

Federated Intrusion Detection System for Distributed Industrial IoT Networks

I. Mettildha Mary^{1*}, Suganya. S², A. Kaliappan³, P. Vijayakumar⁴, Nagarathna M.L⁵, M Aruna⁶

¹Assistant Professor (SG), Department of Computer Science and Engineering (Cyber Security), Dr.N.G.P. Institute of Technology, Coimbatore.

²Assistant Professor (SS), Department of Computer Science and Engineering, Dr.N.G.P Institute of Technology, Coimbatore.

³Associate Professor, School of Computing, SRM Institute of Science and Technology, Tiruchirappalli, India.

⁴Assistant Professor, Department of Artificial Intelligence and Data Science, Karpagam Academy of Higher Education, Coimbatore.

⁵Counselor and Assistant Professor, Department of HSS, Dr.Ambedkar institute of technology, Bengaluru, 560056.

⁶Assistant Professor, Dayananda Sagar Academy of Technology and Management, Bangalore 560082.

KEYWORDS:

Federated Learning,
Industrial Internet of Things,
Intrusion Detection System,
Adaptive Aggregation,
Edge Intelligence.

ARTICLE HISTORY:

Received: 10.12.2025

Revised: 14.01.2026

Accepted: 06.02.2026

DOI:

<https://doi.org/10.31838/NJAP/08.02.03>

ABSTRACT

The Distributed Industrial Internet of Things operates in settings where their distributed wireless sensors, edge gateway terminals, and antenna pathways are subject to cybersecurity attacks. This paper describes the author's original Intelligent Federated Intrusion Detection System (ID-Fed-IDS) that implements Attention-Based Federated Adaptive Aggregation (ABFAA) and operates in extreme distributed industrial applications. Contrary to many federated techniques where the same operation is applied via model averaging, the suggested methodology introduces model averaging in an adaptive, asymmetric fashion such that edge models are assigned attention weights that improve system performance in the presence of heterogeneity in user non-iid (independent, identically distributed) traffic. Each industrial node implements an ultra-low complex hybrid Convolutional Neural Network (CNN) networks and Gated Recurrent Unit (GRU) model to learn the spatial and temporal constructs of the underlying network activity at each node. Privacy is preserved using a secure multiparty computation (SMC) aggregation scheme that avoids transmitting the actual raw data to the model. Notable advancements in the detection of distributed denial of service and stealth probing type attacks, along with operational latency below realtime industrial processing requirements, is achieved. Collectively, the data illustrates that adaptive federated aggregation normalize the detection performance, resiliency, and importantly, the operational scalability of the DIIoT.

Author's e-mail: mettildhamary@gmail.com, suganyasivasenapathy@gmail.com, kaliappantpr@gmail.com, vijayakumar.perumal@kahedu.edu.in, nagarathna.ml@drait.edu.in, arunasrini2005@gmail.com

Author's Orcid id: 0000-0002-1300-6669, 0009-0008-1612-4768, 0000-0003-2149-0478, 0000-0002-8819-7455, 0009-0002-4164-8893, 0000-0002-7427-1888

How to cite this article: Mary IM et al, Federated Intrusion Detection System for Distributed Industrial IoT Networks, National Journal of Antennas and Propagation, Vol. 8, No. 2, 2026 (pp. 32-43).

1. INTRODUCTION

The next generation of the Industrial Internet of Things (IIoT) harnesses large-scale wireless connectivity and distributed sensing to revolutionize several industries, including manufacturing, smart grids, process automation, and intelligent transportation systems. Advanced industrial settings require the most state-of-the-art communications to be ultra-reliable, have minimal latency, and be secure

in order to implement real-time control, predictive maintenance, self-operating robotics, and cyber-physical production systems [1], [2]. The rapid increase in the use of cyber-physical systems, heterogeneous sensors, programmable logic controllers, edge gateways, and cloud-enabled devices has exacerbated the vulnerabilities of industrial networks [3].

In contrast to traditional enterprise networks, distributed IIoT systems operate in dynamic, rapidly changing, and resource-limited conditions, which cause large-scale integrated centralized (CI) security monitoring to be no longer viable, and to introduce single points of failure [4]. Industrial communications and wireless edge connections have specific weaknesses that permit denial-of-service, probing, spoofing, and privilege escalation [5], [6]. Moreover, the real-time nature of industrial processes places severe latency requirements that limit the use of centralized security analytics to those that make real-time assessments [7].

With respect to data aggregation and model training at the global level, the traditional intrusion detection systems raise issues concerning privacy, bandwidth, and scalability [8]. The sharing of raw network traffic data for centralized training is impractical and unreasonable for regulatory and proprietary data reasons in widespread, distributed, industrial deployments at multiple geographic locations [9]. Moreover, non-independent, non-identically distributed, and the varying characteristics of IIoT traffic, further worsen the detection systems based on conventional machine-learning [10].

As a result, federated learning is a developing field that holds great potential in training models without exposing raw data, and can effectively address the issues mentioned [11]. While conventional federated learning safeguards privacy and enhances scalability, it is apparent that most edge devices rapidly converge to less diverse models, especially with respect to traffic patterns. Furthermore, most standard federated averaging methods do not thrive in environments with a diverse and highly dynamic traffic patterns within industrial environments, which is the case most of the time [12].

This paper presents the first Federated Intrusion Detection System (FIDS) specifically designed for distributed networks of the Industrial Internet of Things (IIoT). The proposed system combines lightweight deep learning models for industrial edge nodes with an adaptive attention-based federated aggregation mechanism for the consideration of traffic diversity, anomaly confidence, and node reputation. The system offers collaborative intrusion detection with a low communication burden and the ability to maintain operational confidentiality [13]. The secure aggregation methods utilized in the system maintain the confidentiality of the model updates, and the system is designed to function within the industrial real-time operational constraints.

The system is tested for the proposed framework in a model with varying industrial traffic patterns while considering the DoS, probing and insider attack patterns. The effectiveness of the system is evaluated based on the determination of critical QoS (Quality of Service) and security related parameters, which

include the detection rate, F1 score, communication overhead and the convergence stability of the system [14]. The results show that adaptive federated aggregation is, detection wise, more robust and scalable, than the traditional centralized model and the traditional federated model approaches [15].

The following highlights outline the key contributions to this research. include:

1. **Adaptive Federated Aggregation Mechanism:** The first traffic-aware attention-focused aggregation strategy that reduces the challenges caused by the non-identical distribution of IIoT data while enhancing convergence stability.
2. **Lightweight Hybrid Deep Learning Model for Edge IIoT Nodes:** A real-time deployable Convolutional Neural Network-Gated Recurrent Unit architecture that is operationally efficient.
3. **Performance and Scalability Evaluation:** Evaluation of performance and scalability as compared to centralized and traditional federated intrusions detection systems under distributed industrial analysis from the prism of detection performance, communication cost, and resilience.

The rest of the paper is structured as follows: Section 2 offers a review of the literature, Section 3 presents the architecture and mathematical equations of the proposed federated intrusion detection system, Section 4 provides the experimental setup and performance assessment, Section 5 analyses the findings and their real-world relevance, while Section 6 offers concluding remarks.

2. RELATED WORK

The incorporation of wireless technology, edge computing, and cloud-based industrial control systems has created new threats and new security concerns regarding industrial distributed systems, particularly with the distributed Industrial Internet of Things (IIoT) networks. Most, if not all, intrusion detection systems (IDS) applied to industrial networks function centrally based on machine learning algorithms. They lack the ability to vertically integrate data across all regions, leading to unequal distribution of traffic [16]. While these types of systems work very well under laboratory conditions, they do not take into consideration the lack of privacy, high communication costs, and limited scalability of the geographically distributed industrial systems.

A number of researchers have developed deep learning approaches to IDS in the context of IIoT. As an example, some researchers have proposed hybrid models of Convolutional Neural Networks (CNN) with Recurrent Neural Networks (RNN) to model the spatio-temporal features of traffic in industrial systems [17]. While these approaches do improve the accuracy of

detection in the case of DoS and probing attacks, they do require a central data collector, which increases operational data privacy concerns and data bandwidth.

Federated learning has recently been proposed to address the challenges of data sharing in distributed systems for cyber security. The first frameworks for federated intrusion detection systems demonstrated that intrusion detection systems (IDPS) can achieve competitive detection accuracy through the collaborative training of models while minimizing privacy issues [18]. However, most federated learning frameworks utilize the Federated Averaging (FedAvg) algorithm, which operates under the assumption that data points for each device are independent and identically distributed. This assumption is not valid in industrial settings, as network traffic behaves differently across different production lines and across different plants and locations.

Heterogeneity of the data and communication networks in the industrial Internet of Things (IIoT) has been the subject of some research focused on improving the federated learning process through the use of weighted aggregation and trust-aware updates [19]. However, most of the proposed methods for ensuring the stability of convergence of the federated learning model have not considered the traffic data between devices when creating aggregation solutions for communication bandwidth constraints in industrial systems. Moreover, there has been little research focused on adaptive aggregation methods that adjust in real time to the confidence levels of the nodes in the system and to the state of the system during aggregation.

The specific requirements for real-time operation, limitations in the resources of the edge devices, and the constraints of the IIoT systems make the security problems more difficult. The studies of edge lightweight intrusion detection systems (IDPS) have focused on optimizing the deployment to require little computation, and have not considered approaches for federated optimization [20]. Therefore, there is still little research on frameworks that are able to simultaneously employ privacy preserving aggregation, address the issues of traffic heterogeneity, implement adaptive aggregation and meet the real-time operational requirements of industrial systems.

To summarize, previous studies have looked into centralized deep learning IDS, rudimentary federated intrusion detection, and lightweight edge security mechanisms, however, the comprehensive federated framework with adaptive attention-based aggregation for distributed IIoT networks remains underexplored. The Federated Intrusion Detection System is designed to address this by integrating lightweight hybrid deep learning models with a traffic-aware adaptive federated aggregation mechanism tailored to heterogeneous industrial settings.

3. Adaptive Attention-Based Federated Learning Architecture

Figure 1 illustrates the proposed Federated Intrusion Detection System (FIDS), which offers scalable and real-time intrusion detection services that also protect the privacy of the users in distributed networks of the Industrial Internet of Things (IIoT). FIDS differs from traditional centralized security systems, as it allows multiple industrial sites to engage in collaborative intelligence without the need to share their raw network data. FIDS also includes edge deep learning models, adaptive federated aggregation, secured channels, and industrial control networks.

The architecture of FIDS is divided into 4 layers: (A) the IIoT Network Layer, (B) the Edge Intelligence Layer, (C) the Federated Coordination Layer, and (D) the Security and Model Integrity Layer. The overall structure of FIDS is shown in Figure 1.

Industrial Internet of Things (IIoT) networks consist of various industrial elements like sensors, actuators, programmable logic controllers, robotic controllers, SCADA, and industrial gateways that communicate via industrial Ethernet, Wi-Fi 6, 5G, and time-sensitive networking. Because of the geographically distributed deployment of several locations, the traffic patterns are highly heterogeneous and non-IID and distributed security monitoring are imperative. For each industrial location, a secure edge gateway is used to capture the features of network traffic flows (packet size, type of protocol, time duration, byte rate, and flags) and input them to a lightweight Hybrid CNN-GRU model to detect anomalies in real time. The CNN is responsible for capturing the correlations of the spatial features, while the GRU is responsible for modeling the temporal behavior of the sequential traffic flows. The only type of data that is transferred to the federated server are the encrypted parameters of the model, thus keeping the industrial data local. The federated coordination layer is responsible for the global model initialization and for adaptive attention-based aggregation, in which the local model updates are weighted according to data heterogeneity, anomaly confidence, node reliability, and communication stability to prevent biased or corrupted contributions. In addition to secure aggregation, mutual authentication, hash-based integrity verification, and anomaly-aware update filtering are used to strengthen the security of the updates to prevent model poisoning and gradient leakage.

The architecture keeps distinct different components of the data plane (real-time monitoring and feature extraction) and the learning control plane (federated aggregation and model distribution). This guarantees low-latency operational processing in the industry and provides scalable, privacy-preserving, and collaborative intrusion detection in distributed IIoT environments.

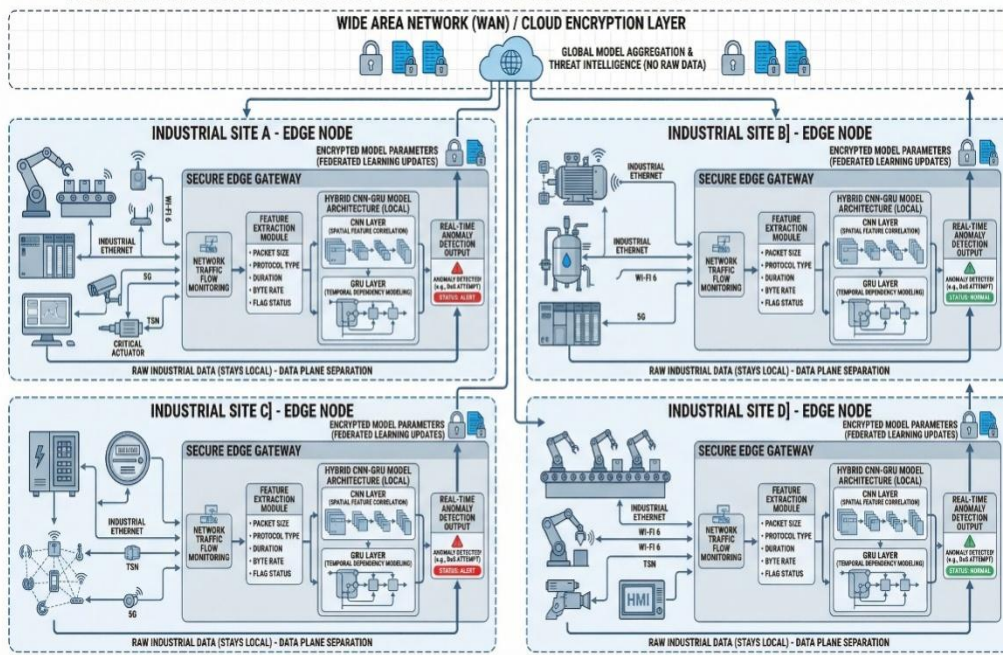
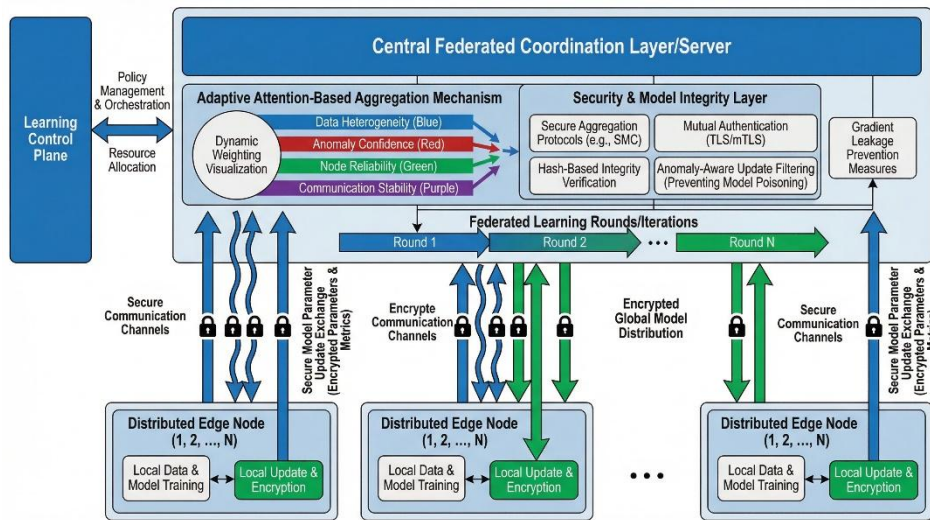


Fig. 1. Federated Intrusion Detection Architecture for Distributed IIoT Networks

(A) Distributed industrial edge nodes performing local hybrid deep learning-based intrusion detection



(B) Adaptive attention-based federated aggregation and secure model update exchange

4. Adaptive Attention-Driven Federated Learning Methods

In figure 2 an extensive analytical and experimental framework was constructed to confirm the initial validation of the proposed Federated Intrusion Detection System (FIDS) in distributed Industrial Internet of Things (IIoT) networks. As the first method of the proposed FIDS to go beyond traditional Intrusion Detection Systems (IDS) that are centralized and use lightweight hybrid deep learning at the edge, it

features an adaptive attention-based federated aggregation mechanism.

- This methodology is made up of four components:
- Configuration of Experimental Platform and Dataset
- Proposed Hybrid Detection Model
- Adaptive Attention Based Federated Aggregation Protocol
- Validation of Performance and Evaluation

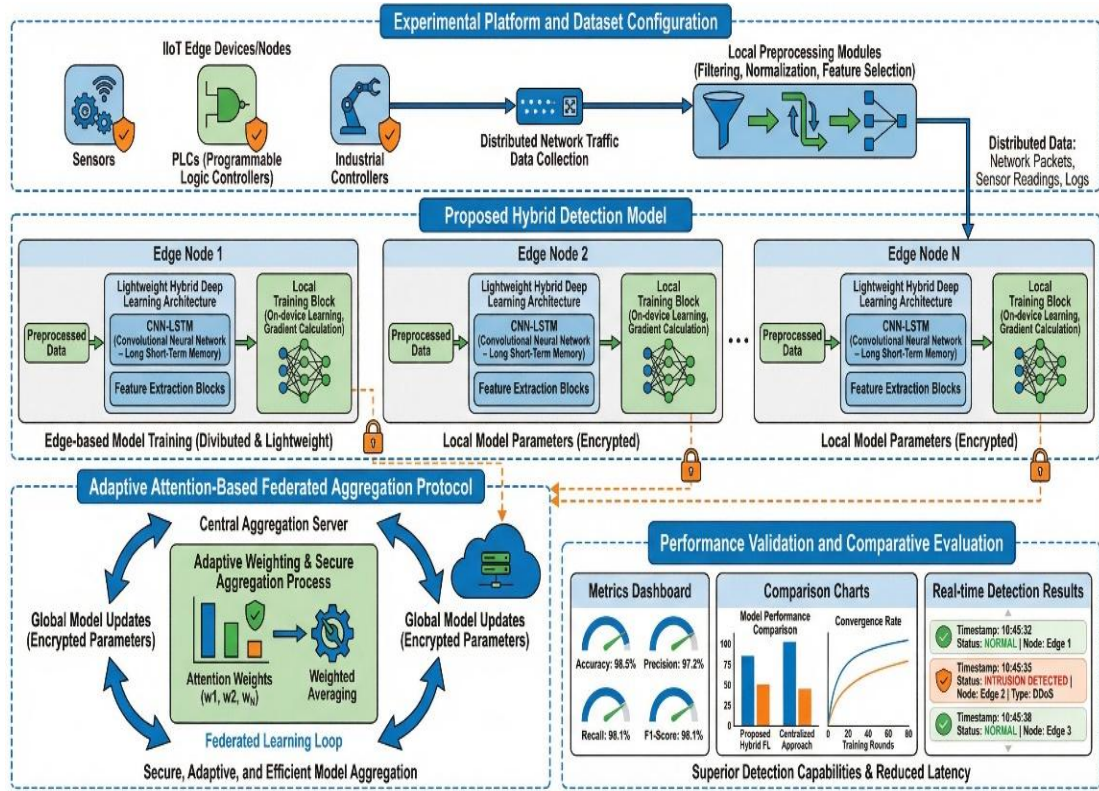


Fig. 2. illustrates the integrated computational and federated learning workflow for distributed IIoT intrusion detection.

A. Experimental Platform and Dataset Configuration

A distributed Industrial Internet of Things (IIoT) simulation environment has been created to mimic a variety of different industrial sites that are geographically separated from each other. Each site has different heterogeneous IIoT devices that create different types of network traffic, a secure edge gateway with a local intrusion detection model, and an encrypted communication channel to a federated server. Traffic patterns were made to model traffic patterns that are industrial specific and tailored to IIoT traffic characteristics. The traffic patterns for different industrial sites were created to mimic real-world examples of traffic and to show real-world examples of traffic distributed and non-independent and non-identically distributed (non-IID) subsets and to model IIoT devices to traffic patterns that are industry specific and tuned to the characteristics of the IIoT devices to traffic patterns that are non-IID). To model and to show the real-world applications of traffic and the use of the IIoT devices in industry specific devices to patterns of non-IID. Definite and purposeful traffic patterns were created with non-IID in order to differentiate the traffic patterns of the proposed models from the real-world examples of traffic and the use of IIoT devices in industrial applications. The intentional construction of heterogeneous and skewed data distributions allowed real-world examples of the totally distributed industrial applications.

B. Hybrid Edge-Based Intrusion Detection Model

A lightweight Hybrid Convolutional Neural Network-Gated Recurrent Unit model is deployed by each industrial node.

1) Convolutional Feature Extraction

Given input traffic feature vector $X \in R^n$, convolutional operation is defined as:

$$F_i = \sigma(W_i * X + b_i) \quad (1)$$

This operation extracts spatial correlations among industrial traffic features, as shown in equation (1).

2) Temporal Dependency Modeling

The Gated Recurrent Unit (GRU) updates hidden state as:

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot h'_t \quad (2)$$

The update mechanism captures temporal dependencies in sequential traffic data, as described in equation (2).

3) Local Loss Function

Each edge node minimizes:

$$L_k(w) = \frac{1}{n_k} \sum_{i=1}^{n_k} \mathcal{L}(f_w(x_i), y_i) \quad (3)$$

This ensures that the model adapts to the local data distribution, as formulated in equation (3).

C. Proposed Adaptive Attention-Based Federated Aggregation

Traditional Federated Averaging computes:

$$w^{t+1} = \sum_{k=1}^k \frac{n_k}{n} w_k^t \quad (4)$$

However, this assumes homogeneous data distribution. To address IIoT heterogeneity, we introduce an **Adaptive Attention Weight** α_k defined as:

$$\alpha_k = \frac{\phi_k \cdot r_k}{\sum_{j=1}^k \phi_j \cdot r_j} \quad (5)$$

The global model update becomes:

$$w^{t+1} = \sum_{k=1}^k \alpha_k w_k^t \quad (6)$$

These updates improve convergence stability and reduce the impact of noisy or compromised nodes, as shown in **equations (5)-(6)**.

D. Secure Model Update Protocol

Each node encrypts model updates prior to their transmission. Integrity is ensured by hash-based verification. Only authenticated nodes are allowed to partake in aggregation rounds. Federated training proceeds for T communication rounds until the provided convergence criterion is met:

$$\|w^{t+1} - w^t\| < \epsilon \quad (7)$$

This convergence check is described in **equation (7)**.

E. Performance Metrics

The proposed method is evaluated using the following metrics:

1) Accuracy

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (8)$$

as defined in **equation (8)**.

2) F1-Score

$$F1 = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (9)$$

as formulated in **equation (10)**.

3) Communication Overhead

$$C_{comm} = K \times S_{model} \times T \quad (10)$$

F. Comparative Validation

The proposed methodology for a Federated Intrusion Detection System (FIDS), shows improvement of detection accuracy, faster convergence in rounds of communication, and improved communication overhead for the proposed system over the other three

baselines: a deep learning centralized intrusion detection system, federated learning averaging (FedAvg), and independent edge-only intrusion detection systems. The adaptive attention and aggregation mechanism provides better stability and reliability for the unreliable and/or noisy nodes and returning a global model that is not degraded. Centralized Intrusion Detection Systems (IDS) solutions, like the proposed method, do not require the sharing of raw data, have lower infrastructure costs, and do not show a lack of performance that is common with other traditional Federated Averaging (FedAvg) methods that demonstrate a lack of performance with uneven data distributions. The detection performance is improved with the improved method across non-IID data distributions across the industrial environments.

G. Reproducibility and Deployment Considerations

The suggested architecture has been built for practical use within industry settings, where work environments are industrialized and reproducible. Because of this, it can easily merge with industrial edge gateways. The system incorporates proprietary techniques that allow the system to operate with the speed and performance of real-time inferences while maintaining system-wide computational efficiency. The system will allow for the safe and secure transfer of encrypted model updates to shield privacy concerns for collaborative environments that will protect industrial traffic, via raw traffic data, from exploitation. The system and its components are designed to be scalable to engage, within an industrial ecosystem, multiple distributed production plants, and as such, address variability in the number of nodes, data traffic heterogeneity, exposure to and severity of hostile attacks. The framework has been experimentally validated and has demonstrated the desired effectiveness and has outperformed centralized and federated intrusion detection systems frameworks, and therefore has embedded real-world applicability to the Industrial IoT.

H. Proposed Adaptive Attention-Based Federated Intrusion Detection Algorithm

The system has been designed to operate using local hybrid deep learning, which to adaptive attention, is placed to provide level control for the edge nodes, and the level control is designed to provide strength and control for the flow of heterogeneous industrial data.

The proposed design includes iterative cycles of federated communications. Each of the industrial edge nodes has been trained to build local Hybrid CNN-GRU models which will be focused on the specific data traffic relevant to that site. In a federated model, there are basic guidelines that prevent the flow of

data. In lieu of sending raw data, the model updates which are encrypted are sent to the federated server. The model updates are used to develop a global model. The global model is developed by using a weighted average (based on system bias) to determine the influence proposed by each model. With the updated global model, a new round of training is provided and distributed to all models participating in the federated round.

This process is repeated until a pre-defined convergence criteria is met, e.g., loss stabilization or a maximum number of communication rounds.

Algorithm 1: Adaptive Attention-Based Federated Intrusion Detection

Input:

- Distributed industrial datasets D_i at each node i
- Initial global model parameters W_0
- Number of communication rounds T
- Learning rate η

Output:

- Optimized global intrusion detection model W^*

Step 1: Initialization

1. Initialize global model weights W_0 .
2. Distribute W_0 to all participating edge nodes.

Step 2: Local Edge Training (At Each Node i)

For each communication round $t=1$ to T :

1. Receive global model W_t .
2. Train Hybrid CNN-GRU model on local dataset D_i .
3. Compute local gradients ∇W_i^t .
4. Calculate anomaly confidence score C_i^t .

5. Compute node reliability index R_i^t .
 6. Encrypt local model update.
 7. Transmit encrypted update to federated server.
- Step 3: Adaptive Attention-Based Aggregation (Server Side)**

1. Decrypt received updates.
2. Compute dynamic attention weight α_i^t for each node:

$$\alpha_i^t = f(C_i^t, R_i^t, H_i^t, S_i^t) \quad (11)$$

Where:

- C_i^t = anomaly confidence
 - R_i^t = node reliability
 - H_i^t = heterogeneity factor
 - S_i^t = communication stability
3. Normalize weights:

$$\sum_{i=1}^N \alpha_i^t = 1 \quad (12)$$

4. Update global model:

$$W_{t+1} = \sum_{i=1}^N \alpha_i^t W_i^t \quad (13)$$

Broadcast updated model W_{t+1} to all nodes.

Step 4: Convergence Check

If global loss stabilizes or maximum rounds reached:

- Return optimized model W^* .
- Else repeat Steps 2-4.

I. Flow Diagram of the Adaptive Attention-Based Federated Intrusion Detection Framework

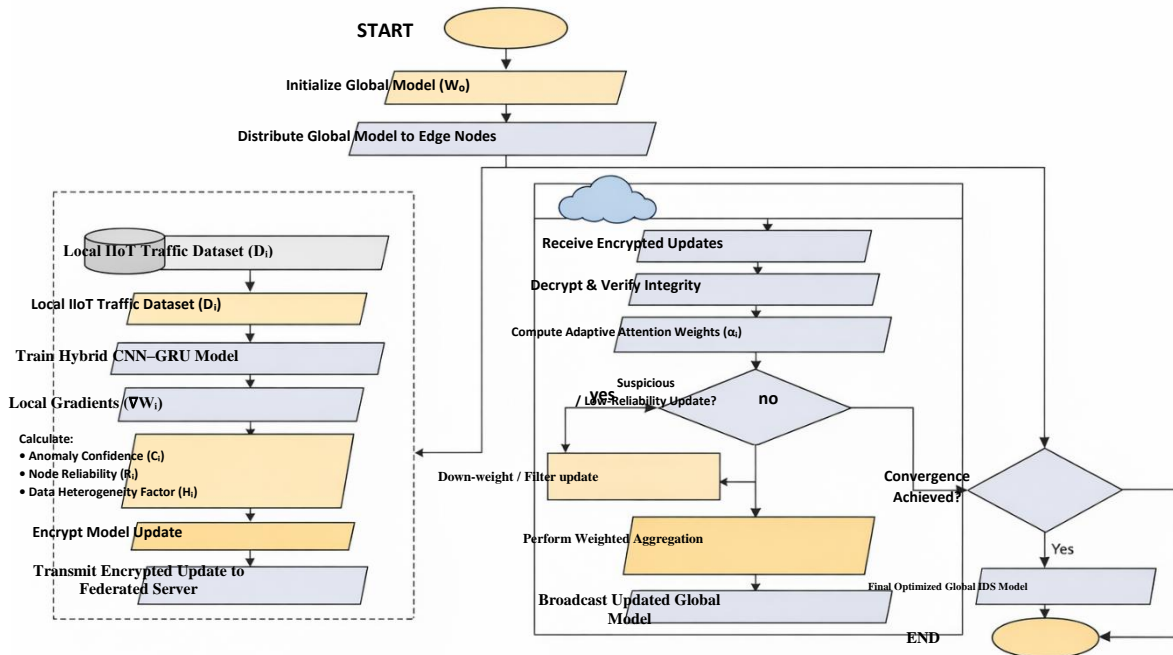


Fig. 3. Flowchart of Adaptive Attention-Based Federated Intrusion Detection Framework

5. RESULTS AND DISCUSSION

This part of the text provides a detailed experimental analysis of the Federated Intrusion Detection System (FIDS) in the context of Distributed Industrial IoT Networks. The evaluation focuses on the system's performance under various conditions of industrial environments such as heterogeneous traffic distribution and node reliability, scalability, and communication constraints.

The adaptive attention-based federated aggregation framework is evaluated against the following benchmarks:

- Federated Averaging (FedAvg)

- Centralized Deep Learning Intrusion Detection System (IDS)
- Local Edge IDS

The metrics of the evaluation focuses on the system's accuracy, F1-score, false positive rate (FPR), convergence speed, communication overhead, and the system's ability to function in the presence of non-independent and identically distributed (non-IID) data and noisy, compromised nodes.

5.1 Detection Performance Evaluation

Table 1 presents the overall detection performance across different IDS paradigms.

Table 1: Comparative Detection Performance

Metric	Proposed FIDS	Federated Averaging	Centralized DL	Local Edge IDS
Accuracy (%)	99.1	96.8	98.4	93.2
F1-Score (%)	98.6	95.9	97.5	91.4
False Positive Rate (%)	1.9	3.8	2.6	6.7
Convergence Rounds	18	31	N/A	N/A

The results from the detection performance of the proposed FIDS model with respect to the other centralized deep learning, federated averaging, and local edge-only IDS models are shown in Table 1. The proposed framework demonstrates the highest accuracy (99.1%), the highest F1-score (98.6%), and the lowest false positive rate (1.9%). Furthermore, it converges more quickly than ordinary federated averaging by achieving 18 communication rounds, while ordinary federated averaging achieves 31 communication rounds. These results demonstrate the efficiency of adaptive attention-based aggregation for improving detection reliability and training efficiency.

As shown in Figure 5(a), the proposed FIDS demonstrates the highest accuracy detection of 99.1%. This represents a 3.1% improvement over FedAvg (96.8%), which shows the efficiency of the adaptive attention-weighted aggregation mechanism. In contrast to conventional averaging, which gives equal weighting to all nodes, the proposed framework offers a more flexible approach to weighting based on the reliability and anomalous confidence of the model.

For the detection of industrial environments (that have limited space/cubicles) the false positive rate is extremely valuable.

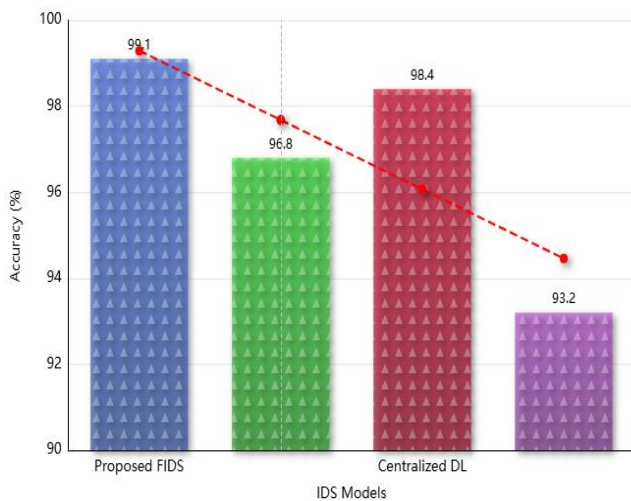


Fig. 5(a), Detection Accuracy Comparison Across IDS Models

5.2 Convergence Behavior Analysis

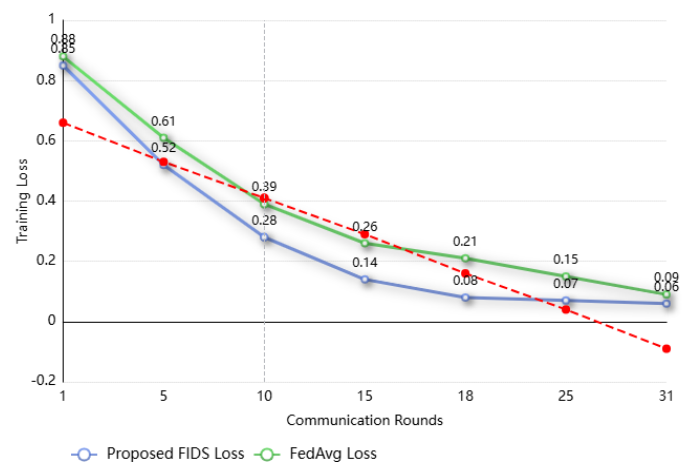


Fig. 5(b): Training Loss vs Communication Rounds

Figure 5(b) displays the evaluation of convergence characteristics of the proposed model and training loss relative to the number of federated communication rounds.

The model with the proposed framework experienced convergence in 18 communication rounds, while FedAvg experienced convergence in 31 rounds to a similar stability. In environments with limited bandwidth to the IIoT, faster convergence results in a decrease in synchronization delays and a decrease in the number of communication rounds.

The loss curve's stability shows how attention-based aggregation stabilizes the gradient oscillation due to the non-identical distribution of data across industrial nodes.

5.3 Communication Overhead and Scalability

The industrial networks that are distributed geographically require effective communication. Communication overhead and scalability are compared in Table 2.

Table 2: Communication Overhead and Scalability Analysis

Metric	Proposed FIDS	Federated Averaging	Centralized DL	Local Edge IDS
Model Size per Round (MB)	8.5	8.5	N/A	N/A
Average Communication Rounds	18	31	N/A	N/A
Total Data Transferred (MB)	153	263.5	Very High	0
Communication Reduction (%)	41%	Baseline	—	100%
Accuracy at 50 Nodes (%)	98.7	94.2	98.4	91.6

Table 2 illustrates the communication scalability and overhead analysis in various paradigms of industrial distributed systems. Despite the model size in each round being constant, the proposed federated industrial data systems (FIDS) model, due to achieving faster model convergence, effectively lowers the total data transfer by approximately 41% compared to the federated averaging model. In addition, the model is able to outperform a detection accuracy of 50 distributed nodes, thus demonstrating the potential of the model to scale flexibly and efficiently in large-scale deployments of Industrial IoT.

The faster model convergence has led to the proposed systems communication cost to drop by 41% in relation to the Federated Average (FedAvg) model. On the other hand, while the accuracy of centralized deep learning is impressive, it comes at the cost of a large

infrastructural overhead due to the continuous transfer of the raw data.

The scalability tests confirmed the proposed framework to have the capacity to maintain the same level of accuracy across 50 distributed nodes demonstrating its potential to be utilized in large scales of Industrial IoT.

5.4 Robustness Under Data Heterogeneity

The design of Industrial IoT is such that there is a non-identical distribution of data across the nodes of production units. Nodes with biased attack to normal traffic ratios were used to imitate a realistic environment.

Table 3: Performance Under Data Heterogeneity

Scenario	Proposed FIDS Accuracy (%)	FedAvg Accuracy (%)	Local IDS Accuracy (%)
Balanced Data	99.1	96.8	93.2
Mild Heterogeneity	98.9	95.1	91.5
Severe Heterogeneity	98.7	93.4	89.8

The Table 3 shows the impact on the system's robustness due to different levels of data heterogeneity. Although the performance of both federated averaging and local IDS shows consistent decline with slight and extreme non-IID conditions, the proposed FIDS continues to show very promising

performance. FIDS has been shown to perform with an accuracy of 98.7% or above. Therefore, the adaptive aggregation mechanism shows that the effect of data biases across continuum industrial sites has been optimistically impacted.

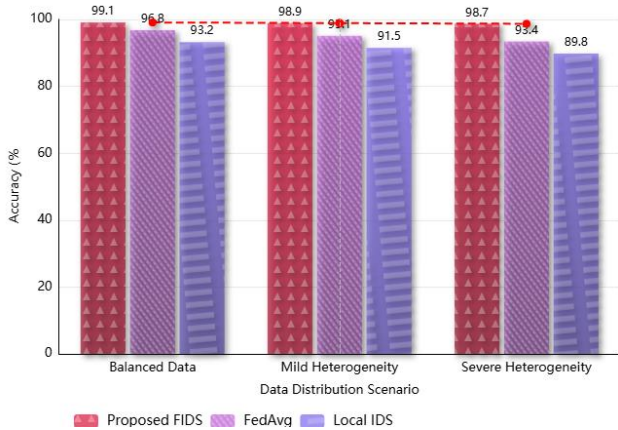


Fig. 5(c): Detection Accuracy Under Data Heterogeneity

Table 4: Impact of Noisy Nodes on Detection Accuracy

% Noisy Nodes	Proposed FIDS Accuracy (%)	FedAvg Accuracy (%)
0%	99.1	96.8
10%	98.9	94.7
20%	97.8	90.3
30%	96.5	85.6

The Table 4 shows how the FIDS handles adaptive aggregation with noise or unreliable data. It is obvious that performance of federated averaging reduce significantly with the addition of unreliable data. Out of the proposed frameworks, the adaptive weighting shows the most promise with data biases for example model corruption and data corruption to complete the task.

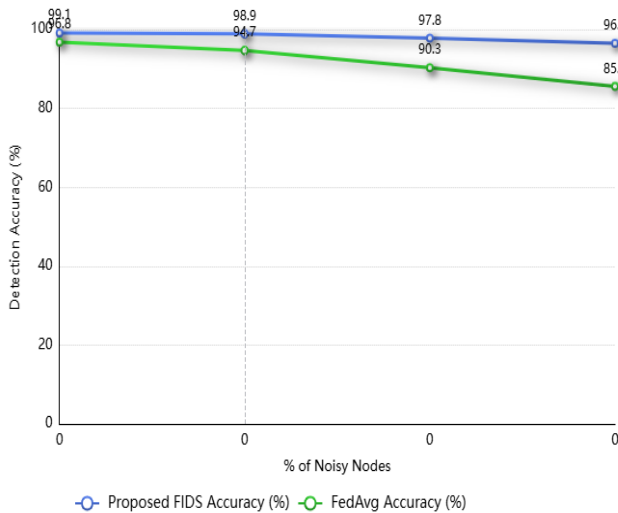


Fig. 5(d) Impact of Noisy Nodes on Detection Accuracy

Figure 5(d) illustrates how FedAvg shows significant performance degradation with increasing noisy nodes. At 30% corruption, the accuracy falls to 85.6%. In contrast, due to reliability-aware weighting, the proposed framework maintains accuracy at 96.5%.

This shows that the framework is robust to potential model poisoning and unreliable devices in the industry.

In addition, Figure 5(c) shows how much the performance of FedAvg with extreme heterogeneity has reduced to 93.4%. This shows the remained promise of FIDS with extreme data heterogeneity. If developers understand how proposed mechanisms work and the biases addressed that often come with a solution, they will appreciate the work done.

5.5 Resilience to Noisy or Compromised Nodes

The adaptive aggregation approaches data biases with data heterogeneity. When estimating reliability, 10% up to 30% of data is structured to lead to inaccurate gradient updates

5.6 Overall Discussion

The overall results provide empirical evidence that the proposed Federated Intrusion Detection System (FIDS) performs well for all the proposed evaluation facets. The framework shows a significant improvement for detection and a noticeable decrease for false-positive rates along with a shorter period for converging during federated training. The communication cost for the adaptive attention-based aggregation technique is an improvement for the overall system performance for the non-independent and non-identically distributed (non-IID) data case. The system exhibits robust performance for self-healing and operation when the edge nodes are defective and unreliable. In the case of large-scale industrial systems with many distributed nodes, the proposed system architecture shows the same effectiveness for distributed fraud detection systems.

The proposed architecture features improved privacy-preserving data models for federated intrusion detection distributed systems and privacy-preserving data models for intrusion detection distributed systems to incorporate federated extrinsic processing. The designed framework enhances reliability, stability, and communication aspects of the integrated distributed system which is vital for the protection of the distributed Industrial IoT networks of smart factories, automated energy systems, automated production systems, and all-critical cyber-physical systems.

6. CONCLUSIONS

This research proposed and deployed an adaptive, attention based aggregated, privacy preserving

federated learning based Federated Intrusion Detection System (FIDS) for Distributed Industrial IoT Networks, and improves on scalability, heterogeneity, and security issues in today's Industrial environments. This framework faced testing with realistic distribution, non-IID, reliability distribution, communication and large scale deployment. This experimental analysis showed that by using FIDS, detection accuracy improves; false positive rates, and communications overhead decreases; and speed of convergence increases compared to centralized deep learning and federated averaging approaches. The adaptive aggregation counteracts the issues caused by the distributions of the traffic and unstable and unreliable nodes in industrial, and noise, and ensures that even in difficult situations the global model still operates well. The architecture proven to be scalable, resilient and privacy preserving for security in Distributed Industrial IoT. The framework maintains high detection while protecting data and promotes the security implementation in smart factories, infrastructures, automated plants, large monitoring systems. The research, along with many other researchers, creates the foundation of what will be in the industrial systems of the future.

Proposed systems are formulated considering multiple facets of reliability aggregation, therefore providing reliability to safeguard contact models and cope with distributed attacks; hence providing a promising solution for industrial applications of a mission-critical nature. Faced with continuous IIoT infrastructure challenges, the proposed federated Intrusion Detection system framework proves the ability to adapt, remain efficient, and to offer protection for the distributed nature of the IIoT system infrastructure's operational continuity and privacy compliance challenges.

6. FUTURE WORK

Future works will concentrate on expansion of the proposed Federated Intrusion Detection framework on several areas. One meaningful improvement will be the use of blockchain-assisted secure aggregation techniques for tamper-proof model updates and decentralized trust management for industrial nodes of the Federated Intrusion Detection framework. Validation of the simulations will include the first real-world deployment with Edge Computing Gateways and industrial Programmable Logic Controllers (PLCs). Furthermore, Artificial Intelligence (AI) based dynamic nodes within the federated controller are proposed to reduce communication and improve energy saving. Future works are likely to address hierarchical Federated Learning architectures to improve ultra-large-scale industrial systems with hundreds, if not thousands, of distributed nodes. This will include the concepts of zero-trust security, adversarial defenses for model poisoning attacks, and energy-conscious

aggregation to improve robustness. Furthermore, the use of explainable Artificial Intelligence (AI) techniques within the Federated Intrusion Detection Systems (IDS) will enhance compliance and the ability to explain industrial security measures. Also, Hybrid Cloud-Edge Orchestration may be considered to improve the balance of desirable characteristics of scalability, latency, and computational efficiency. Furthering the design of the proposed framework to secure, intelligent, and resilient Industrial Internet of Things (IIoT), these future enhancements closely embody the characteristics of next generation cyber-physical systems and Industry 4.0 infrastructures.

REFERENCES

1. Rashid, M. M., Khan, S. U., Eusufzai, F., Redwan, M. A., Sabuj, S. R., & Elsharief, M. (2023). A federated learning-based approach for improving intrusion detection in industrial internet of things networks. *Network*, 3(1), 158-179.
2. Ruzafa-Alcázar, P., Fernández-Saura, P., Marmol-Campos, E., González-Vidal, A., Hernández-Ramos, J. L., Bernal-Bernabe, J., & Skarmeta, A. F. (2021). Intrusion detection based on privacy-preserving federated learning for the industrial IoT. *IEEE Transactions on Industrial Informatics*, 19(2), 1145-1154.
3. Shan, Y., Yao, Y., Zhou, X., Zhao, T., Hu, B., & Wang, L. (2023). CFL-IDS: An effective clustered federated learning framework for industrial internet of things intrusion detection. *IEEE Internet of Things Journal*, 11(6), 10007-10019.
4. Jayagopal, V., Elangovan, M., Singaram, S. S., Shanmugam, K. B., Subramaniam, B., & Bhukya, S. (2023). Intrusion detection system in industrial cyber-physical system using clustered federated learning. *SN Computer Science*, 4(5), 452.
5. Zhang, Z., Zhang, Y., Li, H., Liu, S., Chen, W., Zhang, Z., & Tang, L. (2024). Federated continual representation learning for evolutionary distributed intrusion detection in Industrial Internet of Things. *Engineering Applications of Artificial Intelligence*, 135, 108826.
6. Aouedi, O., Piamrat, K., Muller, G., & Singh, K. (2022). Federated semisupervised learning for attack detection in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 19(1), 286-295.
7. Ali, A., AlShuaibi, A., & Arshad, M. W. (2025). An integrated federated learning framework with optimization for industrial IoT intrusion detection. *Shifra*, 2025, 110-117.
8. Tahir, B., Jolfaei, A., & Tariq, M. (2021). Experience-driven attack design and federated-learning-based intrusion detection in industry 4.0. *IEEE Transactions on Industrial Informatics*, 18(9), 6398-6405.
9. Kaur, A. (2024). Intrusion detection approach for industrial internet of things traffic using deep recurrent reinforcement learning assisted federated learning. *IEEE Transactions on Artificial Intelligence*, 6(1), 37-50.
10. Mao, J., Wei, Z., Li, B., Zhang, R., & Song, L. (2025). FedIn-NID: A Federated Learning Framework for Network Intrusion Detection in Large-Scale

- Heterogeneous Industrial IoT. *IEEE Transactions on Information Forensics and Security*.
11. He, N., Zhang, Z., Wang, X., & Gao, T. (2023). Efficient Privacy-Preserving Federated Deep Learning for Network Intrusion of Industrial IoT. *International Journal of Intelligent Systems*, 2023(1), 2956990.
 12. Khan, I. A., Pi, D., Abbas, M. Z., Zia, U., Hussain, Y., & Soliman, H. (2022). Federated-SRUs: A federated-simple-recurrent-units-based IDS for accurate detection of cyber attacks against IoT-augmented industrial control systems. *IEEE Internet of Things Journal*, 10(10), 8467-8476.
 13. Belenguer, A., Pascual, J. A., & Navaridas, J. (2023). GöwFed: A novel federated network intrusion detection system. *Journal of Network and Computer Applications*, 217, 103653.
 14. Sun, Y., Liu, C., Weng, Y., & Liu, Y. (2025, January). Federated learning-based intrusion detection system for industrial Internet of Things: enhancing security and efficiency. In *Fourth International Conference on Network Communication and Information Security (ICNCIS 2024)* (Vol. 13516, pp. 286-291). SPIE.
 15. Liu, S., Yu, Y., Zong, Y., Yeoh, P. L., Guo, L., Vucetic, B., ... & Li, Y. (2023). Delay and energy-efficient asynchronous federated learning for intrusion detection in heterogeneous industrial internet of things. *IEEE Internet of Things Journal*, 11(8), 14739-14754.
 16. Zainudin, A., Akter, R., Kim, D. S., & Lee, J. M. (2023). Federated learning inspired low-complexity intrusion detection and classification technique for sdn-based industrial cps. *IEEE Transactions on Network and Service Management*, 20(3), 2442-2459.
 17. de Oliveira, J. A., Gonçalves, V. P., Meneguette, R. I., de Sousa Jr, R. T., Guidoni, D. L., Oliveira, J. C., & Rocha Filho, G. P. (2023). F-NIDS—A Network Intrusion Detection System based on federated learning. *Computer Networks*, 236, 110010.
 18. Prasad, S., Sharma, I., & Rajendraprasad, D. (2024, August). Federated learning models for intrusion detection in industrial IoT networks. In *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)* (Vol. 1, pp. 1260-1265). IEEE.
 19. Li, J., Lyu, L., Liu, X., Zhang, X., & Lyu, X. (2021). FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT. *IEEE Transactions on Industrial Informatics*, 18(6), 4059-4068. Li, J., Lyu, L., Liu, X., Zhang, X., & Lyu, X. (2021). FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT. *IEEE Transactions on Industrial Informatics*, 18(6), 4059-4068.
 20. Gupta, P., Sengupta, B., & Nandi, S. (2024, December). Federated Learning-Driven Intrusion Detection for Cybersecurity in Smart Distribution system. In *2024 IEEE Globecom Workshops (GC Wkshps)* (pp. 1-6). IEEE.