]. Traditional ML models only handle data in text, image, and Euclidean forms. In an intricate non-Euclidean structure, it is difficult to effectively capture the spatial information. Graphical neural network (GNN) enhances the model's ability using both node features and network structures. This GNN feature is highly recommended for anomaly detection in smart grids [11,12].

Most previous work either fails to integrate trust-aware mechanisms into energy optimization or relies on overly simplistic assumptions about attacks and grid dynamics. This work addresses energy distribution optimization in IoT-based smart grids under cyberattacks using FL and GNN *FedGNN*. The privacy of sensitive operational data has been maintained while addressing the simultaneous challenges of cyber threats and energy efficiency. The node-level trust scores are dynamically learned and incorporated into energy dispatch decisions. The effect of the compromised nodes is mitigated, and the privacy of distributed measurements is preserved. The proposed solution addresses scalability limitations, including single-point failures in large-scale, centralized smart grid networks. The main objectives of the proposed framework are as follows:

- Integrated federated learning and graph neural networks for a privacy-preserved FedGNN framework
- Metigate false data Attacks for a trust-adaptive aggregation mechanism.
- Trust scores and dispatch decisions embedding for cyber resilient energy optimization.

The integration of FL, GNN, and trust-aware optimization into a single framework confirms the novelty of the proposed framework. Multiple features, including load, voltage, frequency, DER generation, and battery storage, have been considered in the system under multi-node cyberattacks. The practical, scalable solution developed in this work significantly enhances the resilience and security of IoT-enabled smart grids. This *jointly coupled problem* differs from the previous study by treating cyber resilience, privacy preservation, and energy optimization rather than as isolated objectives. The malicious IoT nodes are explicitly modeled to evolve cyber-physical attacks that dynamically adapt system-level decisions with energy optimization.

In this article, Section 2 presents the background study and discussion of the previous literature. In Section 3, the methodology has been discussed in the context of the proposed framework. Section 4 presents a detailed analysis and discussion of the experimental results. Conclusion and future work have been presented in Section 5.

2 Literature Review

Smart grid IoT systems require specialized security measures, such as encryption and intrusion detection, to ensure security. Protecting users, reducing risks, and establishing accountability are the key benefits of a comprehensive control structure. The technical and social goals are aligned through the standards and guidelines that serve as balancing layers [13]. Network attacks are addressed by numerous security solutions to improve the system's overall performance. A central feature of network security is identifying and mitigating cyberattacks in IoT environments [14].

Komninos and Bekara surveyed the challenges posed by potential cyber-attacks in IoT-based smart environments [15,16]. The attacks were categorized into high, moderate, and low based on the severity of their adverse effects. Big Data and Machine Learning applications have been studied in IoT-integrated smart grids [17]. A next-generation method, Role-Based Access Control (RBAC), has been explored to limit

unauthorized access and reduce risk [18]. Cross-domain security challenges in interconnected modern grids have been discussed, highlighting key security issues [19].

AI-driven security solutions have transformed into a powerful approach for providing reliable and scalable infrastructure. The resilience of evolving cyber threats has been improved for real-time detection and response [20]. Machine Learning, combined with blockchain, has enabled decentralized, secure threat-identification systems [21]. Security issues in cloud-based applications have grown significantly with the integration of AI and transfer learning. A privacy-preserving energy management model has been presented in a Peer-to-Peer (P2P) environment [22]. A fair energy allocation has been ensured based on the user's described information. The proposed model manages energy using a quorum-based architecture for false data injection attacks. The results reveal that the model performed well under critical conditions.

Blockchain-based privacy-preserving approaches have been discussed for P2P Energy Trading in Smart Grids [23]. Ethereum smart contracts, MetaMask, and Ganache have been used for the model, enabling secure energy. The model achieved a 12.7% decrease in load compared to existing methods. Blockchain-based privacy-preserving has been discussed for a virtual power plant [24]. A power-flow algorithm combined with a security algorithm is used for real-time monitoring. The model demonstrated excellent efficiency with an average loss of 1.9524 W. Data Integrity Attacks (DIAs) have been identified as a means to address the security of the smart grid [25]. Artificial Neural Networks have been used to enhance detection accuracy with 10 hidden neurons. The model achieved a detection rate of up to 99.5%, resulting in a 21% increase in profit.

Several studies have been presented in recent years on energy and privacy preservation in IoT environments [26,27]. A Comparison of the proposed model with various approaches in smart grid environments is presented in Table 1. These studies employ centralized machine learning models with a primary focus on detecting False Data Attack (FDAs). This framework integrates trust-aware mitigation rather than only detecting FDIAs directly into the energy optimization loop. The proposed method operates in a distributed federated learning environment, where raw measurements remain local to IoT devices. The exploitation of spatial correlations is enabled using GNNs between nodes. The framework based on trust scores also dynamically adjusts node contributions during federated aggregation to improve robustness against coordinated FDIAs.

Table 1: Comparison of the proposed model with various approaches in smart grid environments.

Reference	Approach	Key Features	Objectives	Research Gap
[22]	SHA-256 encryption and Shamir's Secret Sharing	Privacy-preserving energy management	Improved grid stress by up to 76.6%	classification of buyers' or sellers' mode managing energy
[23]	Auction-based dynamic pricing mechanism	Secure energy transactions	Reductions in buyer energy bills by 12.7%	Privacy-preserved P2P energy trading
[24]	Transaction and security algorithm	Peer-to-peer (P2P) transactions	Resulted in an average loss of 1.9524W	Energy resource management, security enhancements
[25]	ANNs with IWSOA	Identifying Data Integrity Attacks	Achieved 99.5% detection rate	Decentralized consensus-based energy management

(Continued)

Table 1 (continued)

Reference	Approach	Key Features	Objectives	Research Gap
This work	FedGNN	Privacy-preserving energy optimization	10% decrease in power consumption and upto 20% increase in Resilience	Multi-location energy optimization

Studies include an AI-based framework for energy efficiency, IRS-enhanced low-carbon power Management using Deep Game Theory, federated anomaly detection using Bayesian game reinforcement learning, and IoT-UAV-inspired intelligent and energy-efficient resource management [28,29]. However, these studies present solutions for individual energy and security issues. A secure framework is necessary from an energy perspective for IoT-based smart homes.

3 Methodology

This work presents a threat-aware energy optimization framework for a smart grid environment. The major components of the methodology include IoT-based data collection for cyberattacks, AI-driven resilience modeling, and trust-aware energy optimization, as shown in Fig. 1. Sensors, smart meters, and distributed energy storage units have been utilized to establish a smart grid environment. Local electrical parameters, including load, voltage, and frequency, were continuously measured by each IoT device at a predefined sampling rate for data collection, in accordance with [30] and [31]. The dataset comprises several data types, including load demand, voltage, frequency, DER generation, battery storage, a cyber-attack indicator, a trust score, and a node ID. Each device maintains a local data-sharing-only model for updates. Cyber-resilience was evaluated by introducing false data injection, enabling the model to test robustness under varying attack intensities. Graph Neural Networks (GNNs) and Federated Learning (FL) approaches have been used to enable resilient energy optimization and preserve privacy. IoT devices and interconnections are modeled as a graph in a smart grid topology, where nodes represent devices and edges represent communication links. The system generates trust or resilience scores for each node as GNNs learn spatial and relational dependencies to identify compromised devices. Model performance is assessed using several metrics, including energy efficiency, deviation from optimal dispatch, and resilience against attacks.

3.1 IoT-Enabled Smart Grid Modeling

Let the smart environment is presented as a graph:

$$\mathcal{G} = (\mathcal{N}, \mathcal{E}) \tag{1}$$

where $\mathcal{N} = \{1, 2, \ldots, N\}$ is the set of nodes representing IoT devices and $\mathcal{E}$ is the set of edges representing communication links. Each node i measures electrical parameters at time t:

$$x_i^t = \begin{bmatrix} P_i^t \\ V_i^t \\ f_i^t \end{bmatrix} \in \mathbb{R}^d, \tag{2}$$

where P_i^t is the load, V_i^t is the voltage, and f_i^t is the frequency. The global measurement matrix is:

$$\mathbf{X}^t = [x_1^t, x_2^t, \ldots, x_N^t]^T \in \mathbb{R}^{N \times d}. \tag{3}$$

The net power injection in case of distributed energy resources (DERs) is:

$$P_i^{\text{net},t} = P_i^t - G_i^t, \tag{4}$$

where G_i^t is the generation at node i. The cyber attacks are represented by a binary indicator a_i^t:

$$a_i^t = \begin{cases} 1, & \text{if node } i \text{ is attacked at time } t \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

The observed corrupted measurement is:

$$\tilde{x}_i^t = x_i^t + a_i^t \cdot \delta_i^t, \tag{6}$$

where δ_i^t is the attack perturbation, which can be stochastic:

$$\delta_i^t \sim \mathcal{U}(-\Delta_i, \Delta_i) \quad \text{or} \quad \delta_i^t = \epsilon\, x_i^t, \tag{7}$$

with Δ_i presents maximum perturbation and ϵ as attack intensity. The global attack measurement matrix is:

$$\tilde{\mathbf{X}}^t = [\tilde{x}_1^t, \tilde{x}_2^t, \ldots, \tilde{x}_N^t]^T. \tag{8}$$

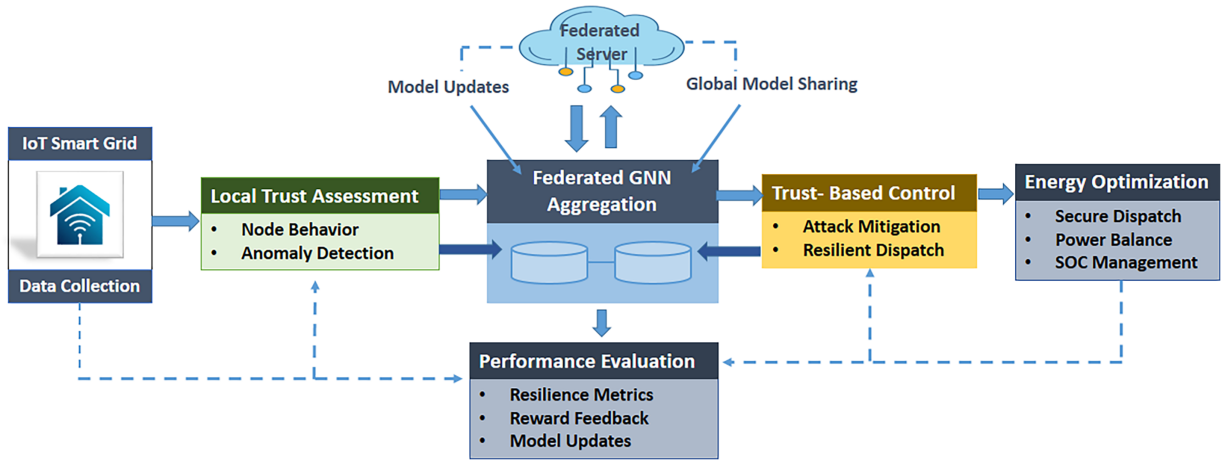

Figure 1: Flow diagram of the proposed FedGNN framework.

3.2 Trust Scoring Using GNN and FL

The proposed AI-based framework integrates Graph Neural Networks (GNNs) for estimating node trustworthiness and modeling spatial correlations, and Federated Learning (FL) for privacy-preserving model training. Each IoT node i collects measurements including load, voltage, frequency, DER generation, and storage:

$$h_i^{(0)} = \tilde{x}_i^t = \begin{bmatrix} P_i^t & V_i^t & f_i^t & G_i^t & E_i^t \end{bmatrix}^T \tag{9}$$

- τ determines the minimum trust level required for a node's model update to significantly influence global aggregation.
- $If\ T_i^{(t)} < \tau$, the node's contribution is down-weighted or excluded.
- τ serves as a resilience control parameter balancing security and availability.

The GNN's input includes node embeddings to capture both electrical parameters and local information.

3.3 GNN Message Passing and Aggregation

At each layer l, node i aggregates information from its neighbors:

$$m_i^{(l)} = \sum_{j \in \mathcal{N}_i} \frac{1}{|\mathcal{N}_i|} h_j^{(l)} \tag{10}$$

Spatial information from connected devices is incorporated to compute the average embedding of neighboring nodes,

$$h_i^{(l+1)} = \sigma\left(W^{(l)} h_i^{(l)} + W_m^{(l)} m_i^{(l)} + b^{(l)} \right) \tag{11}$$

Learnable weights and a nonlinear activation function combine the node's current state with neighbor information. The enhanced neighbor weighting is calculated using the attention mechanism as,

$$\alpha_{ij}^{(l)} = \frac{\exp(\text{LeakyReLU}(a^T [W h_i^{(l)} \| W h_j^{(l)}]))}{\sum_{k \in \mathcal{N}_i} \exp(\text{LeakyReLU}(a^T [W h_i^{(l)} \| W h_k^{(l)}]))} \tag{12}$$

$$h_i^{(l+1)} = \sigma\left(\sum_{j \in \mathcal{N}_i} \alpha_{ij}^{(l)} W h_j^{(l)} \right) \tag{13}$$

The model's resilience is improved by assigning higher weights to more relevant neighbors.

3.4 Node-Level Trust Score

The final embedding is converted to a trust score after L layers,

$$T_i^t = \text{sigmoid}(w_o^T h_i^{(L)} + b_o) \tag{14}$$

The embeddings are mapped to $[0, 1]$ using the sigmoid function to quantify node reliability. High values indicate trustworthy nodes for energy optimization.

3.5 GNN Loss Functions

The prediction accuracy against ground-truth trust labels is measured using the supervised trust loss. It guides the model to correctly identify compromised nodes and is given as,

$$\mathcal{L}_{\text{GNN}} = \frac{1}{|\mathcal{N}|} \sum_{i \in \mathcal{N}} \ell(s_i^t, \hat{s}_i^t) \tag{15}$$

Penalized large trust is differentiated between neighboring nodes using neighbor-smoothness regularization as,

$$\mathcal{L}_{\text{smooth}} = \frac{1}{|\mathcal{E}|} \sum_{(i,j)\in\mathcal{E}} (s_i^t - s_j^t)^2 \tag{16}$$

This ensures spatial consistency and mitigates isolated false positives. The total GNN loss is calculated with combined prediction accuracy and smoothness regularization as,

$$\mathcal{L}_{\text{total}} = \mathcal{L}_{\text{GNN}} + \beta \mathcal{L}_{\text{smooth}} \tag{17}$$

β is the hyperparameter that balances the two objectives.

3.6 FL Formulation

The local model update at node i is given as,

$$\theta_i^{t+1} = \theta_i^t - \eta \nabla_{\theta_i} \mathcal{L}_{\text{total}}^i(\theta_i^t) \tag{18}$$

where each node updates its GNN parameters locally using gradient descent. This preserves privacy since raw measurements are not shared. The central server aggregates local updates weighted by the number of samples. The global aggregation is given as,

$$\theta^{t+1} = \sum_{i=1}^{N} \frac{n_i}{\sum_{j=1}^{N} n_j} \theta_i^{t+1} \tag{19}$$

It produces a global model representing the entire network without sharing raw data. The trust-weighted aggregation assigns a higher weight to nodes with higher trust scores in the global model.

$$\theta^{t+1} = \sum_{i=1}^{N} w_i \theta_i^{t+1}, \quad w_i = \frac{s_i^t n_i}{\sum_{j=1}^{N} s_j^t n_j} \tag{20}$$

This reduces the impact of compromised nodes on the learning process. The addition of Gaussian noise with gradient prevents inference of raw measurements and ensures privacy-preserving model updates. Mathematically,

$$\theta_i^{t+1} = \theta_i^t - \eta\left(\nabla_{\theta_i} \mathcal{L}_{\text{total}}^i + \mathcal{N}(0, \sigma^2 I)\right) \tag{21}$$

The global trust score is further refined to update all nodes' trust scores as,

$$T_i^{t+1} = f_{\text{GNN}}(\theta^{t+1}, \tilde{x}_i^t) \tag{22}$$

3.7 Trust-Aware Energy Optimization

The energy optimization objective is presented as:

$$\min_{P^t} \quad J = \sum_{t=1}^{T} \left[C(P^t) + \lambda \sum_{i=1}^{N} (1 - s_i^t) f(P_i^t) \right], \tag{23}$$

where $C(P^t)$ is operational cost, $f(P_i^t)$ penalizes reliance on untrusted measurements, and λ balances efficiency and resilience. The Power limits

$$P_i^{\min} \le P_i^t \le P_i^{\max}, \quad \forall i, t \tag{24}$$

in terms of power balance, voltage limits, and line flow constraints are given as,

$$\sum_{i=1}^{N} P_i^{\text{net},t} = D^t, \quad \forall t \tag{25}$$

$$V_i^{\min} \le V_i^t \le V_i^{\max}, \quad \forall i, t \tag{26}$$

$$|P_{ij}^t| \le P_{ij}^{\max}, \quad \forall (i,j) \in \mathcal{E}, t \tag{27}$$

Trust-Weighted Dispatch

The trust-weighted optimal dispatch is:

$$P_i^{\text{opt},t} = \arg\min_{P_i^t} \left(C(P_i^t) + \lambda (1 - s_i^t) P_i^t \right) \tag{28}$$

3.8 Performance Metrics

The energy efficiency loss is calculated in terms of performance metrics as,

$$\eta = \frac{C_{\text{attack}} - C_{\text{no-attack}}}{C_{\text{no-attack}}} \times 100\% \tag{29}$$

The average trust score and optimization deviation are calculated as,

$$S_{\text{avg}}^t = \frac{1}{N} \sum_{i=1}^{N} s_i^t \tag{30}$$

$$\Delta P^t = \frac{||P_{\text{baseline}}^t - P_{\text{optimized}}^t||_2}{||P_{\text{baseline}}^t||_2} \tag{31}$$

The resilience under attack intensity α is given as,

$$R(\alpha) = \frac{1}{T} \sum_{t=1}^{T} \sum_{i \in \mathcal{A}_\alpha} s_i^t \tag{32}$$

where $\mathcal{A}_\alpha$ is the set of attacked nodes.

The proposed FedGNN framework leverages three Algorithms 1–3, to collaboratively deliver a trust-aware, energy-efficient solution for the smart grid environment. The computational complexity analysis of the framework involves time and space complexity, as mentioned in Tables 2 and 3.

Algorithm 1: Node-level trust evaluation

Require: IoT node measurements $X_i(t)$, historical observations $H_i(t)$, trust threshold τ
Ensure: Updated trust scores $T_i(t)$

for all IoT nodes $i \in \mathcal{V}$ **do**
  Collect current measurements $X_i(t)$
  Compute deviation from historical pattern:
  $\delta_i(t) = \|X_i(t) - H_i(t)\|$
  Update trust score:
  $T_i(t) = e^{-\beta\delta_i(t)}$
  if $T_i(t) < \tau$ **then**
    Mark node i as suspicious
  else
    Accept node measurements
  end if
end for
return updated trust scores $T_i(t)$

Algorithm 2: Federated graph neural network training

Require: IoT smart grid graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$, local datasets D_i, trust scores T_i
Ensure: Global GNN model parameters θ

Initialize global model parameters θ
Set communication rounds R and local epochs E
for each federated round $r = 1$ to R **do**
  for all IoT nodes $i \in \mathcal{V}$ **in parallel do**
    Receive global model θ
    Train local GNN on dataset D_i for E epochs
    Obtain updated local parameters $\theta_i^{(r)}$
    Send $\theta_i^{(r)}$ to central server
  end for
  Perform trust-weighted aggregation:
  $\theta^{(r+1)} = \sum_{i \in \mathcal{V}} w_i^{(r)} \theta_i^{(r)}$
  where
  $w_i^{(r)} = \frac{T_i}{\sum_j T_j}$
end for
return trained global model θ

Algorithm 3: Trust-aware energy optimization

Require: Predicted load demand $P_i(t)$, DER generation $G_i(t)$, trust scores $T_i(t)$
Ensure: Optimal trust-aware energy dispatch $\hat{P}_i(t)$

for all IoT nodes $i \in \mathcal{V}$ **do**
  Obtain predicted load demand $P_i(t)$
  Retrieve trust score $T_i(t)$
end for

(Continued)

Algorithm 3 (continued)

Solve optimization problem:
$\min \sum_{i \in \mathcal{V}} T_i(t)(P_i(t) - \hat{P}_i(t))^2$
subject to
$\sum_{i \in \mathcal{V}} \hat{P}_i(t) = \sum_{i \in \mathcal{V}} G_i(t)$
$P_i^{min} \leq \hat{P}_i(t) \leq P_i^{max}$
for all nodes $i \in \mathcal{V}$ **do**
  if $T_i(t) < \tau$ **then**
    Reduce influence of node i in dispatch decision
  end if
end for
return trust-aware optimal dispatch $\hat{P}_i(t)$

Table 2: Computational complexity of the proposed algorithms.

Algorithm	Main Operations	Computational Complexity
1	Deviation calculation and trust score update	$\mathcal{O}(NTF)$
2	Local GNN training and federated aggregation	$\mathcal{O}(RNE\|\mathcal{E}\|F)$
3	Trust-weighted optimization and dispatch computation	$\mathcal{O}(N \log N)$

Table 3: Time and space complexity of the proposed algorithms.

Algorithm	Time Complexity	Space Complexity
1	$\mathcal{O}(NTF)$	$\mathcal{O}(NF)$
2	$\mathcal{O}(RNE\|\mathcal{E}\|F)$	$\mathcal{O}(\|\mathcal{E}\|F + NF)$
3	$\mathcal{O}(N \log N)$	$\mathcal{O}(N)$

4 Analysis and Discussion

This section describes the analysis and discussion for the proposed FedGNN framework for secure energy optimization. A complete description of the devices, nodes, and communication setup is provided in the network setup section. The analysis has been done for various performance metrics such as energy efficiency loss η, average trust score S_{avg}, optimization deviation ΔP^t, resilience $R(\alpha)$, and reliability Rel_t to evaluate the effectiveness of the proposed model. The local GNN models are lightweight and can be deployed on edge devices with moderate computational capacity. The model parameters are transmitted only to reduce bandwidth usage. Advanced systems, including Advanced Metering Infrastructure (AMI) and SCADA, can be integrated into the proposed framework without increasing the structural requirements. The distributed microgrids and multi-location energy systems are also supported by the federated design. Training can be performed periodically, and dispatch decisions can be made suitable for real-time control.

4.1 Network and Communication Setup

The smart grid is modeled as a graph $\mathcal{G} = (\mathcal{N}, \mathcal{E})$, where $\mathcal{N}$ denotes the set of IoT nodes, and $\mathcal{E}$ denotes the set of communication links. The network consists of $N = 100$ nodes, including 60 load nodes, 30 DERs (solar and wind), and 10 battery storage nodes. Nodes are connected using a radial, meshed topology to

reflect typical medium-voltage distribution networks. Tables 4 and 5 presents the detailed description of the network and simulation parameters along with the hyperparameter configuration. The GNN used for trust scoring comprises $L = 3$ layers with ReLU activations, and the embedding dimension is set to $d_h = 16$. Federated learning is implemented using a global aggregation interval of 5 time steps, and local learning rate $\eta = 0.01$. Table 6 shows the sensitivity analysis of the proposed FedGNN framework by varying key hyperparameters to evaluate its robustness. The learning rate and clipping ratio exhibited a noticeable mutual influence. The discount factor and GAE parameter were observed to remain stable across a range of values.

Table 4: Network and simulation parameters.

Parameter	Value
Number of nodes (N)	100
Load nodes	60
DER nodes	30
Battery storage nodes	10
Line reactance (X_{ij})	0.1–0.5 pu
Line capacity ($P_{ij}^{\max}$)	50–200 kW
Voltage limits ($V_i^{\min}$, $V_i^{\max}$)	0.95–1.05 pu
Load demand ($P_i^{\min}$, $P_i^{\max}$)	5–50 kW
Battery capacity ($E_i^{\max}$)	50 kWh
Battery charge efficiency (η_{ch})	0.95
Battery discharge efficiency (η_{dis})	0.90

Table 5: Hyperparameter configuration for energy optimization.

Hyperparameter	Symbol	Value
Learning Rate	η	3×10^{-4}
Discount Factor	γ	0.99
GAE Parameter	λ	0.95
Clipping Ratio	ϵ	0.2
Batch Size	B	64
Number of Epochs	K	10
Entropy Coefficient	β	0.01
Value Function Coefficient	c_v	0.5

Table 6: Sensitivity analysis of hyperparameters on system performance.

Hyperparameter	Tested Range	Observed Impact	Stability
Learning Rate (η)	[1e−4, 5e−4]	Faster convergence but unstable for high values	Medium
Discount Factor (γ)	[0.95, 0.99]	Higher long-term reward accumulation	High
GAE (λ)	[0.9, 0.99]	Reduced variance in policy updates	High
Clipping Ratio (ϵ)	[0.1, 0.3]	Controls policy update aggressiveness	Medium

(Continued)

Table 6 (continued)

Hyperparameter	Tested Range	Observed Impact	Stability
Batch Size (B)	[32, 128]	Larger batch improves stability but slower learning	Medium
Entropy Coefficient (β)	[0.001, 0.02]	Encourages exploration but may reduce reward	Low

4.2 Results Analysis

Fig. 2 presents the average trust score over time for various attack intensities α. Results show that the increase in compromised nodes gradually reduces the overall trust level. The trust-aware mechanism can maintain a relatively stable trust score even under higher attack rates. It shows that the proposed model effectively handles malicious behavior in real-time smart-grid environments.

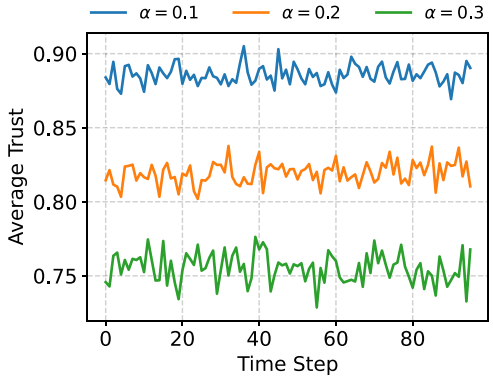

Figure 2: Average trust score over time for various attack intensities.

The energy deviation under various attack scenarios is shown in Fig. 3. The attack severity increases the deviation curve, highlighting the impact of false data. It is evident that the expected and actual energy dispatch differ due to greater attack penetration. It is also notable that adaptive mitigation strategies are necessary in real-time grid operation.

Fig. 4 shows resilience for the trust-aware system over time for varying attack levels. The proposed trust-aware optimization has shown greater resilience even when more nodes are under attack. The Incorporation of trust scores into dispatch decisions is crucial for the system to perform better under adversarial conditions.

The comparison of resilience with and without trust mechanisms is shown in Fig. 5 for the worst-case attack scenario. The proposed trust-aware approach outperforms the no-trust case across all time steps. The system experiences noticeable degradation without trust consideration. The influence of compromised nodes has been mitigated by the trust-enabled framework, thereby improving overall robustness.

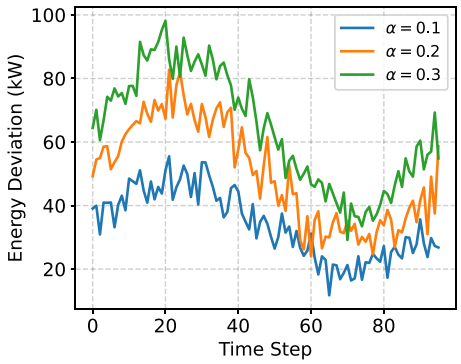

Figure 3: Energy deviation under different levels of attack scenarios.

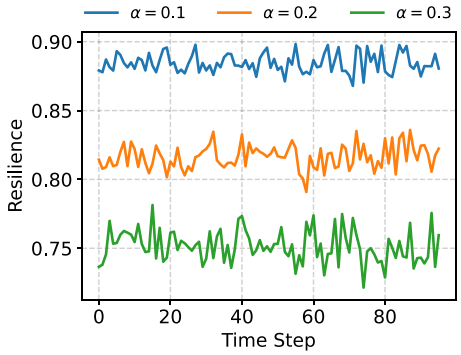

Figure 4: Resilience for the trust-aware over time for varying attack levels.

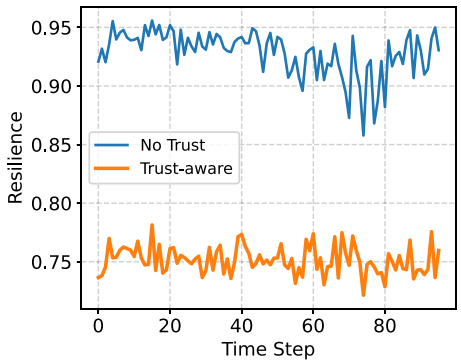

Figure 5: Comparison of resilience with and without trust mechanisms for $\alpha = 0.3$.

A comparative analysis of baseline approaches under severe attack conditions is shown in Fig. 6. The proposed method has been compared with the centralized machine learning method and federated learning without trust. The proposed approach exhibits the highest resilience. The integration of federated learning with trust-aware decision-making has a high impact and is more effective than centralized or trust-agnostic solutions.

Fig. 7a illustrates the trust heatmap across all nodes for different time steps. Lower trust values have been observed in Nodes affected by cyberattacks than in healthy Nodes. It shows that the system dynamically

detects malicious behavior by analyzing the spatial and temporal distributions of trust scores, further supporting the effectiveness of the GNN-based trust inference mechanism.

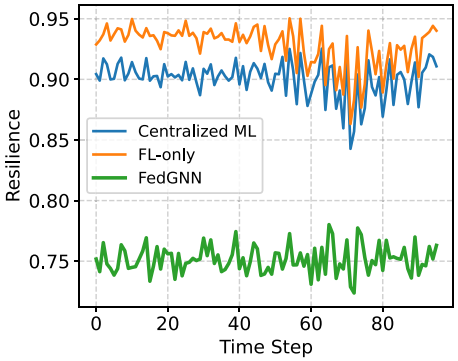

Figure 6: Comparison of the baseline approaches with the proposed framework.

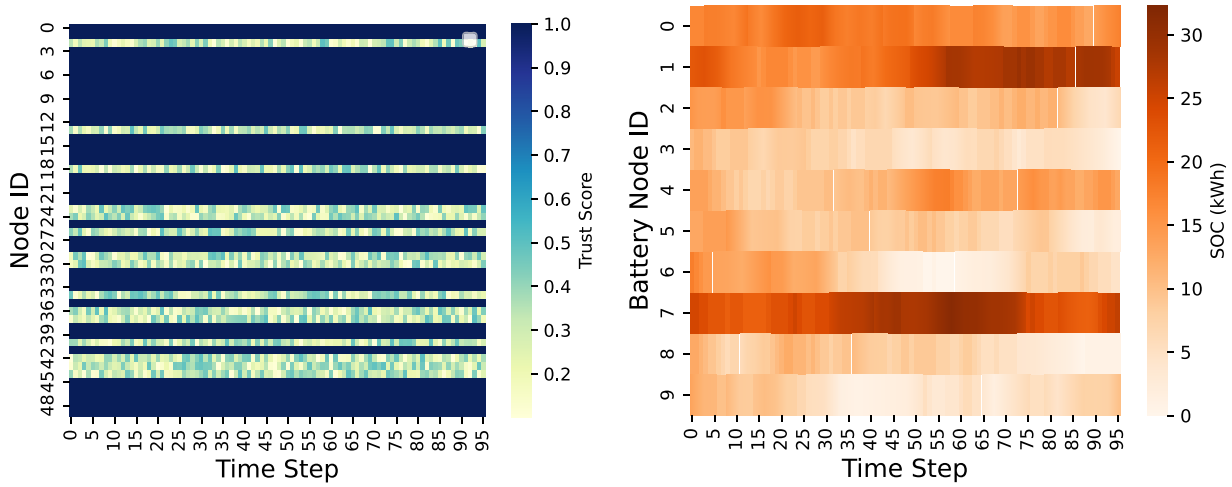

Figure 7: Trust and battery-equipped nodes heatmaps across all nodes for various time steps.

The battery state-of-charge (SOC) heatmap has been shown in Fig. 7b for battery-equipped nodes. The charging and discharging behaviors have been presented in terms of SOC variation under dynamic load and generation conditions. It is notable that battery operations remain stable under attack scenarios, thereby maintaining valuable grid resilience for the energy storage system.

Fig. 8 shows the trust-aware and non-trust optimization for different attack scenarios. The trust-aware strategy consistently yields high resilience value for all attack fractions. The proposed approach adapts effectively to real-time operations across different levels of cyber threats. Results reveal that the proposed approach establishes a closed-loop interaction, in which dynamically inferred trust scores directly influence real-time energy dispatch decisions.

Fig. 9 shows the power utilization of the node-level Load and trust-aware dispatch for various time steps. It is worth mentioning that the proposed FedGNN consumes relatively less power than the original and attacked load. The attack load consumes more power due to the presence of false and malicious nodes. The comparison indicates that the proposed model performs better in a real-time smart grid environment, highlighting its effectiveness and compatibility.

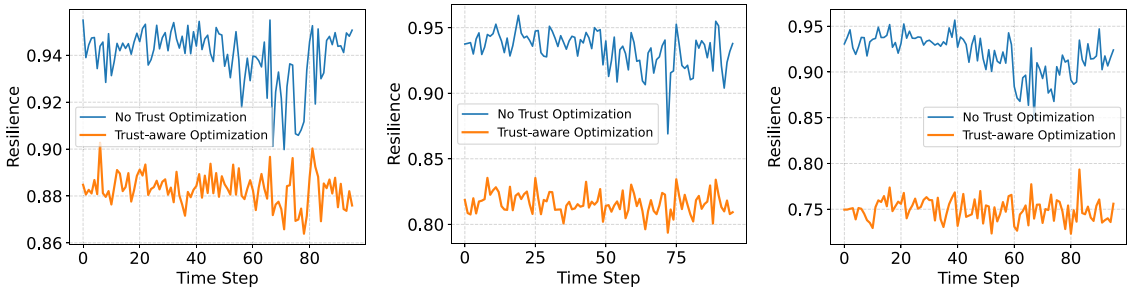

Figure 8: Trust-aware and non-trust optimization for three types of attack level with $\alpha = 0.1$, $\alpha = 0.2$, and $\alpha = 0.3$.

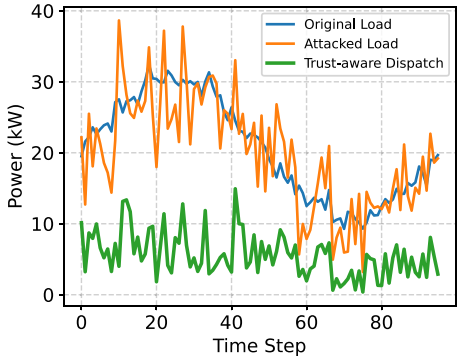

Figure 9: Node-level load and trust-aware dispatch comparisons for various time steps.

The comparison of computational and communication costs is presented in Table 7 for the training rounds. High computational and communication overhead is incurred by centralized learning approaches. The proposed FedGNN framework reduces communication costs and improves scalability. The ablation study has been presented in Table 8 for a severe cyber-attack scenario. Limited resilience improvement has been observed in both the baseline and FL configurations, indicating that learning alone is insufficient for secure real-time operation. Resilience improves with the introduction of static trust, but higher trust variance results from the lack of topology-aware inference. The proposed framework achieves the highest resilience and lowest energy deviation.

Table 7: Computational cost comparison per round or time step.

Method	Computation per Round	Communication Cost	Scalability
Baseline Optimization	$\mathcal{O}(N)$	None	High
Centralized ML	$\mathcal{O}(N \cdot T)$	High (Raw data upload)	Low
Federated Learning (FL)	$\mathcal{O}(N \cdot E)$	Medium (Model updates)	Medium
FL + Static Trust	$\mathcal{O}(N \cdot E)$	Medium	Medium
Centralized GNN	$\mathcal{O}(N^2)$	Very High (Graph data)	Low
Proposed FedGNN	$\mathcal{O}(N \cdot E + \lvert E_g \rvert)$	Low (Encrypted gradients)	High

Table 8: Ablation study of system components under severe cyber attack (α = 0.3).

Method	Avg. Resilience	Energy Deviation (kW)	Trust Variance
Baseline (No AI)	0.81	6.42	–
FL only (No Trust)	0.83	5.98	–
FL + Static Trust (No GNN)	0.87	4.76	0.042
Centralized ML + Trust (No FL)	0.88	4.21	0.031
Proposed (FL + GNN + Trust)	0.93	2.89	0.014

A boxplot-based statistical analysis of system resilience for FedGNN-based and trust-unaware control under different attack rates ($\alpha = 0.1, 0.2, 0.3$) is shown in Fig. 10. The resilience distribution over time for a certain attack intensity is displayed in each pair of boxplots. The median resistance of the no-trust strategy deteriorates and exhibits greater variation as the attack proportion increases, indicating unstable system operation under adversary control. In contrast, the FedGNN-based method consistently produces narrower interquartile intervals and higher median resistance across all attack levels. These findings demonstrate that the suggested strategy not only improves average performance but also enhances robustness and stability against diverse, time-varying cyberattacks.

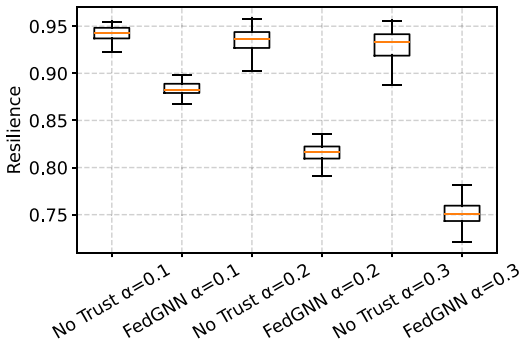

Figure 10: Statistical analysis of system resilience under different attack rates.

The relationship between the system's resilience under high attack intensity (α = 0.3) and the average trust score estimated by the FedGNN model is shown in Fig. 11. Each point represents a time step and captures the dynamic relationship between operational performance and trust assessment. Higher levels of trust are clearly and positively correlated with better resilience outcomes.

The total system demand and the corresponding provided energy under a severe cyberattack scenario (α = 0.3) are shown in Fig. 12. The provided power under no-trust optimization and the suggested FedGNN-based trust-aware control are depicted by the solid curves, whilst the dashed curve shows the overall baseline demand aggregated across all nodes. The provided energy closely matches the attacked demand in the absence of trust mechanisms, suggesting that compromised nodes still affect system-wide dispatch decisions. The FedGNN-based method, on the other hand, deliberately restricts energy distribution to low-trust nodes, thereby reducing the provided power profile.

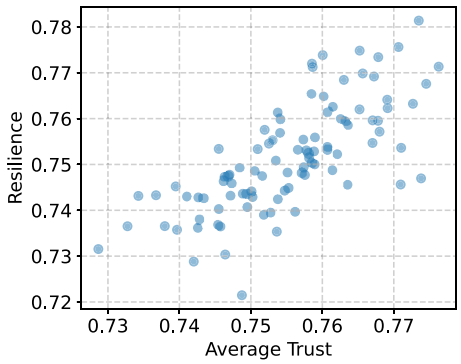

Figure 11: Comparison of system's resilience under high attack intensity ($\alpha = 0.3$) and the average trust score.

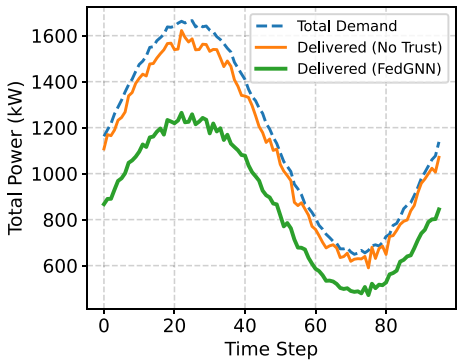

Figure 12: Total system load vs. delivery.

Table 9 presents the impact of the hyperparameters on the learning performance of the proposed FedGNN model. The discount factor determines the relative importance of future rewards, the clipping range governs the stability of policy updates, and the learning rate controls the size of those updates. A moderate learning rate of 3×10^{-4} paired with a large discount factor ($\gamma = 0.99$) yields the highest average resilience and the most consistent convergence behavior. To avoid oscillatory updates and delayed adaptation, a well-designed setup balances learning speed and stability. Reduced resilience and unstable convergence result from higher learning rates and broader clipping ranges, as aggressive updates cause the policy to respond to noisy reward signals during cyberattacks. These findings underscore the importance of fine-tuning PPO hyperparameters to achieve consistent, robust energy management performance under hostile smart grid conditions.

Table 9: FedGNN hyperparameters factor prioritization.

Learning Rate	Discount Factor (γ)	Clip Range	Avg. Resilience	Convergence Stability
1×10^{-4}	0.95	0.20	0.89	High
3×10^{-4}	0.99	0.20	0.93	Very High
5×10^{-4}	0.99	0.30	0.90	Medium
1×10^{-3}	0.95	0.30	0.85	Low

The cyber-resilience of the FedGNN framework is evaluated against trust-related criteria in Table 10. While the trust update rate β regulates how rapidly trust values adjust to observed node activity, the trust threshold establishes the minimal trust score necessary for a node to meaningfully contribute to energy dispatch choices. The findings show that the maximum average resilience, while maintaining a very low false isolation rate, is achieved with an intermediate trust threshold ($\tau = 0.7$) and a moderate update rate ($\beta = 0.1$). System resilience is weakened when the trust threshold is set too low, as malicious nodes are not appropriately penalized. In contrast, overly rigid criteria or rapid trust updates increase the risk of incorrectly isolating benign nodes, thereby degrading overall energy delivery. These results demonstrate the need of adaptive trust modeling in federated smart grid optimization for striking a balance between security and operational effectiveness.

Table 10: FedGNN trust parameters factor prioritization.

Trust Threshold (τ)	Trust Update Rate (β)	Avg. Resilience	False Isolation Rate
0.60	0.05	0.87	Low
0.70	0.10	0.93	Very Low
0.80	0.10	0.91	Medium
0.85	0.15	0.88	High

Table 11 presents a comparative analysis of the baseline methods under coordinated false-data attacks. The performance parameters, including federated, Graph-based, and trust-aware, have been included to evaluate the methods. The centralized GNN offered moderate resilience, was vulnerable to coordinated attacks, and had privacy limitations. FedAvg exhibited improved privacy, limited structural awareness, and instability under high attack ratios. The Trust-Unaware FL-GNN captured the topology but lacked malicious-node mitigation, and its performance degraded as α increased. The combined anomaly detection and dispatch separation offered no integrated optimization with slower mitigation response. The proposed FedGNN outclassed all the baseline methods with the highest resilience, lowest power imbalance, and stability under increasing attack ratios.

Table 11: Comparison with baseline methods under coordinated false data attacks.

Method	Federated	Graph-Based	Trust-Aware	Performance Summary
Centralized GNN	No	Yes	No	Moderate resilience, vulnerable to coordinated attacks, privacy limitations
FedAvg	Yes	No	No	Improved privacy, limited structural awareness, unstable under high attack ratios
Trust-Unaware FL-GNN	Yes	Yes	No	Captures topology, lacks malicious node mitigation, performance degrades as α increases

(Continued)

Table 11 (continued)

Method	Federated	Graph-Based	Trust-Aware	Performance Summary
Anomaly Detection + Dispatch Separation	No	No	Partial	Detection possible, no integrated optimization, slower mitigation response
Proposed FedGNN	Yes	Yes	Yes	Highest resilience, lowest power imbalance, stable under increasing attack ratios

Table 12 shows the generalization capability of the proposed FedGNN framework for various attack types. The proposed framework supported all attack types. The mitigation mechanism clearly provides a brief description of all attack types.

Table 12: Generalization capability of the proposed FedGNN framework.

Attack Type	FedGNN Support	Mitigation Mechanism
False Data Injection Attack	Yes	Trust-weighted aggregation and graph inconsistency detection
Data Replay Attack	Yes	Temporal trust evolution and anomaly deviation tracking
Load Manipulation Attack	Yes	Node-level trust scoring with topology-aware validation
Model Poisoning (Federated)	Yes	Trust-based aggregation filtering
Topology Perturbation Attack	Yes	Graph-structured consistency verification

5 Conclusion

This study presents *FedGNN*, an integrated Federated Learning (FL) and Graph Neural Networks (GNN) framework for IoT-based, cyber-resilient energy optimization in a smart grid environment. A three-layer architecture has been introduced, including IoT devices, AI components, and an optimization phase. IoT devices share model updates using FL and update the aggregation server. FL trains trust inference in a distributed manner to ensure scalability, while GNN captures inter-node dependencies. A trust-weighted representation has been produced, which serves as input to the energy optimization layer. The energy optimization component incorporates a resilience-aware objective function to balance trust scores and energy efficiency. The constraints include device operating limits, network capacity, and load-demand balance. The results clearly demonstrate the system resilience strategy for trust-aware optimization across different attack intensities up to 12%. Future work on *FedGNN* includes multi-location energy optimization with multimodal infrastructure.

Acknowledgement: The authors extend their appreciation to the deanship of research and graduate studies at King Khalid University for funding this work through a large research project under grant number (RGP2/603/45). The

authors thank Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, for supporting this research through the Researchers Supporting Project number (PNURSP2026R510).

Funding Statement: This research work is supported by the Deanship of Research and Graduate Studies, King Khalid University, for funding this work through a large research project under grant number (RGP2/603/45). Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, through the Researchers Supporting Project number (PNURSP2026R510).

Author Contributions: Conceptualization: Alanoud Al Mazroa and Fahad Masood; Methodology: Alanoud Al Mazroa, Bakri Hussain Awaji, Fahad Masood; Software: Bakri Hussain Awaji and Jawad Ahmad; Validation: Mohammad Alhefdi and Abeer Aljohani; Formal analysis: Mohammad Alhefdi, Abeer Aljohani; Investigation; Abeer Aljohani and Jawad Ahmad; Resources: Alanoud Al Mazroa and Jawad Ahmad; Data curation: Fahad Masood and Jawad Ahmad; Writing—original draft preparation: Fahad Masood and Jawad Ahmad; Ceptualization: Alanoud Al Mazroa and Fahad Masood; Methodology: Alanoud Al Mazroa, Bakri Hussain Awaji and Jawad Ahmad; Writing—review and editing: Mohammad Alhefdi and Abeer Aljohani; Visualization, Mohammad Alhefdi and Abeer Aljohani; Supervision: Jawad Ahmad. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: All the data used in this study are mentioned in the article. Additional information may be provided upon request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

List of symbols and abbreviations

$\mathcal{G}(\mathcal{V},\mathcal{E})$	IoT-based smart grid graph
$\mathcal{V}$	Set of nodes (IoT devices)
$\mathcal{E}$	Set of edges (communication links)
N	Number of IoT nodes
$X_i(t)$	Real-time measurement of node i
$H_i(t)$	Historical measurement of node i
$\delta_i(t)$	Measurement deviation of node i
$T_i(t)$	Trust score of node i
τ	Trust threshold
β	Trust sensitivity parameter
D_i	Local dataset at node i
θ	Global model parameters
$\theta_i^{(r)}$	Local model parameters at round r
R	Number of federated learning rounds
E	Number of local training epochs
w_i	Aggregation weight of node i
F	Feature dimension
$P_i(t)$	Power demand at node i
$\hat{P}_i(t)$	Optimized power dispatch
$G_i(t)$	Distributed energy generation
$E_i(t)$	Energy storage (battery state)
η_{ch}, η_{dis}	Charging/discharging efficiency
P_i^{min}, P_i^{max}	Power bounds of node i
α	Attack fraction (ratio of compromised nodes)
$\Delta P_i(t)$	Attack-induced perturbation

FDIA	False Data Injection Attack
FL	Federated Learning
GNN	Graph Neural Network
FedGNN	Proposed Federated GNN framework
DER	Distributed Energy Resources
SOC	State of Charge (battery)

References

1. Masood F, Khan MA, Alshehri MS, Ghaban W, Saeed F, Albarakati HM, et al. AI-based wireless sensor IoT networks for energy-efficient consumer electronics using stochastic optimization. IEEE Trans Consum Electron. 2024;70(4):6855–62. doi:10.1109/TCE.2024.3416035.
2. Qays MO, Ahmad I, Abu-Siada A, Hossain ML, Yasmin F. Key communication technologies, applications, protocols and future guides for IoT-assisted smart grid systems: a review. Energy Rep. 2023;9(2020):2440–52. doi:10.1016/j.egyr.2023.01.085.
3. Asiri F, Malwi WA, Masood F, Alshehri MS, Zhukabayeva T, Shah SA, et al. Privacy preserving federated anomaly detection in IoT edge computing using bayesian game reinforcement learning. Comput Mater Contin. 2025;84(2):3943. doi:10.32604/cmc.2025.066498.
4. Liu M, Teng F, Zhang Z, Ge P, Sun M, Deng R, et al. Enhancing cyber-resiliency of der-based smart grid: a survey. IEEE Trans Smart Grid. 2024;15(5):4998–5030. doi:10.1109/TSG.2024.3373008.
5. Zhang Z, Deng R, Yau DK, Cheng P, Chow MY. Security enhancement of power system state estimation with an effective and low-cost moving target defense. IEEE Trans Syst Man Cybern: Syst. 2022;53(5):3066–81.
6. Zhang Z, Liu M, Sun M, Deng R, Cheng P, Niyato D, et al. Vulnerability of machine learning approaches applied in IoT-based smart grid: a review. IEEE Internet Things J. 2024;11(11):18951–75. doi:10.1109/JIOT.2024.3349381.
7. Gupta H, Agarwal P, Gupta K, Baliarsingh S, Vyas OP, Puliafito A. Fedgrid: a secure framework with federated learning for energy optimization in the smart grid. Energies. 2023;16(24):8097. doi:10.3390/en16248097.
8. Zhang Z, Rath S, Xu J, Xiao T. Federated learning for smart grid: a survey on applications and potential vulnerabilities. ACM Trans Cyber-Phys Syst. 2026;10(1):1–26. doi:10.1145/3760788.
9. Wen J, Zhang Z, Lan Y, Cui Z, Cai J, Zhang W. A survey on federated learning: challenges and applications. Int J Mach Learn Cybern. 2023;14(2):513–35. doi:10.1007/s13042-022-01647-y.
10. Chen T, Zhang X, You M, Zheng G, Lambotharan S. A GNN-based supervised learning framework for resource allocation in wireless IoT networks. IEEE Internet Things J. 2021;9(3):1712–24. doi:10.1109/JIOT.2021.3091551.
11. Qiu J, Zhang X, Wang T, Hou H, Wang S, Yang T. A GNN-based false data detection scheme for smart grids. Algorithms. 2025;18(3):166. doi:10.3390/a18030166.
12. Dzafic D, Džafić I, Akagic A. Anomaly detection in smart grid time-series data using graph deviation networks. Eng Appl Artif Intell. 2026;165(2):113512. doi:10.1016/j.engappai.2025.113512.
13. Abdullahi SM, Lazarova-Molnar S. On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: a comprehensive guide with recent advances. Int J Inf Secur. 2025;24(1):53. doi:10.1007/s10207-024-00951-8.
14. Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. Wirel Netw. 2014;20(8):2481–501. doi:10.1007/s11276-014-0761-7.
15. Komninos N, Philippou E, Pitsillides A. Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun Surv Tutor. 2014;16(4):1933–54. doi:10.1109/COMST.2014.2320093.
16. Bekara C. Security issues and challenges for the IoT-based smart grid. Procedia Comput Sci. 2014;34:532–7. doi:10.1016/j.procs.2014.07.064.
17. Hossain E, Khan I, Un-Noor F, Sikander SS, Sunny MSH. Application of big data and machine learning in smart grid, and associated security concerns: a review. IEEE Access. 2019;7:13960–88. doi:10.1109/ACCESS.2019.2894819.
18. Fragkos G, Johnson J, Tsiropoulou EE. Dynamic role-based access control policy for smart grid applications: an offline deep reinforcement learning approach. IEEE Trans Hum Mach Syst. 2020;52(4):761–73. doi:10.1109/THMS.2022.3163185.

19. Gunduz MZ, Das R. Cyber-security on smart grid: threats and potential solutions. Comput Netw. 2020;169(11):107094. doi:10.1016/j.comnet.2019.107094.
20. Rajaperumal TA, Columbus CC. Transforming the electrical grid: the role of AI in advancing smart, sustainable, and secure energy systems. Energy Inform. 2025;8(1):51. doi:10.1186/s42162-024-00461-w.
21. Mollah MB, Zhao J, Niyato D, Lam KY, Zhang X, Ghias AM, et al. Blockchain for future smart grid: a comprehensive survey. IEEE Internet Things J. 2020;8(1):18–43. doi:10.1109/JIOT.2020.2993601.
22. Amin W, Huang Q, Li J, Khan AA, Subramaniam U, Selvam S. A secure energy management model for Peer-to-Peer smart grids with user-centric constraints. Internet Things. 2025;33(9):101678. doi:10.1016/j.iot.2025.101678.
23. Nazir I, Mushtaq N, Ishfaq H, Amin W, Maaliw RR, Shi X, et al. Blockchain enabled reserved pricing and privacy preserving model for peer-to-peer energy trading in smart grid. IEEE Trans Consum Electron. 2025;71(3):8716–26. doi:10.1109/TCE.2025.3596907.
24. Kaif AD, Alam KS, Das SK, Chen G, Islam S, Muyeen SM. Blockchain-integrated cyber-physical smart meter design and implementation for secured energy trading in virtual power plants. IEEE Trans Autom Sci Eng. 2025;22:15083–93. doi:10.1109/TASE.2025.3566938.
25. Aghajari HA, Niknam T, Sharifhosseini SM, Taabodi MH, Pourbehzadi M. Enhanced resilience in smart grids: a neural network-based detection of data integrity attacks using improved war strategy optimization. Elect Power Syst Res. 2025;239(3):111249. doi:10.1016/j.epsr.2024.111249.
26. Gozuoglu A. IoT-enhanced battery management system for real-time SoC and SoH monitoring using STM32-based programmable electronic load. Internet Things. 2025;30:101509. doi:10.1016/j.iot.2025.101509.
27. Kumar S, Ramaswamy KC, Mathiyalagan SR, Giri J, Kanan M. An efficient battery management system for electric vehicles using IoT & Blockchain. Results Eng. 2025;27(3):106284. doi:10.1016/j.rineng.2025.106284.
28. Masood F, Ahmad J, Al Mazroa A, Alasbali N, Alazeb A, Alshehri MS. Multi IRS-aided low-carbon power management for green communication in 6G smart agriculture using deep game theory. Comput Intell. 2025;41(1):e70022. doi:10.1111/coin.70022.
29. Alasbali N, Masood F, Alnazzawi N, Ghaban W, Alazeb A, Basurra S, et al. IoT-UAV enabled intelligent resource management in low-carbon smart agriculture using federated reinforcement learning. IEEE Trans Consum Electron. 2025;71(2):6933–41. doi:10.1109/TCE.2025.3572552.
30. Arzamasov V. Electrical grid stability simulated data. UCI machine learning repository; 2018 [cited 2026 Mar 20]. Available from: https://doi.org/10.24432/C5PG66
31. Moustafa N. A new distributed architecture for evaluating AI-based security systems at the edge: network TON_IoT datasets. Sustain Cities Soc. 2021;72:102994. doi:10.1016/j.scs.2021.102994.