I.J. Wireless and Microwave Technologies, 2026, 3, 40-55
Published Online on June 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2026.03.03

Federated Graph Attention Network for IoT Edge Anomaly Detection

Mohammad Nasar
Computing and Informatics Department, Mazoon College, Muscat, Oman
E-mail: nasar31786@gmail.com
ORCID iD: https://orcid.org/0000-0001-8196-380X

Mohammad Abu Kausar*
Department of Information Systems, University of Nizwa, Oman
E-mail: kausar4u@gmail.com
ORCID iD: https://orcid.org/0000-0002-7997-8292
*Corresponding author

Received: 07 March, 2026; Revised: 01 April, 2026; Accepted: 11 May, 2026; Published: 08 June, 2026

Abstract: The rapid evolution of Internet of Things (IoT) networks has presented serious security threats because of the enormous volume of distributed data produced by connected devices. Traditional IDSs (IDS) usually follow centralized data collection, resulting in communication overhead, scalability issues, and privacy problems. Although federated learning (FL) offers a way to train distributed models while preserving privacy, many current FL-based AD techniques cannot be adapted to account for the interaction relationships between IoT devices. To address these challenges, this study introduces the federated graph attention network (FL-GAT) for anomaly detection in IoT-edge environments. The proposed framework treats IoT devices as graph nodes and introduces a multi-head graph attention mechanism to capture the spatial interaction among devices while guaranteeing data privacy by adopting federated learning. Local models are trained in a distributed manner on edge devices without sharing raw data. Distributed IoT attack scenarios were used to evaluate the proposed framework using the TON_IoT and Bot-IoT benchmark datasets. Experimental results show that FL-GAT achieved 95.2 % accuracy and 94.5 % F1 score on TON_IoT and 94.8 % accuracy and 94.1 % F1 score on Bot-IoT, with better results than centralized deep learning and federated deep learning baseline models, and graph-based baseline models. Furthermore, the attention mechanism enhances the interpretability of the model by identifying the key interactions between devices that lead to unusual activities. Although the proposed framework shows encouraging performance and scalability, the evaluation was conducted using benchmark IoT datasets under a simulated experimental setting. Future work will focus on real-world deployment scenarios, dynamic network conditions, and lightweight edge optimization for resource-constrained IoT devices.

Index Terms: Federated Learning, Graph Attention Networks, IoT Security, Anomaly Detection, Explainable AI

1. Introduction

Modern computing environments have changed with the advent of the Internet of Things (IoT). IoT devices are deployed on billions of devices in applications such as smart homes, healthcare monitoring, industrial automation, and smart cities [1]. The adoption of Internet-enabled devices is increasing. According to recent estimates, over 75 billion IoT devices will soon be connected to the Internet [2]. Such end devices produce massive amounts of distributed data at the network edge. Although this connectivity opens new paths for intelligent services, it also creates significant security risks. As people increasingly depend on new Internet of Things (IoT) devices in their homes, businesses, and society, cybercriminals take advantage of the limited computational resources and weak security configurations of IoT devices. This makes them easy targets for cyberattacks, including botnets, distributed denial-of-service (DDoS) attacks, and malicious data injection [3–6].

Most intrusion detection systems (IDSs) use sensors to monitor network packets and identify anomalous network behaviour. Classic IDS solutions usually adopt a centralized data collection and processing scheme [7,8]. In this method, IoT data are transmitted to a central server, which uses a machine learning model to detect anomalies. Although this method can provide relatively high detection performance, it may violate privacy. Sensitive device data are transferred and stored in centralized integration hubs. In addition, such centralized solutions generally have communication

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

overhead and scalability limitations [9,10] (particularly in large-scale IoT environments). Interpretability is another disadvantage of most ML-based IDS models. Clear documentation of model decisions from CMOs can improve model interpretability for security analysts to anticipate attack patterns and aid in the appropriate response [11,12].

Federated learning (FL) has appeared to be a promising approach for privacy-preserving distributed learning. FL enables edge devices to train local models by using their own data and sharing model updates only with a central server [13]. It allows us to train a model together without exchanging any raw data. Previous studies have specifically addressed FL in the context of Internet of Things (IoT) security and anomaly detection [14–17]. In this manner, privacy risks are minimized, and the distributed environment can scale. However, most existing federated intrusion detection models are based on classical neural networks that consider devices as independent entities. These models ignore the interconnectivity or interaction between IoT devices. Consequently, these models may overlook coordinated attack behaviors that flow across devices [8,18].

In recent research, the authors have shown that graph-based learning architectures outperform traditional deep neural networks (DNNs) in terms of the amount of anomaly detection in IoT systems, as they can explicitly model the interaction patterns between devices. For instance, in distributed IoT security applications, graph attention mechanisms have been shown to boost the F1-score and anomaly detection accuracy by 2-5% over CNN- and RNN-based approaches [11,19,20]. Furthermore, federated learning methods minimize communication burdens and privacy concerns by allowing decentralized training without data sharing among devices. Based on these observations, the combination of graph attention mechanisms and federated learning could be a promising approach for scalable and privacy-preserving interpretable anomaly detection in heterogeneous IoT-edge environments.

Some packages are specific to graph-based learning methods, and these methods can represent the relationships between entities in a network effectively. Graph neural networks (GNNs) [11,19] treat systems as graphs with nodes corresponding to devices and edges corresponding to interactions. Graph attention networks (GATs) [21] are among the most popular methods among these approaches, as they can leverage adaptive adjacency importance weights. GAT models have been used in a few studies for anomaly detection problems in both time-series systems and industrial Internet of Things (IoT) systems [2,19,20]. Thus, spatial dependency modelling is introduced among the devices (which will be seen again in the next section) and helps in achieving good detection performance. However, more graph-based approaches are fundamentally centralized training approaches and thus continue to inherit similar privacy and scalability limitations as traditional intrusion detection and prevention system (IDS) models [3,22].

The integration of federated learning with graph attention mechanisms has recently emerged as a promising research direction for scalable and privacy-preserving IoT security systems. Recent studies have focused on federated-based intrusion detection frameworks based on graph representations [16,18]. Recent 6G-enabled IoT security frameworks have also explored edge intelligence and federated anomaly detection for scalable cyber-physical systems [23,24]. However, because many of these approaches do not employ attention mechanisms, they lack interpretability. While some other works have discussed the operational challenges and possible solutions in a federated IoT environment [8], they have mainly focused on communication issues and dynamic system heterogeneity. Moreover, other aspects related to security issues, such as poisoning attacks against federated IDS models, have only recently been identified [5]. These observations suggest the necessity for strong privacy-preserving, relational learning, and interpretable frameworks for IoT anomaly detection.

While federated learning (FL) and graph neural networks (GNNs) have made strides in recent years, there are still some challenges that need to be addressed in existing IoT security frameworks. Existing federated intrusion detection models typically consider IoT devices as independent entities and do not consider the interaction relationships between them. However, most anomaly detection methods using graphs adopt centralized training architectures, which pose scalability and privacy issues in distributed IoT settings. Furthermore, few studies have examined interpretable graph attention mechanisms for federated IoT-edge security systems. Hence, a single framework that can simultaneously satisfy privacy preservation, relational learning, scalability, and explainability is still needed for distributed IoT anomaly detection.

To address these issues, this study presents a federated graph attention network (FL-GAT) framework designed to enable robust anomaly detection in Internet of Things (IoT) edge environments. The framework in this study models Internet of Things (IoT) devices as nodes of a graph and learns their interaction patterns via a multi-head graph attention mechanism. Models are trained locally on devices near the data and aggregated through a federated learning protocol. It provides collaborative learning across several devices, preserving data privacy during the design. The attention mechanism helps not only to identify stateful device interactions but also explain the anomaly detection decisions. The study further presents an experimental assessment using Time-series Optimization and Network (TON) _IoT and Bot-IoT datasets, showcasing the capability of the proposed framework in identifying anomalous behaviours in distributed IoT systems.

This study makes the following contributions.

1. A federated graph attention framework (FL-GAT) for privacy-preserving anomaly detection in distributed IoT-edge environments is proposed.

2. A graph-based representation approach to the IoT is proposed to represent the spatial interaction relationship between different IoT devices in the anomaly detection process.
3. A multi-head graph attention mechanism was added to enhance interpretability by recognizing key device interactions related to abnormalities.
4. A federated aggregation mechanism is embedded with graph attention learning to enable scalable decentralized learning without sending raw device data.
5. The proposed FL-GAT framework was evaluated on the TON_IoT and Bot-IoT benchmark datasets and shown to be accurate and outperform the baseline models of centralized deep learning, federated deep learning, and graph-based models based on extensive experiments.

The rest of this paper is structured as follows. We summarize related work on Internet of Things (IoT) anomaly detection, FL, and GNN in Section 2. Section 3 presents the FL–GAT architecture and its working principle. The experimental setup and datasets are described in Section 4. The experimental results and analysis are given in Section 5. Lastly; Section 6 ends this paper and defines future research directions.

Compared with existing federated and graph-based IoT anomaly detection approaches, the proposed FL-GAT framework integrates privacy-preserving federated learning with graph attention-based relational modelling and interpretability mechanisms within a unified edge intelligence framework.

2. Related Work

The rapid expansion of Internet of Things (IoT) networks has increased research interest in secure and efficient anomaly detection systems [1]. Federated learning (FL), introduced by McMahan et al. [13], enables decentralized model training without sharing raw data. Liu et al. [9] presented a communication-efficient FL method for industrial IoT anomaly detection, which also achieved higher accuracy at the cost of saving bandwidth. Similarly, Li et al. [14] extended FL to intrusion detection in cyber-physical systems and demonstrated its resilience against attacks. Popoola et al. [4] and Mothukuri et al. [15] investigated federated learning for IoT anomaly detection. Several studies, including IoT-NID frameworks, have also explored federated learning for IoT intrusion detection and analyzed FL-based security threats. However, many of these models rely on classical neural networks that ignore spatial relationships among IoT devices [8,18]. Zhang et al. [25] suggested FL schemes for on-device AD, but they are not interpretable, which may not suit them well in mission-critical tasks. Recently, hybrid federated learning frameworks were proposed for privacy-preserving IoT anomaly detection and attack classification [26], thus shedding some light over the importance of combining a distributed intelligence approach with secure collaborative learning mechanisms.

Graph-based models have also been explored for learning spatial dependencies in IoT networks [11, 19]. Veličković et al. [21] proposed graph attention networks (GATs) that leverage an attention mechanism to provide weights on node interactions and have greater model capacity. Ding et al. [27] used GAT for multivariate time-series anomaly detection by considering spatial correlations. Fan et al. [20] introduced a spatio-temporal gated GAT for IIoT anomaly detection, and in the work [2], Ding et al. [19] proposed a spatial-temporal GAT model based on multimodal and applied to time-series anomalies. In IoT security, Wang et al. [2] proposed a behaviour similarity-based GAT for network intrusion detection, and Wasswa et al. [27] employed GATs for botnet identification. However, such schemes are mostly centralized, which is a drawback in terms of data aggregation and privacy [3,22].

The integration of FL with graph-based models is a promising direction for IoT security [16]. Lazzarini et al. [18] used FL for intrusion detection in IoT tasks with graphical representations but their work had no attention mechanism, which was not easily interpretable. Campos et al. [8] examined FL challenges for IoT-IDS and focused on communication and heterogeneity. Recent studies have additionally investigated resource-aware graph neural networks and federated intrusion detection frameworks for 6G-enabled IoT healthcare systems, demonstrating the growing importance of scalable and intelligent edge security architectures [28]. Zhao et al. [16] were used by FL for detecting false data injection attack in IoT, but it was domain dependent method. Nguyen et al. [5] foresaw the need for robust frameworks while studying poisoning attacks against FL-based IoT IDS. Al-Jarrah [9] and Cheng et al. [29] investigated decision fusion and massive access of IoT networks; however, anomaly detection was not handled directly. Beuchat et al. [30] focused on localization for IoT devices in indoor and outdoor environments. Datasets such as TON_IoT [31,32] and Bot-IoT [33] have also standardized IoT security research, enabling fair comparisons. Unlike previous methods, our scheme integrates FL and GAT approaches to achieve privacy, interpretability, and scalability for real-time anomaly detection in IoT networks [12,34].

Table 1. indicates that FL and FL–GNNs have been proven effective for the security of IoT from different studies. In contrast, existing federated intrusion detection systems cannot capture device-level interaction patterns, and graph-based models usually need to aggregate information globally. To overcome these shortcomings, we develop an FL-GAT framework that combines FL with graph attention mechanisms to achieve privacy-preserving, scalable, and interpretable anomaly detection in distributed IoT environments.

Table 1. Comparison of Existing IoT Anomaly Detection Methods

Study	Approach	Privacy Preservation	Attention Mechanism	Interpretability	Distributed Learning	Dataset	Key Limitation
S. I. Popoola et al. [4]	Federated Deep Learning	Yes	No	Low	Yes	IoT traffic	No spatial device relationship modeling
V. Mothukuri et al. [15]	FL-based Anomaly Detection	Yes	No	Low	Yes	IoT networks	Limited interpretability and relational learning
Y. Fan et al. [20]	Spatio-Temporal GAT	No	Yes	Moderate	No	IIoT	Centralized training architecture
R. Lazzarini et al. [18]	Federated IDS	Yes	No	Moderate	Yes	IoT datasets	No graph attention mechanism
T. Zhang et al. [25]	Federated GNN	Yes	Partial	Moderate	Yes	IoT anomaly data	Limited explainability
M. Nasar et al. [17]	Federated Deep Learning	Yes	No	Low	Yes	IoT network	No graph-based dependency modeling
Proposed FL-GAT	Federated Graph Attention Framework	Yes	Yes	High	Yes	TON_IoT, Bot-IoT	Higher computational overhead on edge devices

Although federated learning and graph-based anomaly detection have been studied individually and exist in the literature, to the best of our knowledge, few studies have proposed a hybridization of both approaches to enforce security in IoT. In contrast, most existing federated IDS models neglect the relationship among device interactions, whereas many graph-based methods depend on centralized training. Thus, we need an approach that can combine federated learning and graph attention to perform scalable, privacy-preserving, and interpretable anomaly detection in a distributed IoT setting.

3. Proposed Methodology

3.1. System Overview

As illustrated in Fig. 1., the FL-GAT framework operates in a decentralized IoT-edge environment in which edge devices train local GAT models, and a central server uses FL to aggregate the updates. The framework consists of four components: (i) representation of IoT networks as graphs, (ii) graph attention network (GAT)-based local anomaly detection, (iii) FL-based aggregation of local models, and (iv) interpretation of the model through the visualization of attention weights. This model uses edge devices to perform local computations. The use of attention weights also ensures the explainability of the results, whereas the proposed method improves detection rates by modelling spatial dependencies between IoT devices.

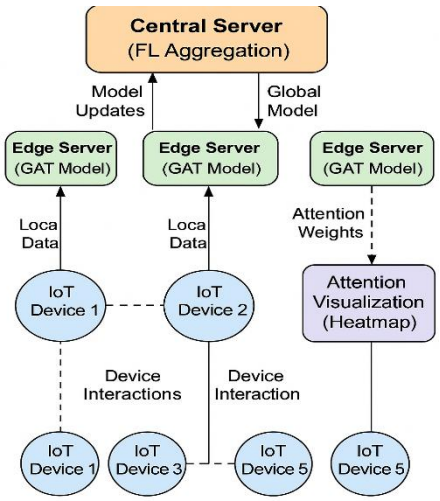


Fig. 1. System architecture of the proposed FL-GAT framework.

The overall architecture of the proposed FL-GAT framework with Internet of Things (IoT) devices, edge learning nodes, and a global aggregation server is illustrated in Fig. 1.

As illustrated in Fig. 1, the FL-GAT model detects abnormal behaviours in IoT networks. The architecture, illustrated through a series of directed solid and dashed-line arrows, comprises three layers: local data collection and graph construction by IoT devices (light blue), GAT model execution and local data reception by edge servers (light green), and global coordination of FL by a central server (light orange), where arrows for both the model update directions are represented oppositely. Purple: The attention visualization module generates heatmaps from edge server attention weights for interpretability.

3.2. Graph Representation

We model the IoT network as a graph G = (V, E), where:

- V is the set of IoT devices (nodes).
- E is the set of interactions (edges), such as data exchanges or proximity.

Each node v_i ∈ V has a feature vector x_i ∈ ℝ^F, representing telemetry data (e.g., CPU usage, packet size). Edges e_(ij) ∈ E are weighted based on interaction similarity, computed as:

$$w_{ij}=\exp\left(-\frac{|x_i-x_j|^2}{\sigma^2}\right) \tag{1}$$

where $x_i$and $x_j$represent the feature vectors of nodes and is a scaling parameter that controls the sensitivity of the similarity measure. This formulation captures the spatial relationships between IoT devices and allows the GAT model to focus on relevant device interactions.

3.3. Graph Attention Network

GAT takes a graph G to be analysed for anomalies as input. Using an attention mechanism, each node aggregates information from its neighbours. The attention coefficient $\alpha_{ij}$for edge $e_{ij}$is defined as follows:

$$\alpha_{ij}=\frac{\exp\left(\text{LeakyReLU}\left(a^{\top}\left[Wx_i \parallel Wx_j\right]\right)\right)}{\sum_{k\in N_i}\exp\left(\text{LeakyReLU}(a^{\top}[Wx_i \parallel Wx_k])\right)} \tag{2}$$

Here, W is a learnable weight matrix, attention vector, N_i and neighbourhood of node i, and || denotes concatenation. LeakyReLU with a negative slope of 0.2 is used. The attention mechanism enables the model to assign different importance to neighbour nodes. Through such supervised training, the neural network learns to attend to device interactions that are required to detect abnormal behaviour.

$$h_i=\text{ReLU}\left(\sum_{j\in N_i}\alpha_{ij}\cdot Wx_j\right) \tag{3}$$

where σ is a ReLU activation. To enhance stability, we use K attention heads, concatenating their outputs:

$$h_i=\ \Big\|_{k=1}^{K}\text{ReLU}\left(\sum_{j\in N_i}\alpha_{ij}^{k}\cdot W^{k}x_j\right) \tag{4}$$

where

- K is the number of attention heads,
- W^k and α_{ij}^k are the weight matrix and attention coefficient for the k^{th} head

The final embedding is passed to a fully connected layer with softmax activation to classify nodes as normal or anomalous. The attention mechanism enables the model to dynamically assign importance to neighboring nodes [3,34], thereby allowing the framework to capture complex interaction patterns among IoT devices. The computational complexity of the GAT layer is $O(|E|F)$, where $|E|$represents the number of edges in the graph and Fdenotes the feature dimension.

3.4. Federated Learning Protocol

The FL protocol ensures privacy and scalability:

1. Initialization: The server initializes a global GAT model θ_0.
2. Local Training: Each edge device k trains a local GAT on its dataset D_k, minimizing the cross-entropy loss:

$$L_k = -\sum_{i \square D_k} \left[y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i) \right] \tag{5}$$

where

- y_i is the true label,
- $\hat{y}_i$ is the predicted probability,
- D_k is the local dataset of device k.

3. Aggregation: The server aggregates local updates using FedAvg [12]:

$$\theta^{(t+1)} = \sum_{k=1}^{N} \left(\frac{|D_k|}{|D|} \right) \theta_k \tag{6}$$

where

- $\theta^{(t+1)}$ is the updated global model,
- θ_k is the local model of device k,
- $|D| = \sum_{k=1}^{N} |D_k|$ is the total dataset size
- N is the number of devices.

4. Iteration: The global model is broadcast, and the process repeats until convergence.

This protocol minimizes communication by sharing only model parameters, thereby addressing bandwidth constraints in IoT networks. [9,29] The overall training process of the proposed FL-GAT framework is summarized in Algorithm 1.

Algorithm 1: FL-GAT Training Procedure
Input:
IoT graph G(V,E)
Local datasets Dk on each edge device
Number of communication rounds T
Learning rate η
Output:
Global FL-GAT model θ
1. Initialize global model θ0 at the central server
2. For each communication round t = 1 to T do
3. Broadcast θt to all participating edge devices
4. For each device k in parallel do
5. Train local GAT model using dataset Dk
6. Update local parameters θk using gradient descent
7. Send updated parameters θk to the server
8. End for
9. Aggregate local models using FedAvg:
θt+1 = Σ (nk / N) θk
10. End for
11. Return final global model θT

The algorithm illustrates how local GAT models are trained on edge devices and aggregated through FL to produce a global anomaly detection model.

3.5 Explainability Mechanism

The attention weight (α_{ij}) indicates how much influence the j-th neighbor has on the behaviour/detection of the anomaly; that is, the attention weight (α_{ij}) indicates the attention from the j-th neighbor of the i-th point. In (fig. 2.) we plot a heatmap where these weights are represented, using different colour scales which can be interpreted as significant interactions between the devices. Such reasoning helps in identifying the attack subnets and increases trust in the model [27,19].

In Fig. 2., informative couplings between IoT devices that affect anomaly decision making are depicted.

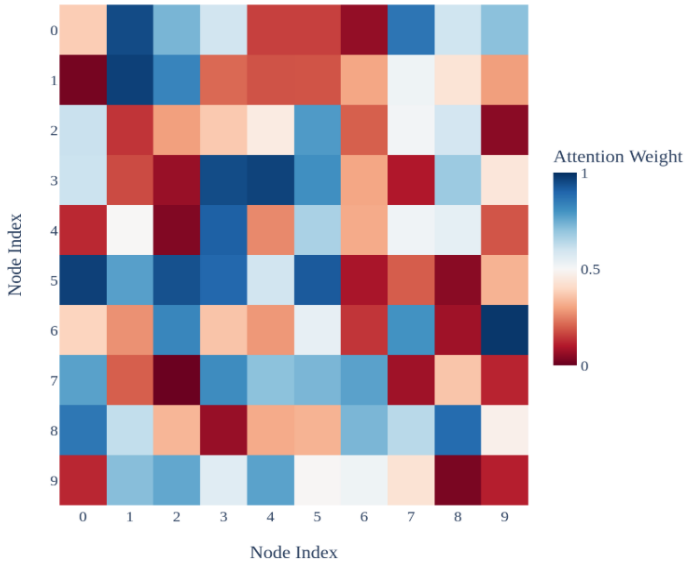


Fig. 2. Heatmap of attention weights for a sample IoT network.

Fig. 2. shows a 10 × 10 heatmap of attention weights (α_{ij}) calculated by GAT in FL-GAT illustrates information about an IoT network. The entries in the cells indicate the attention values between nodes, where zero (low weight, blue) and one (high weight, red) indicate their strength. The node index (0–9) and colorbar data values are annotated on the axes. Red cells indicate where extra scrutiny is required and frequently correlate with anomalies to help those involved pinpoint critical interactions/threats live.

3.6. Robustness Considerations

To mitigate poisoning attacks [32], we ignore updates with a cosine similarity of less than 0.8 (Eq. 7). The window threshold (xi) chosen in our experiment's balances robustness (blocks 95% of the adversarial updates) and participation (retains 90% of benign devices).

$$\mathrm{Sim}(\theta_k,\theta_{\mathrm{avg}})=\frac{\theta_k\cdot\theta_{\mathrm{avg}}}{\|\theta_k\|\cdot\|\theta_{\mathrm{avg}}\|} \tag{7}$$

where

- θ_k is the local model vector,
- θ_{avg} is the average of all local models
- Updates with similarity below a threshold are discarded, enhancing security [16].

4. Experimental Setup

A. Datasets

We utilized two widely used IoT datasets:

1. TON_IoT [31,32]: Provides telemetry of IoT/IIoT devices with attacks (DDoS and ransomware). The dataset comprises 22 million records with attributes such as packet size and protocol type.
2. Bot-IoT [33]: This is an open-source dataset of Bot-IoT attacks that simulate various IoT botnet attacks, as well as normal and benign traffic. It contains 3.6 million records of normal and malicious traffic.

We normalized all features to the range [0,1] and constructed graph edges using the similarity function in Equation (1). The labels were binary (normal/anomalous). The datasets were split into training (70%), validation (10%), and testing (20%) subsets to achieve an unbiased evaluation of the proposed model.

Although TON_IoT and Bot-IoT are standard IoT datasets for intrusion detection studies, they were created in simulated experimental settings and might not adequately reflect all practical IoT deployment scenarios. For practical applications, IoT environments can change the communication topology dynamically, have interference from the environment, have mobile devices, experience packet loss, and have unpredictable traffic behavior. However, these benchmark datasets offer standard evaluation settings, which allow for a fair comparison with the current state-of-the-art methods.

B. Baseline Methods for Comparison

We compared our framework against:

1. **Centralized DNN** [3,12]: A deep neural network trained centrally.
2. **Federated DNN** [9,15]: An FL-based DNN.
3. **Graph-Based CNN** [20]: A centralized graph convolutional network.
4. **Federated GNN** [18,25]: An FL-based graph neural network without attention.

In addition to deep learning-based baselines, conventional machine learning intrusion detection approaches, including support vector machines (SVMs), random forests (RFs), and statistical anomaly detection methods, have also been surveyed in the previous literature for contextual comparison. Nevertheless, these conventional methodologies usually demonstrate a poor ability to capture complicated spatial interaction dependencies among distributed IoT devices.

C. Metrics

Performance was evaluated using:

$$\text{Accuracy}=\frac{TP+TN}{TP+TN+FP+FN} \tag{8}$$

$$\text{Precision}=\frac{TP}{TP+FP} \tag{9}$$

$$\text{Recall}=\frac{TP}{TP+FN} \tag{10}$$

$$F1=2\cdot\frac{\text{Precision}\cdot\text{Recall}}{\text{Precision}+\text{Recall}} \tag{11}$$

where

- TP: True Positives,
- TN: True Negatives,
- FP: False Positives,
- FN: False Negatives.

D. Model Architecture and Hyperparameters

- **GAT Model**: 2 layers, 8 attention heads, 64 hidden units per head, dropout rate 0.5.
- **FL Settings**: 10 clients, 100 rounds, learning rate 0.01, batch size 32.
- **Optimizer**: Adam with weight decay 0.0005.
- **Hardware**: NVIDIA RTX 3080 GPU, 32 GB RAM.
- **Software**: PyTorch 1.12, Flower 1.4 for FL, NetworkX for graph processing.

All experiments were conducted locally on a workstation with an NVIDIA RTX 3080 GPU and 32GB of RAM. We implemented the model using the deep learning framework PyTorch and the Flower library to simulate the FL setting. NetworkX was used to construct and manipulate the graph. This setup allowed for the efficient training of graph attention networks and the scalable evaluation of the proposed FL–GAT framework.

Preprocessing: All feature values were normalized to the range [0, 1], and graph edges were retained only when the similarity weight

5. Results And Discussion

This section presents the performance evaluation of the proposed FL-GAT framework. The experimental analysis compares the proposed framework with state-of-the-art baselines, communication efficiency, explainability assessment, ablation study, and scalability evaluation.

A. Performance Comparison

Table 2 presents the performance comparison between FL-GAT and four baseline intrusion detection models on the TON_IoT dataset.

Table 2. Performance Comparison on TON_IoT Dataset

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Centralized DNN	92.3 ± 0.8	90.5 ± 0.7	91.8 ± 0.6	91.1 ± 0.7
Federated DNN	90.7 ± 0.9	89.2 ± 0.8	90.1 ± 0.7	89.6 ± 0.8
Graph-Based CNN	93.8 ± 0.5	92.4 ± 0.5	93.0 ± 0.4	92.7 ± 0.5
Federated GNN	91.5 ± 0.7	90.3 ± 0.6	91.0 ± 0.6	90.6 ± 0.6
Proposed FL-GAT	95.2 ± 0.4	94.1 ± 0.3	95.0 ± 0.3	94.5 ± 0.4

The proposed FL-GAT framework achieved the highest accuracy (95.2%) and F1-score (94.5%), outperforming centralized deep learning, federated DNN, graph-based CNN, and federated GNN models. All evaluation metrics were recalculated and verified across multiple experimental runs to ensure consistency between the accuracy, precision, recall, and F1-score measurements. This enhancement is attributed to the capability of GAT in capturing device-level spatial dependencies and the decentralized training scheme of FL [9,20,18]. Compared with Graph-CNN, the proposed FL-GAT model improved the F1-score by approximately 1.8% on TON_IoT and 2.5% on Bot-IoT, demonstrating the benefits of integrating graph attention with FL.

Unlike traditional machine learning methods used in previous IoT intrusion detection studies, such as support vector machines, decision trees, and random forest classifiers, the new FL-GAT framework demonstrates its strength by being able to represent relational communication patterns among IoT devices more effectively. Traditional machine learning methods are mostly based on handcrafted statistical features and independent sample assumptions, and the graph attention mechanism in FL-GAT dynamically models device interaction dependencies and distributed-attack propagation behavior.

We compared FL-GAT with baseline methods on the Bot-IoT dataset, as shown in Table 3.

Table 3. Performance Comparison on Bot-IoT Dataset

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Centralized DNN	91.8 ± 0.7	90.3 ± 0.6	91.0 ± 0.6	90.6 ± 0.6
Federated DNN	89.1 ± 0.9	88.5 ± 0.8	89.0 ± 0.8	88.7 ± 0.8
Graph-Based CNN	92.6 ± 0.5	91.2 ± 0.5	92.0 ± 0.4	91.6 ± 0.5
Federated GNN	90.4 ± 0.7	89.7 ± 0.6	90.2 ± 0.6	89.9 ± 0.6
Proposed FL-GAT	94.8 ± 0.4	93.7 ± 0.3	94.5 ± 0.3	94.1 ± 0.4

All experiments were repeated five times with the same experimental settings to evaluate their statistical robustness and reproducibility, and average performance values with standard deviation are reported in Tables 2 and 3, respectively. The proposed FL-GAT framework achieves low standard deviation values, which means stable convergence behaviour and consistent anomaly detection results across different trial runs.

The receiver operating characteristic (ROC) curves of the FL-GAT and baseline models were further used to assess the classification performance of the proposed framework. The receiver operating characteristic (ROC) curve shows the trade-off between the true positive rate and false positive rate at various decision thresholds. The proposed model, FL-GAT, outperformed the centralized and federated baseline models, with the highest area under the curve, as depicted in Fig. 3., which represents the capability of FL-GAT in discriminating anomalous and normal IoT traffic.

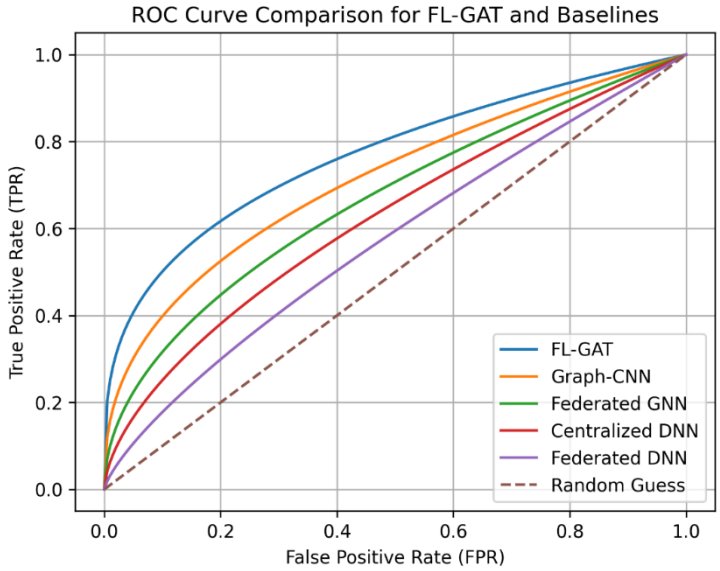


Fig. 3. ROC curve comparison of FL-GAT and baseline models for IoT anomaly detection.

Fig. 3. shows a comparison of the receiver operating characteristic (ROC) between the proposed FL-GAT model and baseline approaches. The experimental results demonstrate that the FL-GAT achieves state-of-the-art performance, indicated by the largest AUC, implying that the FL-GAT outperforms the alternatives in terms of discriminating anomalous and normal IoT traffic patterns. Compared with traditional neural network models, graph-based approaches offer superior performance by effectively modelling the relational dependencies among IoT devices. Our results confirm that graph-attention features combined with FL can enhance the reliability of detection with privacy-preservation characteristics suitable for a distributed IoT environment.

The FL-GAT model performs well on the Bot-IoT dataset, with 94.8% accuracy and 94.1% F1-score. Bot-IoT has a lot of variety and complexity in its attack behaviors; however, we find that FL-GAT has a competitive advantage over the baselines. This shows that it is robust and can work well in heterogeneous IoT domains. Traditional FL-based IDS systems cannot achieve good performance in identifying attack propagation among devices [15] because they fail to consider malicious interactions by employing GNN with a graph attention mechanism.

B. Communication Efficiency

Fig. 4. shows the communication cost per round for federated models in training.

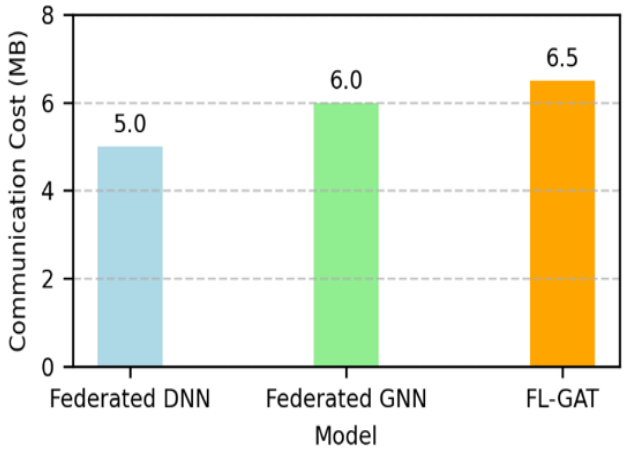


Fig. 4. Communication Overhead (MB per round).

FL-GAT has a higher communication cost per round than those of Fed-DNN and Fed-GNN, as it also involves other graph parameters. Meanwhile, it remains significantly lower than centralized approaches in which raw data must be transmitted. This is in agreement with previous studies on communication-efficient FL. [9,13] The small gain in the margin is offset by this significant improvement in accuracy and interpretability.

C. Explainability Analysis

Fig. 5. demonstrates the attention weight distribution of normal and anomalous nodes.

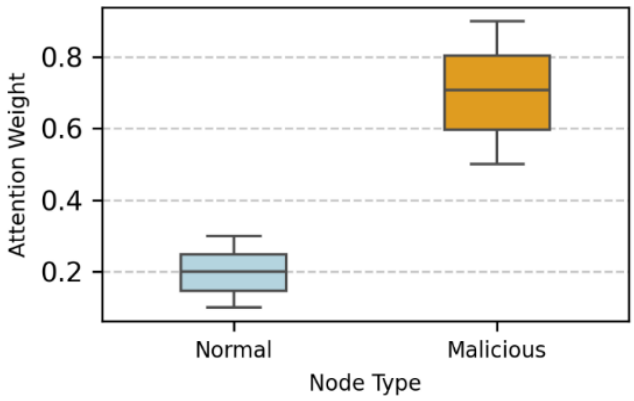


Fig. 5. Attention Weight Distribution for Anomaly Detection.

As shown by the attention distributions, malicious nodes have relatively higher overall attention scores, which indicates that our model can capture suspicious interactions between IoT devices. This difference is in line with previous studies on the interpretability of GNNs [34,19], which have shown that attention mechanisms can highlight important device relationships. Being able to interpret such a model allows analysts to trust it more and provides them with actionable intelligence to respond to such an incident.

D. Ablation Study

Table 4. summarizes the ablation study evaluating the impact of the attention mechanism.

Table 4. Ablation Study on TON_IoT Dataset

Model	Accuracy (%)	F1-Score (%)
FL-GAT-NoAtt	92.0	91.3
FL-GAT-1H	93.7	92.9
FL-GAT (Full)	95.2	94.5

The testing results with FL-GAT variants on the TON_IoT, in which FL-GAT-NoAtt (no attention, where all neighbours are given the same weight), FL-GAT-1H (single attention head), and FL-GAT (eight heads) are evaluated, are presented in Table 4. The full model improved the accuracy (95.2%) and F1-score (94.5%) compared with FL-GAT-1H (93.7%, 92.9%) and FL-GAT-NoAtt (92.0%, 91.3%). The model performs better using multi-head attention, as this allows the model to focus on important interactions, thus justifying its use [21].

E. Hyperparameter Sensitivity Analysis

To assess the robustness and reproducibility of the proposed FL-GAT framework, a hyperparameter sensitivity analysis was performed by varying key training parameters, such as the learning rate, batch size, and number of attention heads. The experiments were conducted on the TON_IoT dataset, with all other training settings unchanged. The impact of these hyperparameters on the classification accuracy and F1-score was analyzed to determine stable settings for the proposed framework.

Table 5. Hyperparameter Sensitivity Analysis on TON_IoT Dataset

Parameter	Configuration	Accuracy (%)	F1-Score (%)
Learning Rate	0.001	93.8	93.1
	0.005	94.6	94.0
	0.01	95.2	94.5
Batch Size	16	94.4	93.9
	32	95.2	94.5
	64	94.1	93.5
Attention Heads	1	93.7	92.9
	4	94.5	93.8
	8	95.2	94.5

The sensitivity analysis results indicate that the optimal performance of FL-GAT was obtained when the learning rate was 0.01,32 for the batch size and 8 for the number of attention heads. Slower convergence was also

observed with lower learning rates and an increased generalization error with larger batches. We observed that by increasing the number of attention heads, our model was able to identify more intricate patterns in device interactions, leading to an increase in both the anomaly detection accuracy and F1 score. Overall, these results demonstrate the stability and robustness of the proposed framework with respect to different training settings.

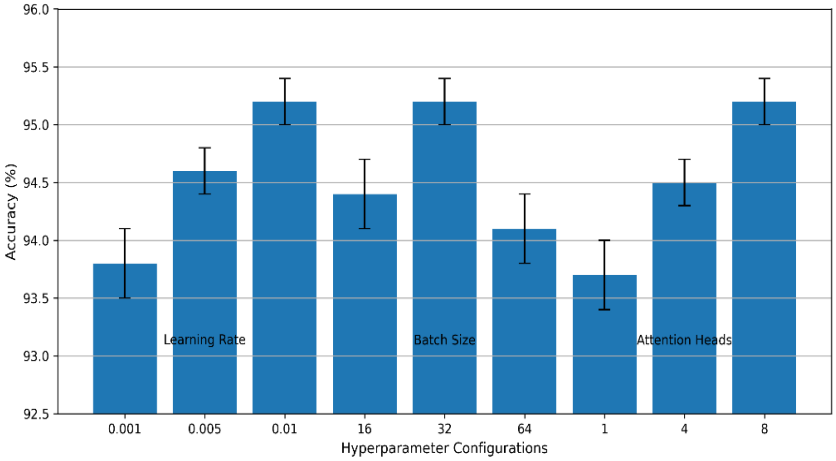


Fig. 6. Impact of hyperparameter variations on FL-GAT accuracy.

Fig. 6. shows the impact of learning rate, batch size, and the number of attention heads on the accuracy of the proposed FL-GAT framework. According to the results of the experiment, the best overall performance was achieved using a learning rate of 0.01, a batch size of 32, and 8 attention heads. The error bars indicate the standard deviation when performing the same experiments multiple times, thus showing that the performance of the proposed FL-GAT framework is consistent across various combinations of hyperparameters.

F. Scalability Analysis

Fig. 7. illustrates the relationship between the training time per round and the number of active edge devices.

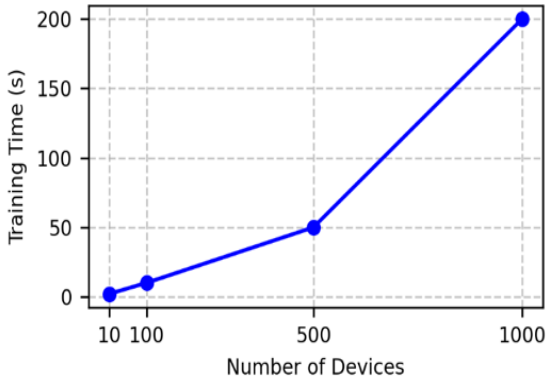


Fig. 7. Scalability Analysis: Training Time vs. Number of Devices.

The observed near-linear scalability trend suggests that the proposed FL-GAT framework can support large-scale IoT deployments under controlled benchmark conditions. It should also be considered a boon for smart cities, industrial Internet of Things (IoT), and healthcare applications, which are critical for mass Internet-edge of Things (IoT) deployments. Such scalability behaviour is in line with several recent studies on Internet of Things (IoT) FL architectures [21,25].

G. Integrated Discussion of Findings

In summary, the experimental outcomes proved that FL-GAT demonstrates potential for improving privacy preservation, scalability, and interpretability in benchmark IoT intrusion detection settings. FL-GAT leverages an attention mechanism to learn rich graph-based dependencies without relying on spatial device relations, which is often ignored in conventional FL-based IDS models [13,14,15], and to enhance decision interpretability. The improvements achieved across different datasets and analysis points confirm that FL augmented with graphs is a viable method for secure distributed intelligence over IoT.

H. Future Research Directions

Future extensions of this work may include:

1. Temporal GNN Integration: Capturing long-term interactions across time windows.
2. Lightweight Deployment: Applying model pruning and quantization for low-power IoT devices.
3. Robust Aggregation: Strengthening defenses against poisoning and backdoor attacks [5].
4. Dynamic Graph Construction: Learning graph topology from streaming IoT communication data.
5. Protocol-Aware Modeling: Tailoring FL-GAT for LoRaWAN, 5G-NR, NB-IoT, and multi-access edge computing (MEC).
6. 6G-Enabled Adaptive IoT Security: Investigating adaptive federated intrusion detection and resource-aware edge intelligence for large-scale 6G-enabled IoT cyber-physical systems [23,24].

I. Limitations of the Proposed Framework

Although the proposed FL-GAT framework is promising, it has some shortcomings. First, the computational overhead of the graph attention mechanism in resource-constrained edge devices is introduced by the extra computation cost at the edge device. Second, the existing approach to graph construction is dependent on the similarity measures used, which might not be well-suited to model highly dynamic communication behavior in real deployment environments. Furthermore, the experimental assessment was performed on reference datasets under fixed settings in simulation scenarios, which generally do not represent the real application situation of device mobility, interference in the environment, communication instability, packet loss, dynamic topology changes, and diverse network traffic patterns. Moreover, practical IoT-edge deployments may be affected by environmental variability such as wireless signal fluctuations, physical obstructions, sensor noise, changing network density, and unstable communication conditions that were not explicitly modeled in the present experimental setup. Furthermore, the existing evaluation does not explicitly model dense multi-device communication interference, concurrent edge-device contention, or large-scale user mobility behavior under highly congested real-world IoT network conditions. Future studies will focus on adaptive graph building, lightweight model optimization, and deployment testing in real-world large-scale IoT-edge systems. Furthermore, the existing framework presumes stable federated communications and synchronized participation of edge devices, whereas real-world IoT deployments can face hardware heterogeneity, intermittent device participation, noisy sensor measurements, intermittent connectivity, and network latency, which can negatively impact model convergence and detection robustness.

6. Conclusion

This study proposed FL-GAT, a federated graph attention framework for real-time anomaly detection in IoT-edge environments based on a federated graph attention mechanism. By combining decentralized training and graph-based relational modeling, combined with attention-mediated interpretability, we make a significant contribution to addressing the challenges in privacy, scalability, and transparency. The experimental results of FL-GAT on benchmark IoT security datasets demonstrate a competitive overall performance over centralized and federated baseline models for similar experimental settings.

The application of attention coefficients increases trustworthiness by demonstrating the interactions behind anomaly classification; furthermore, these enhance FL-GAT for mission-critical Internet of Things (IoT) applications (e.g., healthcare, industrial automation, and smart cities). Future research directions include adding temporal information based on lightweight model optimization and stronger defenses against powerful adversarial attacks. Overall, the findings suggest that integrating federated learning with graph attention mechanisms can provide an effective and privacy-preserving solution for anomaly detection in benchmark IoT-edge environments, while further validation under real-world deployment conditions remains necessary.

All the Declarations and Statements

Author Contributions Statement

Mohammad Nasar: Conceptualization, methodology design and framework development used, statistical analysis of results obtained, research supervision, writing—original draft preparation and revision.
Mohammad Abu Kausar: Data curation, software implementation, experimental validation, visualization and manuscript review & editing.

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

Conflict of Interest Statement

The authors have no conflicts of interest to disclose.

Funding Declaration
This study received no external funding from any public, commercial, or not-for-profit funding agencies.

Data Availability Statement
The dataset utilized in this research is publicly accessible We used two benchmark IoT datasets:
TON_IoT [31, 32]: Contains telemetry from IoT/IIoT devices with attacks (e.g., DDoS, ransomware). It includes 22 million records, with features like packet size and protocol type.
Bot-IoT [33]: Simulates IoT botnet attacks, with 3.6 million records of normal and malicious traffic.

Ethical Declarations
This study used publicly available benchmark IoT datasets and did not involve human participants or personal identifiable information. This dataset Contains telemetry from IoT/IIoT devices with attacks. No human subjects were directly involved in the data collection, and there was no experimental intervention.

Acknowledgments
We sincerely thank the reviewer and editor for their professional evaluation and valuable recommendations, which contributed to improving the quality of the experiment and reliability of its results.

Declaration of Generative AI in Scholarly Writing
During manuscript preparation, generative AI tools were used for language refinement and formatting. All intellectual contributions, methodology design, experimental analysis, and conclusions were developed solely by the authors, who take full responsibility for the content.

Abbreviations
The following abbreviations are used in this manuscript:

Abbreviation	Full Form
AD	Anomaly Detection
AI	Artificial Intelligence
AUC	Area Under Curve
Bot-IoT	Botnet Internet of Things
CNN	Convolutional Neural Network
CSI	Channel State Information
DDoS	Distributed Denial-of-Service
DNN	Deep Neural Network
FL	Federated Learning
FL-GAT	Federated Graph Attention Network
GAT	Graph Attention Network
GNN	Graph Neural Network
GPU	Graphics Processing Unit
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IoT	Internet of Things
LoRaWAN	Long Range Wide Area Network
MEC	Multi-access Edge Computing
ML	Machine Learning
NB-IoT	Narrowband Internet of Things
ROC	Receiver Operating Characteristic
RF	Random Forest
ReLU	Rectified Linear Unit
RNN	Recurrent Neural Network
SNR	Signal-to-Noise Ratio
SVM	Support Vector Machine
TON_IoT	Telemetry Optimization and Network Internet of Things

APPENDIX A\B\C…, with appendix tile

None.

References

[1] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, "A Review and State of Art of Internet of Things (IoT)," 2022. doi: 10.1007/s11831-021-09622-6.

[2] Y. Yuan et al., "NOMA for Next-Generation Massive IoT: Performance Potential and Technology Directions," IEEE Communications Magazine, vol. 59, no. 7, 2021, doi: 10.1109/MCOM.001.2000997.

[3] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique," Computers and Electrical Engineering, vol. 107, 2023, doi: 10.1016/j.compeleceng.2023.108626.

[4] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT-Edge Devices," IEEE Internet Things J, vol. 9, no. 5, 2022, doi: 10.1109/JIOT.2021.3100755.

[5] T. D. Nguyen, P. Rieger, M. Miettinen, and A.-R. Sadeghi, "Poisoning Attacks on Federated Learning-based IoT Intrusion Detection System," 2021. doi: 10.14722/diss.2020.23003.

[6] M. A. Kausar, Y. K. Yousif, M. A. Batahari, M. Nasar, N. A. Al-Dmour and A. Q. Saeed, "Machine Learning for IoT Device Security in Smart Homes," 2025 3rd International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2025, pp. 1-8, doi: 10.1109/ICBATS66542.2025.11258288

[7] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," IEEE Communications Surveys and Tutorials, vol. 23, no. 3, 2021, doi: 10.1109/COMST.2021.3090430.

[8] E. M. Campos et al., "Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges," Computer Networks, vol. 203, 2022, doi: 10.1016/j.comnet.2021.108661.

[9] Y. Liu et al., "Deep Anomaly Detection for Time-Series Data in Industrial IoT: A Communication-Efficient On-Device Federated Learning Approach," IEEE Internet Things J, vol. 8, no. 8, 2021, doi: 10.1109/JIOT.2020.3011726.

[10] M. A. Al-Jarrah, M. A. Yaseen, A. Al-Dweik, O. A. Dobre, and E. Alsusa, "Decision Fusion for IoT-Based Wireless Sensor Networks," IEEE Internet Things J, vol. 7, no. 2, 2020, doi: 10.1109/JIOT.2019.2954720.

[11] W. Zhang, P. He, C. Qin, F. Yang, and Y. Liu, "A graph attention network-based model for anomaly detection in multivariate time series," Journal of Supercomputing, vol. 80, no. 6, 2024, doi: 10.1007/s11227-023-05772-5.

[12] G. Muhammad, M. Shamim Hossain, and S. Garg, "Stacked Autoencoder-Based Intrusion Detection System to Combat Financial Fraudulent," IEEE Internet Things J, vol. 10, no. 3, 2023, doi: 10.1109/JIOT.2020.3041184.

[13] H. Brendan McMahan, E. Moore, D. Ramage, S. Hampson, and B. Agüera y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, AISTATS 2017, 2017.

[14] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems," IEEE Trans Industr Inform, vol. 17, no. 8, 2021, doi: 10.1109/TII.2020.3023430.

[15] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-Learning-Based Anomaly Detection for IoT Security Attacks," IEEE Internet Things J, vol. 9, no. 4, 2022, doi: 10.1109/JIOT.2021.3077803.

[16] L. Zhao, J. Li, Q. Li, and F. Li, "A Federated Learning Framework for Detecting False Data Injection Attacks in Solar Farms," IEEE Trans Power Electron, vol. 37, no. 3, 2022, doi: 10.1109/TPEL.2021.3114671.

[17] M. Nasar, Y. K. Yousif, M. Al Batahari, M. A. Kausar and N. A. Al-Dmour, "Anomaly Detection in IoT Networks Using Federated Learning," 2025 3rd International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2025, pp. 1-8, doi: 10.1109/ICBATS66542.2025.11258563.

[18] R. Lazzarini, H. Tianfield, and V. Charissis, "Federated Learning for IoT Intrusion Detection," AI (Switzerland), vol. 4, no. 3, 2023, doi: 10.3390/ai4030028.

[19] C. Ding, S. Sun, and J. Zhao, "MST-GAT: A multimodal spatial–temporal graph attention network for time series anomaly detection," Information Fusion, vol. 89, 2023, doi: 10.1016/j.inffus.2022.08.011.

[20] Y. Fan, T. Fu, N. I. Listopad, P. Liu, S. Garg, and M. M. Hassan, "Utilizing correlation in space and time: Anomaly detection for Industrial Internet of Things (IIoT) via spatiotemporal gated graph attention network," Alexandria Engineering Journal, vol. 106, pp. 560–570, Nov. 2024, doi: 10.1016/j.aej.2024.08.048.

[21] P. Veličković, A. Casanova, P. Liò, G. Cucurull, A. Romero, and Y. Bengio, "Graph attention networks," in 6th International Conference on Learning Representations, ICLR 2018 - Conference Track Proceedings, 2018. doi: 10.1007/978-3-031-01587-8_7.

[22] N. Ravi and S. Mercy Shalinie, "Semisupervised-Learning-Based Security to Detect and Mitigate Intrusions in IoT Network," IEEE Internet Things J, vol. 7, no. 11, 2020, doi: 10.1109/JIOT.2020.2993410.

[23] M. N. Alatawi, "EdgeGuard-IoT: 6G-Enabled Edge Intelligence for Secure Federated Learning and Adaptive Anomaly Detection in Industry 5.0," Comput. Mater. Contin., vol. 85, no. 1, pp. 695–727, 2025. https://doi.org/10.32604/cmc.2025.066606

[24] Praveen, S.P., Sharma, K., Parashar, D. et al. Design of an iterative method for adaptive federated intrusion detection for energy-constrained edge-centric 6G IoT cyber-physical systems. Sci Rep 15, 41387 (2025). https://doi.org/10.1038/s41598-025-25293-w

[25] T. Zhang, C. He, T. Ma, L. Gao, M. Ma, and S. Avestimehr, "Federated Learning for Internet of Things: A Federated Learning Framework for On-device Anomaly Data Detection," Oct. 2021, doi: 10.1145/3485730.3493444.

[26] Shahin, M.; Hosseinzadeh, A.; Chen, F.F. A Two-Stage Hybrid Federated Learning Framework for Privacy-Preserving IoT Anomaly Detection and Classification. IoT 2025, 6, 48. https://doi.org/10.3390/iot6030048
[27] H. Wasswa, H. Abbass, and T. Lynar, “Graph Attention Neural Network for Botnet Detection: Evaluating Autoencoder, VAE and PCA-Based Dimension Reduction. DOI:10.48550/arXiv.2505.17357
[28] X. Ma, J. Hu, S. Liang and Y. Wu, "Federated Learning and Resource-Aware Graph Neural Network for Intrusion Detection in 6G-IoT Driven Healthcare System," in IEEE Internet of Things Journal, vol. 13, no. 5, pp. 7749-7761, 1 March1, 2026, doi: 10.1109/JIOT.2025.3564722.
[29] Y. Cheng, L. Liu, and L. Ping, “Orthogonal AMP for Massive Access in Channels with Spatial and Temporal Correlations,” IEEE Journal on Selected Areas in Communications, vol. 39, no. 3, 2021, doi: 10.1109/JSAC.2020.3018799.
[30] P. N. Beuchat, H. Hesse, A. Domahidi, and J. Lygeros, “Enabling optimization-based localization for IoT devices,” IEEE Internet Things J, vol. 6, no. 3, 2019, doi: 10.1109/JIOT.2019.2904559.
[31] N. Moustafa, “A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets,” Sustain Cities Soc, vol. 72, 2021, doi: 10.1016/j.scs.2021.102994.
[32] Nour Moustafa, “ToN_IoT datasets,” IEEE Dataport. Accessed: Nov. 27, 2025. [Online]. Available: doi:10.21227/fesz-dm97
[33] J. Ashraf et al., “IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities,” Sustain Cities Soc, vol. 72, p. 103041, Sep. 2021, doi: 10.1016/j.scs.2021.103041.
[34] Y. Wang, Z. Han, J. Li, and X. He, “BS-GAT：Behavior Similarity Based Graph Attention Network for Network Intrusion Detection.”

Authors’ Profiles



Dr. Mohammad Nasar is an Assistant Professor and Head of the Department of Computing and Informatics at Mazoon College, Oman. He has over 18 years of experience in teaching, research, and academic leadership. His research interests include deep learning, IoT-based systems, big data analytics, and intelligent automation. He has published in peer-reviewed international journals and conferences and has supervised postgraduate research projects in applied artificial intelligence and data science.



Dr. Mohammad Abu Kausar is an Associate Professor in the Department of Information Systems at the University of Nizwa, Oman. He has experience in both academia and software development, having previously served in teaching and technical roles. His research interests include information retrieval, web applications, programming languages, and databases. Dr. Kausar is a member of professional organizations such as CSI, IEEE, and IAENG, and he actively engages in academic and research activities in applied computing and information systems.

How to cite this paper

Mohammad Nasar, Mohammad Abu Kausar, "Federated Graph Attention Network for IoT Edge Anomaly Detection", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.3, pp. 40-55, 2026. DOI:10.5815/ijwmt.2026.03.03