International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 August 2026* ***Revised:*** *12 September 2026* ***Accepted:*** *30 October 2026*

Energy-Efficient Adaptive Trust Self-Supervised Federated Graph Contrastive Learning for Intrusion Detection in Resource-Constrained VPN-IoT Networks

S.Sangeetha M.Sc.,M.Phil.,M.Ed.

Research scholar, Department of Computer Science, Navarasam Arts and Science College for Women , Arachalur, Erode-638101

Affiliated to Bharathiar University, Coimbatore, Tamil Nadu, India

Sansen1941@gmail.com

Dr. L.Sudha M.Sc.,M.C.A.,M.Phil.,Ph.D.

Research Supervisor,Associate Professor,

VET Institute ofAtrs and Science College (Co-education), Erode-12

sudhal@vetias.ac.in

Abstract

A VPN-assisted Internet of Things (VPN-IoT) network is prone to different security threats owing to decentralized architectures, inadequate computational resources, and dynamic traffic patterns. The state-of-the-art intrusion detection techniques struggle to attain more detection accuracy while maintaining low energy consumption and preserving privacy. In order to handle these problems, this paper implements an Energy-Efficient Adaptive Trust Self-Supervised Federated Graph Contrastive Learning (EATSFGCL) framework. The proposed EATSFGCL integrates self-supervised contrastive learning and federated learning to discover significant traffic representations from unlabeled data while keeping raw network data on local devices. Graph neural networks are utilized in EATSFGCL to find the relationships among IoT devices and their communication activities where it assists to predict abnormal traffic patterns. An adaptive trust mechanism in EATSFGCL estimates the reliability of each mobile node and their model updates to decrease the influence of untrustworthy or attacked devices during federated training. In addition, an energy-aware optimization strategy in EATSFGCL considers device resource availability and communication costs to support efficient model training and deployment. Thus EATSFGCL improve attack detection performance under heterogeneous network conditions while minimizing energy usage and communication overhead. The effectiveness of EATSFGCL is determined in terms of detection accuracy, computational complexity, packet delivery ratio, energy consumption.

Keywords: Internet of Things (IoT), Federated Learning, Self-Supervised Contrastive Learning, Graph Neural Network, Adaptive Trust, Virtual Private Network.

1. INTRODUCTION

The Internet of Things (IoT) unites dissimilar devices, such as sensors, smart appliances, healthcare equipment, and industrial systems, to broadcast data and give intelligent services. But, the rising number of associated devices has formulated several security problems where IoT devices comprises of inadequate processing power, memory, and battery capacity, creating it complex to implement robust security systems. Virtual Private Networks (VPNs) present secure communication channels, however encryption can limit the visibility of network traffic and formulate intrusion discovery more difficult. As a result, efficient security solutions are desired to recognize malicious activities using available traffic attributes while achieving privacy and optimizing resource utilization.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 August 2026* ***Revised:*** *12 September 2026* ***Accepted:*** *30 October 2026*

The state-of-the-art intrusion detection systems (IDS) rely on predefined rules, attack characteristics, or labelled training data. These IDS may not work well while new attacks appear or network traffic patterns change. Federated learning (FL) facilitates multiple mobile devices to train a shared model without sharing their original traffic information. Self-supervised learning decreases the necessity for labelled samples, while graph neural networks (GNNs) finds associations among IoT devices and their communication activities. Graph contrastive learning can further enhances feature sign through learning similarities among dissimilar views of network data. Several research problems are unsolved in designing precise IDS for resource-constrained VPN-IoT networks. These incorporate predicting abnormal activates in encrypted traffic, finding meaningful patterns from unlabeled network traffic information, handling non-independent and identically distributed (non-IID) client information, and minimizing the power of untrustworthy or compromised users. Moreover, frequent model training and communication may enhance energy usage. The state-of-the-art federated aggregation may not consider trust and resource availability together. Thus, an adaptive framework is required to improve threat identification performance, security, privacy, and energy usage.

In state-of-the-art works, Kushwaha et al. [1] implemented an energy-aware federated learning (EAFL) to minimize the resource and communication requirements during the attack detection process. It enhances energy efficiency and privacy-related problems in IoT security. Though, graph-based traffic relationship modelling, adaptive trust-based client selection, and resilience against malicious participants was remained unaddressed. Nahian et al. [2] developed a bandwidth-aware federated self-supervised learning (BAFSL) to decrease dependence on labelled data. But, energy optimization was not focused. In order to handle the above drawbacks, this research work implements EATSFGCL framework for reliable intrusion identification in VPN-IoT networks.

2. RELATED WORKS

In conventional research work, Hritcan et al. [3] investigated the performance of diverse VPN technologies in IoT network. Though, intrusion identification was not concentrated. Devadhas et al. [4] presented a scalable VPN framework that incorporates machine learning-based intrusion recognition for secure remote communication. But, self-supervised graph representation learning was remained open issue. Khraisat et al. [5] presented a federated learning for boosting security without considering the central collection of raw device data. Though, a device energy limitation in VPN-IoT networks was unsolved.

Puviarasu and Sudha [6] implemented a model for precise and real-time intrusion finding across IoT devices. However, adaptive trust under resource constraints necessitates further analysis. Sinha et al. [7] developed a data-driven intrusion discovery system to find out malicious network behavior in resource-constrained environments. But, a VPN-encrypted traffic was not focused. Manzano et al. [8] investigates distributed data management for security applications. However, trust evaluation and energy-aware node selection was not performed. Razooqi and Pekar [9] review diverse VPN traffic analysis methods in network. Though, intrusion detection across resource-constrained IoT devices was remained open issue.

Pramanik [10] implemented a technique for guarding data during IoT aggregation. Though, it does not give full solution for energy-efficient intrusion discovery. Ajmire et al. [11] implemented a federated contrastive graph transformer framework for scalable threat identification in Industrial IoT application. However, energy usage was more. Kacha et al. [12] performed energy-efficient and privacy-preserving attack identification in edge-based networks. But, adaptive trust mechanism was not applied to minimize the impacts of compromised nodes.

Visuvanathan et al. [13] presented BHFVAL, a blockchain-enabled hierarchical federated variational autoencoder model for securely predicting intrusion in vehicular networks. Though, communication costs, energy requirements, and scalability were remained open issue. Sorour et al. [14] intended an LSTM-JSO framework to noticing dynamic attack patterns in distributed IoT environments. But, finding the graph-based relationships among devices and communication overhead was not solved. Sharma et al. [15] investigated blockchain-based zero-trust networks to assist secure communication across IoT environments. However, the computational and communication costs were very higher.

Elumalai et al. [16] implemented an energy-aware federated intelligence framework for increasing the lifetime of devices with restricted power and computing resources. But, robust intrusion prediction

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 August 2026* ***Revised:*** *12 September 2026* ***Accepted:*** *30 October 2026*

was not achieved in encrypted VPN traffic. Li et al. [17] presented an EfficientNet to enhance the classification performance of diverse attack types. Though, energy-efficient operation was not done on constrained IoT devices. Sharma et al. [18] studied an optimized TabNet model to discover complex patterns in network traffic. However, privacy preservation was not effectual. Borra et al. [19] constructed a hybrid intrusion detection model to predicting the attacks that change over time. But, accuracy of threat identification was not sufficient while increasing number of input devices. In order to overcome the above drawbacks, a novel EATSFGCL Framework is introduced in this paper.

3. PROPOSED EATSFGCL FRAMEWORK

The EATSFGCL Framework is proposed with aiming at enhancing the performance of malicious activities detection in VPN-IoT networks with better energy optimization. The EATSFGCL Framework integrates five key concepts i.e. self-supervised contrastive learning, federated learning, graph neural networks, adaptive trust management, and energy-aware optimization. The EATSFGCL Framework predicts useful traffic patterns from unlabeled network data, guards the privacy of participating nodes, finds relationships among IoT devices, decreases the effect of unreliable clients, and optimizes energy utilization. The architecture diagram of EATSFGCL Framework is presented in Figure 1.

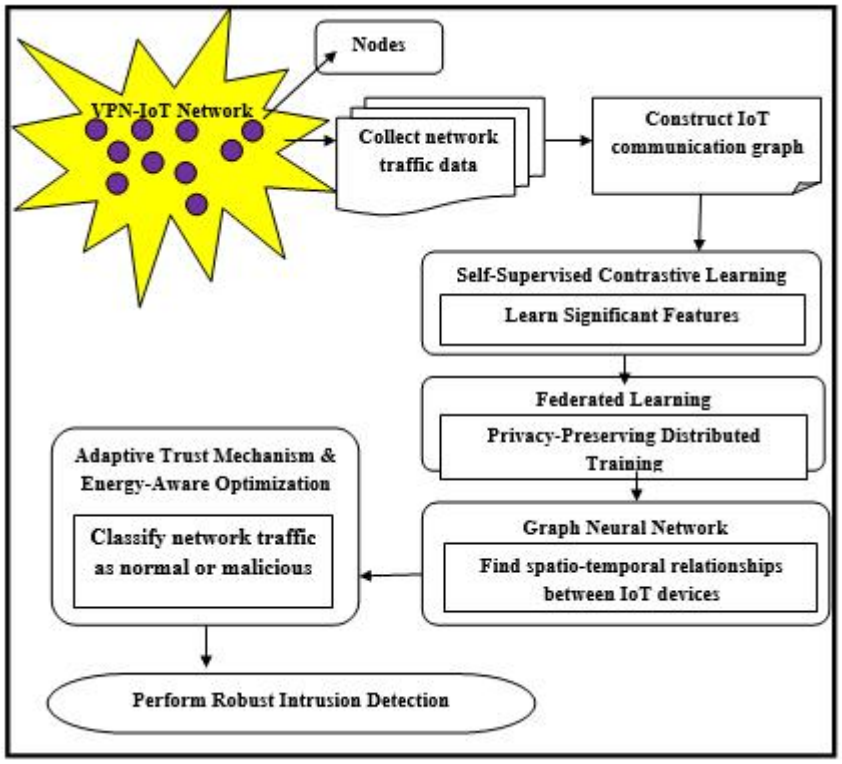

Figure 1 Architecture of EATSFGCL Framework

As demonstrated in Figure 1, initially each IoT node gathers network-flow information i.e. packet size, flow duration, packet direction, and inter-arrival time. Subsequently, EATSFGCL Framework construct the IoT network as a graph in which each node describe a device and each edge point outs a communication relationship. Then, Self-supervised graph contrastive learning in EATSFGCL framework discovers useful traffic representations. During each training round, the EATSFGCL framework determines trust and utility scores for each node to identify reliable node with adequate resources. Finally, the trained model classifies network traffic as normal or malicious with better accuracy.

3.1 Self-Supervised Contrastive Learning

Self-Supervised Contrastive Learning (SSCL) is utilized in proposed EATSFGCL Framework to find out meaningful features from unlabeled network traffic without necessitating predefined labels for all training

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 August 2026* ***Revised:*** *12 September 2026* ***Accepted:*** *30 October 2026*

instances. In EATSFGCL, two dissimilar views of each traffic sample are constructed using suitable data transformations. The SSCL learns to bring the feature representations of associated views closer while separating distinct representations. This process assists to detect the key traffic patterns for distinguishing normal activities from potential attacks. Let x_i describe i^{th}network traffic sample. Two augmented views are constructed through using different transformation functions to the original sample which mathematically represented as,

$$x_i^{(1)} = T_1(x_i) \quad (1)$$

$$x_i^{(2)} = T_2(x_i) \quad (2)$$

In equation (1) and (2), $x_i^{(1)}$, $x_i^{(2)}$ indicates the two augmented views of the original sample x_i whereas $T_1(.)$ and $T_2(.)$ describe the corresponding data transformation functions. The encoder changes these two augmented traffic views into feature representations using following equation,

$$z_i^{(1)} = f_\theta(x_i^{(1)}) \quad (3)$$

$$z_i^{(2)} = f_\theta(x_i^{(2)}) \quad (4)$$

In equation (3) and (4),$z_i^{(1)}$ and $z_i^{(2)}$ point outs the learned feature representations, $f_\theta(.)$ describes the encoder function and θ indicates its trainable parameters. The contrastive loss is measured with the support of Normalized Temperature-scaled Cross-Entropy (NT-Xent) function which obtained mathematically as,

$$\mathcal{L}_{SSCL} = -log\left(\frac{\exp(sim(z_i,z_j)/\tau)}{\sum_{k\neq i}\exp(sim(z_i,z_j)/\tau)}\right) \quad (5)$$

In equation (5), $\mathcal{L}_{SSCL}$ is self-supervised contrastive loss, z_i, z_j signifies the feature embeddings of a positive pair, $sim()$ determines cosine similarity, and τ is the temperature parameter. Reducing this loss encourages the model to find out consistent and informative traffic features from unlabeled data. These learned features are afterward utilized by the intrusion detection classifier.

3.2 Federated Learning

Federated Learning (FL) in allows multiple IoT nodes to train a shared intrusion discovery model without sharing their raw network traffic information to a central server. Each node trains the model using its locally available traffic records and transmits only the updated model parameters to the server. The server integrates these updates to enhance the global model while maintaining the raw traffic data at the client side. Let $w_t$represents the global model parameters at communication round t. The local model update performed by node i is mathematically described as,

$$w_{t+1}^{(i)} = w_t - \eta\nabla\mathcal{L}_i(w_t) \quad (6)$$

In equation (6), w_{t+1}^idefines the updated local model parameters of node i, η point outs the learning rate and $\eta\nabla\mathcal{L}_i(w_t)$ indicates the gradient of local training loss with respect to the model parameters. The server unites the local model parameters with the support of Federated Averaging (FedAvg) method which obtained mathematically as,

$$w_{t+1} = \sum_{i\in S_t}\frac{n_i}{\sum_{j\in S_t} n_j} w_{t+1}^{(i)} \quad (7)$$

In equation (7), S_t indicates the set of participating nodes, $n_i$describes the number of local training samples available at node i, $w_{t+1}^{(i)}$depicts the updated local model parameters and $w_{t+1}^{(i)}$ defines the combined global model parameters. This facilitates collaborative intrusion recognition while keeping raw network traffic data at the local clients.

3.3 Graph Neural Networks

Graph Neural Networks (GNNs) are utilized in EATSFGCL to find out connections among IoT devices depends on their communication behaviors and traffic patterns. In EATSFGCL, each IoT node or communication entity is indicated as a graph node, while the communication links among them formulates graph edges. Traffic attributes, such as packet size, flow duration, and communication frequency are considered to the nodes or edges. To identify changes in communication actions over time, the graph is updated with the help of recent network traffic observations. The IoT network at the time t denoted as a graph using,

$$G_t = (V, E_t, X_t) \quad (8)$$

In equation (8), G_t demonstrates the IoT network graph at time t, V illustrates the collection of IoT nodes, E_t indicates the communication links between devices, and X_t shows the related network traffic features. The GNN updates each node's representation through integrating its own attributes with information from nearest nodes using,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 August 2026* ***Revised:*** *12 September 2026* ***Accepted:*** *30 October 2026*

$$h_v^{(l+1)} = \sigma\left(w_s^{(l)} h_v^{(l)} + \sum_{u \in \mathcal{N}(v)} \alpha_{uv}^{(l)} W_n^{(l)} h^l{}_u\right) \quad (9)$$

In equation (8), $h_v^{(l)}$and $h_v^{(l+1)}$describes the node attributes before and after the update respectively. Here, $\mathcal{N}(v)$ denotes set of nearby nodes of node v whereas $w_s^{(l)}$ and $W_n^{(l)}$ are trainable weight matrices while $\alpha_{uv}^{(l)}$ depicts the significance of nearby node u to node v. The activation function $\sigma(.)$ establishes non-linearity into the learning procedure. This above process supports GNN to predict correlations among IoT devices and discovers useful representations of their communication behavior.

3.4 Adaptive Trust Mechanism

In federated learning, some devices may comprise faulty information, unreliable connections, or compromised devices that present harmful model updates. If all updates are considered equally, these devices may impacts the accuracy and reliability of the global model. Therefore, adaptive trust mechanism is utilized in EATSFGCL to determine the reliability of each participating node depends on its model-update consistency, validation performance, and communication activities. A trust score is considered to each node and updated during consecutive training rounds. A node which includes maximum trust scores gets greater influence during global model aggregation. A low-trust client obtains lesser influence on the global model. The trust score is mathematically estimated using below,

$$T_i^{(t)} = \beta_1 C_i^t + \beta_2 V_i^t + \beta_3 R_i^t \quad (10)$$

In equation (10), $T_i^{(t)}$ depicts the trust score of node i at training round t where C_i^t, V_i^t and R_i^t demonstrates model-update consistency, validation-based reliability, and communication reliability respectively. The weighting coefficients β_1, β_2 and β_3 point out the relative significance of these factors. All reliability parameters are normalized before determining the trust score.

3.5 Energy-Aware Optimization

The energy-aware optimization mechanism is utilized in EATSFGCL enhances resource efficiency through choosing IoT nodes based on their residual energy, available bandwidth, expected contribution to model training, and trust score. This mechanism decreases redundant computation and communication overhead while achieving robust intrusion identification. A utility score is mathematically determined using,

$$U_i^t = \mu_1 \hat{E}_i^t + \mu_2 \hat{B}_i^t + \mu_3 \hat{Q}_i^t + \mu_4 \hat{T}_i^t \quad (11)$$

In equation (11),U_i^t indicates the utility score of node i at training round t. Here, $\hat{E}_i^t$,$\hat{B}_i^t$, $\hat{Q}_i^t$ point outs normalized remaining energy, available bandwidth, and expected training contribution respectively whereas $\hat{T}_i^t$ depicts the node's trust score, while μ_1, μ_2, μ_3 and $\mu_4$are weighting coefficients whose sum equals 1. A higher utility score indicates that a client is more suitable for participating in federated training under the defined selection criteria. The proposed EATSFGCL model selects IoT nodes using the trust score in equation (10) and the utility score in equation (11). Trust evaluation assists to recognize reliable nodes while utility evaluation prioritizes node with adequate energy, available bandwidth, and useful training contributions. The EATSFGCL first verifies whether nodes is trustworthy and contain enough energy, then ranks eligible nodes according to their utility scores and thus chooses the best candidates for training. Thus EATSFGCL enhances resource efficiency while achieving reliable data communication in VPN-IoT network.

The algorithmic process of EATSFGCL is represented as follows,

// Energy-Efficient Adaptive Trust Self-Supervised Federated Graph Contrastive Learning Algorithm

Input: Number of nodes or devices '$v_1, v_2, .. v_N$' in VPN-IoT

Output: Attain robust attack detection with better energy efficiency

Step 1: Begin

Step 2: **For** all the node devices 'v_i'

Step 3: Collect network traffic data

Step 4: Construct the IoT communication graph

Step 5: Apply self-supervised graph contrastive learning to learn traffic representations

Step 6: **For** each training round

Step 7: Train local models on available client data

Step 8: Determine node trust scores using (10)

Step 9: Determine utility scores using (11)

Step 10: Choose the top-k eligible node through ranking

Step 11: Aggregate local model updates using trust-based weights

Step 12: Update and distribute the global model

Step 13: **End For**

Step 14: Classify network traffic as normal or malicious using the trained global model**.**

Step 15: **End For**

Step 16:End

Algorithm 1 Hierarchical Spatio-Temporal Graph Auto-Encoder with Federated Contrastive Learning

By using the above algorithmic process, EATSFGCL framework enhances detection efficiency against heterogeneous and evolving threat while decreasing communication overhead and device energy usage when compared to state-of-the-art works.

4. Experimental setup

The proposed EATSFGCL framework is implemented with the help of NS-2.34 simulator and the IoT-23 dataset. NS-2.34 models IoT network communication whereas IoT-23 gives benign and malicious traffic samples for intrusion recognition. The dataset is preprocessed to mine relevant traffic attributes which are utilized for self-supervised graph representation learning and federated model training. Adaptive trust and energy-aware selection are utilized to find outs reliable clients and get better resource efficiency. The network utilizes an emulated IPsec/OpenVPN tunnel, the Random Waypoint mobility model, and Dynamic Source Routing (DSR). Node speeds varies from 0 to 20 m/s, with CBR traffic over UDP, a packet size of 512 bytes, and a data packet count ranging from 25 to 250. The network adopts IEEE 802.11 MAC, a Two-Ray Ground propagation model, a transmission range of 250 m, and an initial energy of 1000 joules per node. The attack scenarios comprise flooding, unauthorized access, and impersonation, including situations where a compromised node operates inside the VPN. These settings are considered to test intrusion detection performance, network reliability, and energy efficiency under varying traffic and attack condition. The performance of EATSFGCL model is estimated using following parameters,

- Attack Detection Accuracy
- Communication Overhead
- Packet Delivery Ratio
- False Alarm Rate

4.1 Test Case 1: Attack Detection Accuracy

Attack detection accuracy estimates the percentage of network traffic samples that are reliably classified as normal or malicious by the proposed model. It point outs the overall capability of the framework to recognize network activities correctly. Higher accuracy represents better classification performance.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 August 2026* ***Revised:*** *12 September 2026* ***Accepted:*** *30 October 2026*

Table 2 Comparative Performance of Attack Detection Accuracy

Number of Devices	Attack Detection Accuracy (%)		
	EAFL	BAFSL	EATSFGCL
40	87.44	89.12	95.4
80	87.85	89.67	95.53
120	88.06	89.99	95.92
160	88.28	90.49	96.22
200	88.76	90.98	96.67
240	89.09	91.45	96.95
280	89.64	91.78	97.49
320	89.89	92.26	97.89
360	90.13	92.63	98.2
400	91.56	93.12	98.85

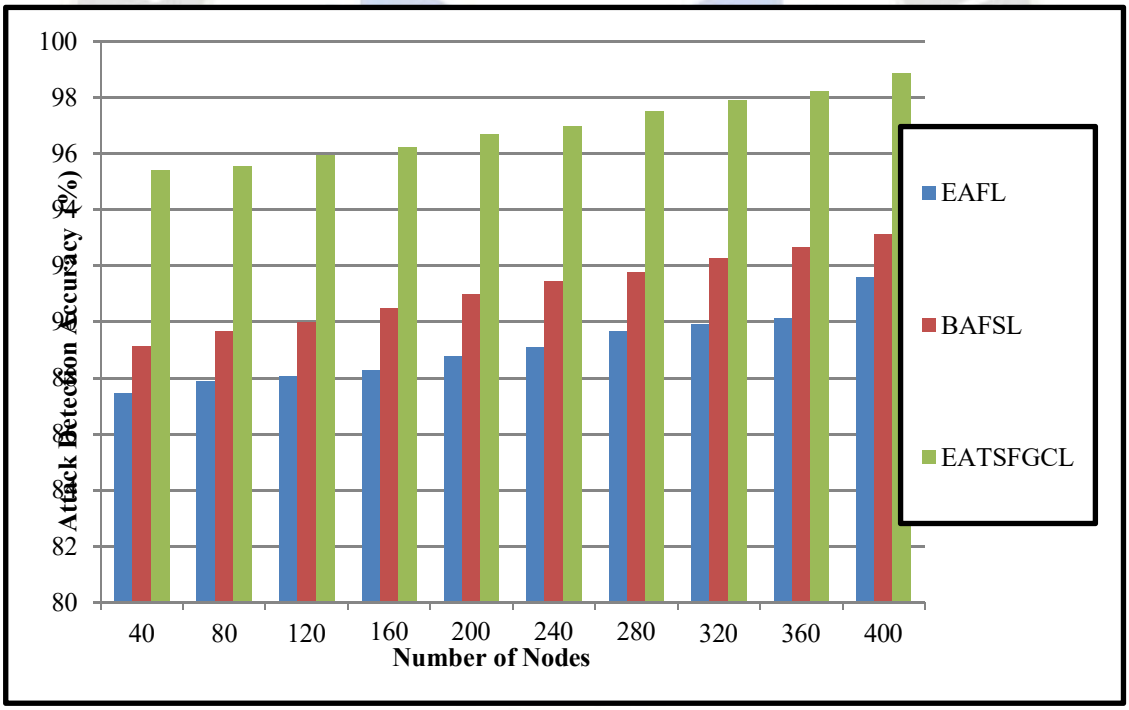

Figure 2 Comparative Graphical Performances for Attack Detection Accuracy

Table 2 and Figure 2 graph demonstrates the attack detection accuracy of EAFL, BAFSL, and the proposed EATSFGCL method as the number of IoT nodes increases from 40 to 400. The results illustrate that detection accuracy increases progressively for all three methods as the network size increases. EAFL attains approximately 87–90% accuracy, while BAFSL records around 89–91%. In comparison, the proposed EATSFGCL method gets the highest accuracy, increasing from approximately 95% to 98%. This enhancement designates that the proposed approach can recognize malicious network activities more efficiently than the two existing methods across the tested node counts. The integration of self-supervised feature learning, graph-based traffic analysis, adaptive trust evaluation, and energy-aware node selection may contribute to this better performance. Overall, the graph

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 August 2026* ***Revised:*** *12 September 2026* ***Accepted:*** *30 October 2026*

proves that EATSFGCL provides more reliable attack detection.

4.2 Test Case 2: Communication Overhead

Communication overhead determines the total amount of time taken to securely communicate the data between IoT nodes. Lower communication overhead designates more reliable use of network bandwidth.

Table 3 Comparative Performance of Communication Overhead

Number of Devices	Communication Overhead (ms)		
	EAFL	BAFSL	EATSFGCL
40	20.2	16.7	10.4
80	22.4	20.6	13.2
120	24.8	22.9	16.1
160	31.9	25.4	18.3
200	35.5	29.8	23.9
240	38.3	35.9	25.7
280	39.7	37.4	28.6
320	44.8	42.6	32.1
360	47.4	45.3	34.6
400	50.6	49.5	37.4

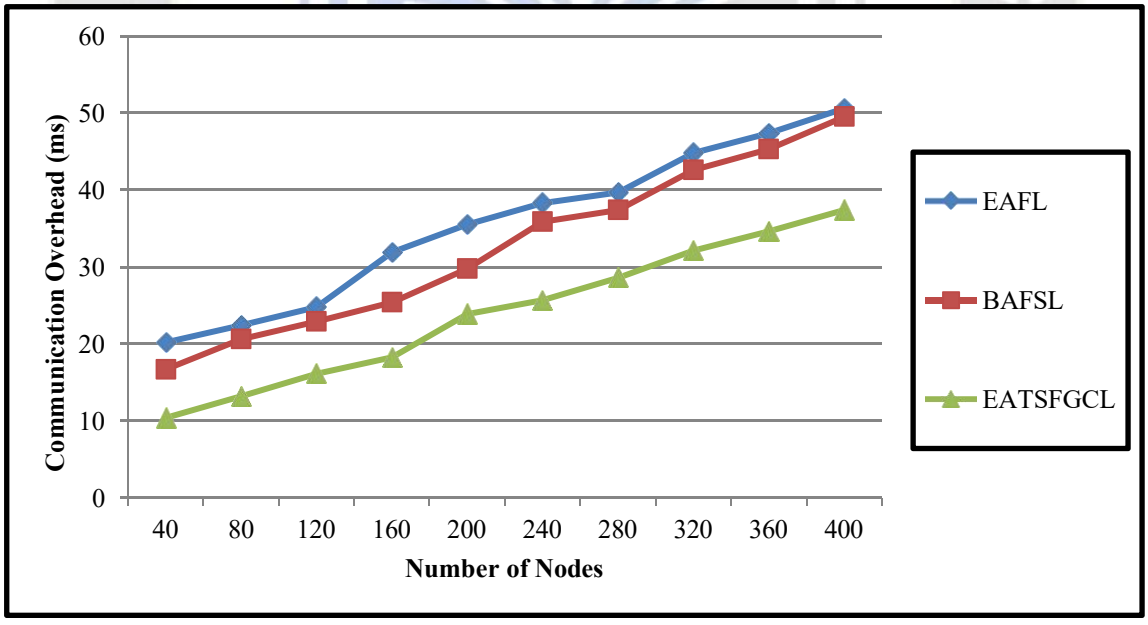

Figure 3 Comparative Graphical Performances for Communication Overhead

Table 3 and Figure 3 depicts the communication overhead results of EAFL, BAFSL, and the proposed EATSFGCL method while the number of IoT nodes raises from 40 to 400. The communication overhead increases for all three methods as the network size grows. EAFL illustrates the highest communication overhead, rising from approximately 20 ms to 50 ms, while BAFSL increases from around 16 ms to 49 ms. On the contrary, the proposed EATSFGCL method achieves lower communication overhead, increasing

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 August 2026* ***Revised:*** *12 September 2026* ***Accepted:*** *30 October 2026*

from approximately 10 ms to 37.5 ms. This reduction suggests that the proposed EATSFGCL manages computational resources more effectively when the number of nodes increases. Its self-supervised feature learning, graph-based processing, and energy-aware node selection may assist to decrease redundant computation during model training. Overall, EATSFGCL demonstrates better communication overhead when compared to existing EAFL and BAFSL.

4.3 Test Case 3: Packet Delivery Ratio

Packet delivery ratio determines the percentage of data packets reliably reached at their destinations compared with the total number of packets forwarded by the source nodes. It point outs the reliability of data communication in the network. A higher PDR reflects better network performance.

Table 4 Comparative Performance of Packet Delivery Ratio

Number of Data Packets	Packet Delivery Ratio (%)		
	EAFL	BAFSL	EATSFGCL
25	88.55	90.23	95.58
50	88.96	90.78	95.92
75	89.15	90.91	96.02
100	89.37	91.57	96.49
125	89.87	91.86	96.89
150	90.18	92.54	97.25
175	90.75	92.85	97.54
200	90.98	93.37	97.92
225	91.24	93.74	98.30
250	92.67	94.35	98.91

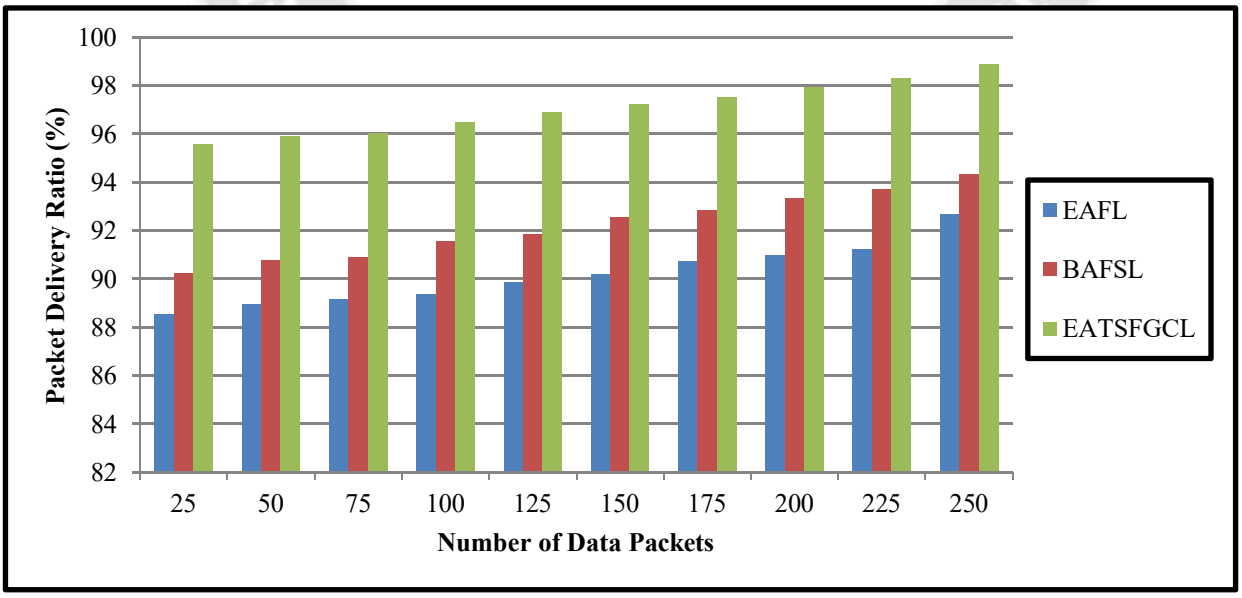

Figure 4 Comparative Graphical Performances for Packet Delivery Ratio

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 August 2026* ***Revised:*** *12 September 2026* ***Accepted:*** *30 October 2026*

Table 4 and Figure 4 describes the packet delivery ratio results of EAFL, BAFSL, and the proposed EATSFGCL method while considering more number of input data packets raises from 25 to 250. The packet delivery ratio increases for all three methods when the network size enlarges. EAFL shows higher packet delivery ratio, rising from approximately 88.55% to 92.67 %, while BAFSL increases packet delivery ratio from around 90.23% to 94.35%. On the contrary, the proposed EATSFGCL method achieves maximum packet delivery ratio, increasing from approximately 95.58 % to 98.91 %. This enhancement indicates that EATSFGCL provides better packet delivery and more reliable communication than the other two methods.

4.4 Test Case 4: False Alarm Rate

False Alarm Rate determines the proportion of normal network traffic samples that are erroneously classified as malicious by the proposed model. A lower false rate represents better detection reliability.

Table 5 Comparative Performance of False Alarm Rate

Number of Devices	False Alarm Rate (%)		
	EAFL	BAFSL	EATSFGCL
40	12.56	10.88	4.6
80	12.15	10.33	4.47
120	11.94	10.01	4.08
160	11.72	9.51	3.78
200	11.24	9.02	3.33
240	10.91	8.55	3.05
280	10.36	8.22	2.51
320	10.11	7.74	2.11
360	9.87	7.37	1.8
400	8.44	6.88	1.15

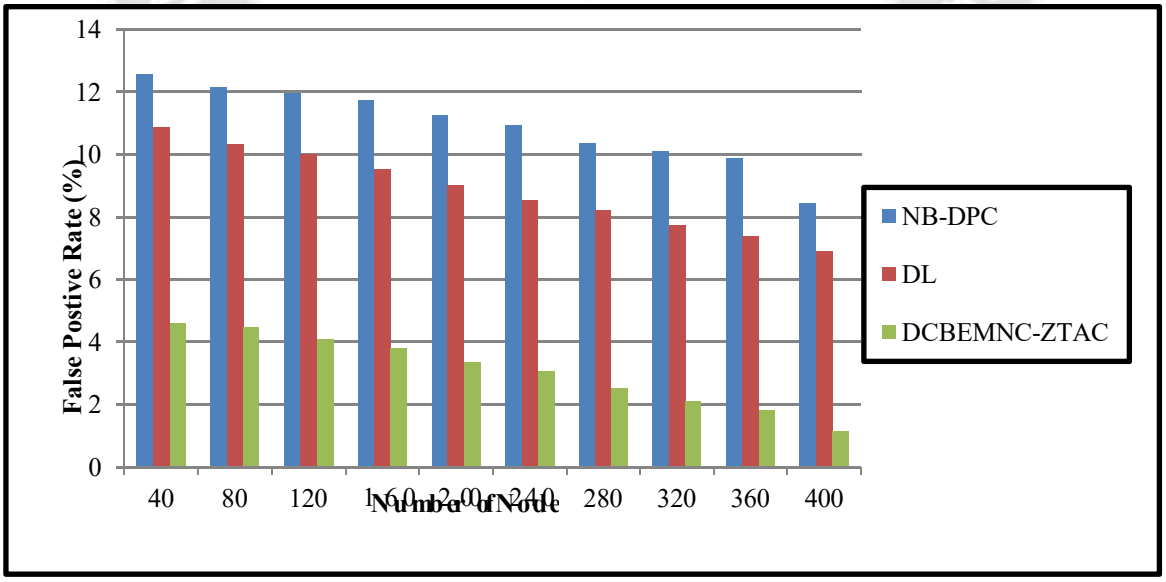

Figure 5 Comparative Graphical Performances for False Alarm Rate

Table 5 and Figure 5 shows the false rate results of EAFL, BAFSL and the proposed EATSFGCL method while considering a large number of input nodes raises from 40 to 400. The false rate of threat identification reduces for all three methods when the network size extends. EAFL illustrates more false rate, rising from approximately 12.56% to 8.44%, while BAFSL attained higher false rate from around 10.88 % to 6.88 %. On the contrary, the proposed EATSFGCL method obtained lesser false alarm rate from approximately 4.6% to 1.15%. This minimized false rate point outs that proposed EATSFGCL provides reliable attack identification performance than the other two methods.

5. CONCLUSION

The proposed EATSFGCL framework presents an effective solution to threat identification in VPN-IoT networks with better resource efficiency. Through integrating self-supervised learning, graph-based feature analysis, federated training, adaptive trust evaluation, and energy-aware node selection, the EATSFGCL enhances attack recognition performance while minimizing computational and communication costs. The observed results show higher detection accuracy and lower computational complexity than EAFL and BAFSL under the evaluated conditions. Overall, proposed EATSFGCL provide a reliable, privacy-preserving, and resource-efficient security solution for VPN-IoT networks.

REFERENCES

[1] Kushwaha, Vipin Kumar, Deepak Kumar Verma, Satya Prakash Yadav, and Himanshu Gupta. "Energy-Aware Federated Learning for IoT Intrusion Detection Using Latent Feature Encoding." *IEEE Access* (2026).

[2] Nahian, Shaikh, Mahfujur Rahman Faraji, Shahadat Molla, Shakh Md Shakib, Md Nazmul Houqe Nayem, Mahammad Mahedi Hassan Ratul, and Fakir Mashuque Alamgir. "BASFL-IDS: Bandwidth-Aware Federated Self-Supervised Learning for IoT Intrusion Detection." In *2026 International Conference on Power, Electronics, Communications, Computing, and Intelligent Infrastructure (PECCII)*, pp. 1-6. IEEE, 2026.

[3] Hritcan, Daniel-Florin, Adrian Graur, Doru-Gabriel Balan, and Edi-Marian Timofte. "A performance analysis of VPN technologies used in an IoT environment." *Advances in Electrical and Computer Engineering* 25, no. 2 (2025): 81-88.

[4] Devadhas, David Neels Ponkumar, S. Arun Kumar, Syed Mahammed Afzal, Mahmad Muskhan, Sangaraju Joshika, and R. Julian Menezes. "Secure Remote Access: A Scalable VPN Framework using Machine Learning-based Intrusion Detection with Random Forest." In *2025 International Conference on NexGen Networks and Cybernetics (IC2NC)*, pp. 21-25. IEEE, 2025.

[5] Khraisat, Ansam, Ammar Alazab, Moutaz Alazab, Areej Obeidat, Sarabjot Singh, and Tony Jan. "Federated learning for intrusion detection in IoT environments: a privacy-preserving strategy." *Discover Internet of Things* 5, no. 1 (2025): 72.

[6] Puviarasu, A., and V. K. Sudha. "Enhanced IoT security: privacy-preserving federated learning model for accurate, real-time intrusion detection across devices." *Ain Shams Engineering Journal* 17, no. 1 (2026): 103866.

[7] Sinha, Priyanshu, Dinesh Sahu, Shiv Prakash, Rajkumar Singh Rathore, Pratibha Dixit, Vivek Kumar Pandey, and Iryna Hunko. "An efficient data driven framework for intrusion detection in wireless sensor networks using deep learning." *Scientific Reports* 15, no. 1 (2025): 34046.

[8] Manzano, Ricardo, Marzia Zaman, Darshana Upadhyay, Nishith Goel, and Srinivas Sampalli. "Federated learning framework based on distributed storage and diffusion model for intrusion detection on IoT networks." *IEEE Access* 13 (2025): 79571-79595.

[9] Razooqi, Yasameen Sajid, and Adrian Pekar. "VPN traffic analysis: A survey on detection and application identification." *IEEE Access* 13 (2025): 132830-132848.

[10] Pramanik, Sabyasachi. "An effective secured privacy-protecting data aggregation method in IoT." In *Achieving Full Realization and Mitigating the Challenges of the Internet of Things*, pp. 186-217. IGI Global Scientific Publishing, 2022.

[11] Ajmire, Sachin Shankarrao, Aniket Sanjayrao Wankhade, Karuna Vivekanand Agarkar, and Shailesh R. Thakare. "Federated Contrastive Graph Transformer Framework for Scalable and Privacy-Preserving Anomaly Detection in

Industrial IoT Networks." In *2025 9th International Conference on Computing, Communication, Control and Automation (ICCCBEA)*, pp. 1-8. IEEE, 2025.

[12] Kacha, Paras, Swati Shinde, Bal Singh Virdee, and Ashish Khanna. "Energy-efficient and privacy-preserving intrusion detection in edge-based networks using federated self-supervised learning." *International Journal of Wireless and Microwave Technologies* 16, no. 3 (2026): 254-276.

[13] Visuvanathan, G. Elavel, Md Shohel Sayeed, and Sumendra Yogarayan. "BHFVAL: block chain-enabled hierarchical federated variational auto encoder framework for secure intrusion detection in vehicular networks." *Scientific Reports* 15, no. 1 (2025): 45742.

[14] Visuvanathan, G. Elavel, Md Shohel Sayeed, and Sumendra Yogarayan. "BHFVAL: block chain-enabled hierarchical federated variational auto encoder framework for secure intrusion detection in vehicular networks." *Scientific Reports* 15, no. 1 (2025): 45742.

[15] Sorour, Shaymaa E., Mohammed Aljaafari, Amany M. Shaker, and Ahmed E. Amin. "LSTM-JSO framework for privacy preserving adaptive intrusion detection in federated IoT networks." *Scientific Reports* 15, no. 1 (2025): 11321.

[16] Sharma, Ankita, Shalli Rani, and Wadii Boulila. "Blockchain-based zero trust networks with federated transfer learning for IoT security in industry 5.0." *PLoS One* 20, no. 6 (2025): e0323241.

[17] Elumalai, G., Dhanalakshmi Gopal, Jayaprakash Chinnadurai, and V. V. Teresa. "An energy-aware federated intelligence framework for sustainable WSN-IoT ecosystems." *Peer-to-Peer Networking and Applications* 19, no. 6 (2026): 137.

[18] Li, Huadong, Xiongzhi Xiao, Jianfeng Feng, and Huanquan Luo. "An EfficientNet hybrid deep learning detection framework of network intrusion with an optimized mixture-of-experts architecture." *Scientific Reports* (2026).

[19] Sharma, Yogesh Kumar, Shakti Kundu, Kavitha Venkatachari, Sonu Kumari, Sultan Mesfer Aldossary, Manel Ayadi, Mitiku Dubale Anamo, and Arshad Hashmi. "High-precision intrusion detection in IoT networks using an optimized TabNet model with AMP and Optuna." *Journal of Cloud Computing* (2026).

[20] Borra, Chandrakanth Reddy, Ramya Vani Rayala, Piyush Kumar Pareek, and Srinivas Cheekati. "Advancing IoT security with temporal-based Swin transformer and LSTM: A hybrid model for balanced and accurate intrusion detection." In *2025 International Conference on Intelligent and Cloud Computing (ICoICC)*, pp. 1-7. IEEE, 2025.