Privacy-Enhanced Federated Learning Model for Secure Internet of Things Environments

Mohammed Ajuji *, Yusuf Musa Malgwi , Asabe Sandra Ahmadu , Mohammed Kabir Ahmed

Posted Date: 20 May 2026

doi: 10.20944/preprints202605.1277.v1

Keywords: federated learning; internet of things; intrusion detection; privacy-preserving machine learning; adaptive client selection; differential privacy; cybersecurity; edge intelligence; non-IID data; secure aggregation

 doi:10.20944/preprints202605.1277.v1

Article

Privacy-Enhanced Federated Learning Model for Secure Internet of Things Environments

Mohammed Ajuji [1,*], Yusuf Musa Malgwi [2], Asabe Sandra Ahmadu [2] and Mohammed Kabir Ahmed [2]

[1] Department of Computer Science, Faculty of Science, Gombe State University, Gombe State - Nigeria
[2] Department of Computer Science, Faculty of Computing, Modibbo Adama University, Yola – Nigeria
* Correspondence: majuji@gsu.edu.ng

Abstract

The rapid growth of Internet of Things (IoT) ecosystems has significantly increased cybersecurity threats due to device heterogeneity, resource limitations, and exposure to distributed attacks. Although Federated Learning (FL) has emerged as a promising privacy-preserving machine learning paradigm for decentralized intrusion detection, existing FL approaches often suffer from non-independent and identically distributed (non-IID) data, communication inefficiency, adversarial attacks, and unstable convergence in heterogeneous IoT environments. This study proposes a Privacy-Enhanced Federated Learning (PEFL) framework for adaptive and secure intrusion detection in large-scale IoT networks. The framework integrated differential privacy, secure aggregation, adaptive client selection, trust-aware federated optimization, and edge-assisted hierarchical coordination to improve robustness, scalability, and communication efficiency. The framework was evaluated using benchmark cybersecurity datasets, including CICIDS2017, UNSW-NB15, TON_IoT, and Bot-IoT under heterogeneous and adversarial conditions. Experimental results established that the proposed PEFL framework achieved improved intrusion detection accuracy, faster convergence stability, enhanced resilience against poisoning attacks, and reduced communication overhead compared with conventional FL approaches such as FedAvg and FedProx. The findings further indicated that adaptive client selection and trust-aware aggregation significantly improve model reliability and robustness in resource-constrained IoT environments. This framework will contribute toward the development of scalable, privacy-preserving, and deployable federated intrusion detection systems for next-generation intelligent IoT infrastructures.

Keywords: federated learning; internet of things; intrusion detection; privacy-preserving machine learning; adaptive client selection; differential privacy; cybersecurity; edge intelligence; non-IID data; secure aggregation

1. Introduction

The rapid proliferation of the Internet of Things (IoT) has transformed modern digital ecosystems by enabling interconnected devices to support intelligent services across healthcare, smart cities, industrial automation, transportation, and critical infrastructure [1–3]. However, the increasing deployment of IoT devices has significantly expanded cybersecurity and privacy risks due to device heterogeneity, limited computational resources, and continuous exposure to untrusted networks [4–6]. Traditional centralized machine learning approaches for intrusion detection and cybersecurity analytics often require the collection of sensitive data at centralized servers, thereby introducing privacy leakage risks, scalability limitations, and communication overhead [7–9].

Federated Learning (FL) has emerged as a promising distributed machine learning paradigm that enables collaborative model training without sharing raw data among participating devices [10]. By allowing local model training at edge devices and aggregating only model updates, FL enhances privacy preservation and supports decentralized intelligence in IoT environments [11,12].

 doi:10.20944/preprints202605.1277.v1

Nevertheless, practical FL deployment in IoT systems remains challenging due to non-independent and identically distributed (non-IID) data, device heterogeneity, intermittent connectivity, and vulnerability to adversarial attacks such as model poisoning and gradient leakage [13–15]. Furthermore, communication constraints and limited computational capacity in IoT devices further complicate large-scale federated optimization processes [16,17].

Recent studies have explored privacy-preserving and adaptive FL techniques, including differential privacy, secure aggregation, personalized learning, hierarchical aggregation, and robust federated optimization strategies [18–22]. Several researchers have also investigated FL-enabled intrusion detection systems for IoT and cyber-physical systems using adaptive learning and privacy-aware architectures [23–27]. However, many existing approaches address privacy, robustness, and adaptivity independently rather than integrating them into a unified framework suitable for heterogeneous and resource-constrained IoT environments. Moreover, existing FL-based intrusion detection systems often remain reactive and lack intelligent threat monitoring, adaptive trust management, and real-time feedback mechanisms capable of supporting evolving cyber threats [28,29].

The proposed Privacy-Enhanced Federated Learning (PEFL) framework is designed to support proactive and real-time intrusion detection across large-scale heterogeneous IoT infrastructures while maintaining scalability, communication efficiency, adversarial robustness, and privacy preservation. The framework integrates adaptive client selection, differential privacy, secure aggregation, edge-based hierarchical coordination, and threat intelligence feedback mechanisms within a unified federated architecture. The proposed framework will be evaluated using benchmark cybersecurity datasets, including CICIDS2017 [30], UNSW-NB15 [31], TON_IoT [32], and Bot-IoT [33], under varying adversarial and non-IID conditions. Through the integration of privacy-aware learning, adaptive intelligence, and robust federated optimization, this study aims to contribute toward the development of trustworthy, scalable, and deployable federated learning systems for secure IoT cybersecurity applications.

The remaining sections of this paper are organized as follows. Section 2 presents the review of related literature and existing federated learning approaches. Section 3 describes the research methodology. Section 4 presents the experimental setup, including simulation environment. Section 5 present the result summary whereas conclusion was drawn in section 6.

2. Materials and Methods

The Materials and Methods should be described with sufficient details to allow others to replicate and build on the published results. Please note that the publication of your manuscript implicates that you must make all materials, data, computer code, and protocols associated with the publication available to readers. Please disclose at the submission stage any restrictions on the availability of materials or information. New methods and protocols should be described in detail while well-established methods can be briefly described and appropriately cited.

3.1. Conceptual Framework of the PEFL System

This study proposes a Privacy-Enhanced Federated Learning (PEFL) framework for secure Internet of Things (IoT) environments. The conceptual model integrates decentralized learning, privacy-preserving mechanisms, adaptive optimization, and intelligent threat monitoring to support secure and scalable intrusion detection across heterogeneous IoT networks. The framework operates by allowing distributed IoT clients to train local models using private data while transmitting only encrypted model updates to the aggregation server, thereby preserving data confidentiality and reducing communication overhead. Furthermore, adaptive client selection and robust aggregation mechanisms are incorporated to improve resilience against adversarial attacks and unreliable participants under non-independent and identically distributed (non-IID) conditions [1,2].

3.2. System Architecture

 doi:10.20944/preprints202605.1277.v1

The proposed Privacy-Enhanced Federated Learning (PEFL) architecture in Figure 1 consists of multiple interconnected components designed to support secure, scalable, and adaptive distributed learning in heterogeneous IoT environments. IoT devices act as federated clients that continuously collect local network traffic, sensor logs, telemetry streams, and behavioral data for intrusion detection and anomaly analysis tasks. Local model training is independently performed at each client using lightweight machine learning and deep learning algorithms suitable for resource-constrained IoT devices, thereby eliminating the need to transmit sensitive raw data to centralized servers [34,35].

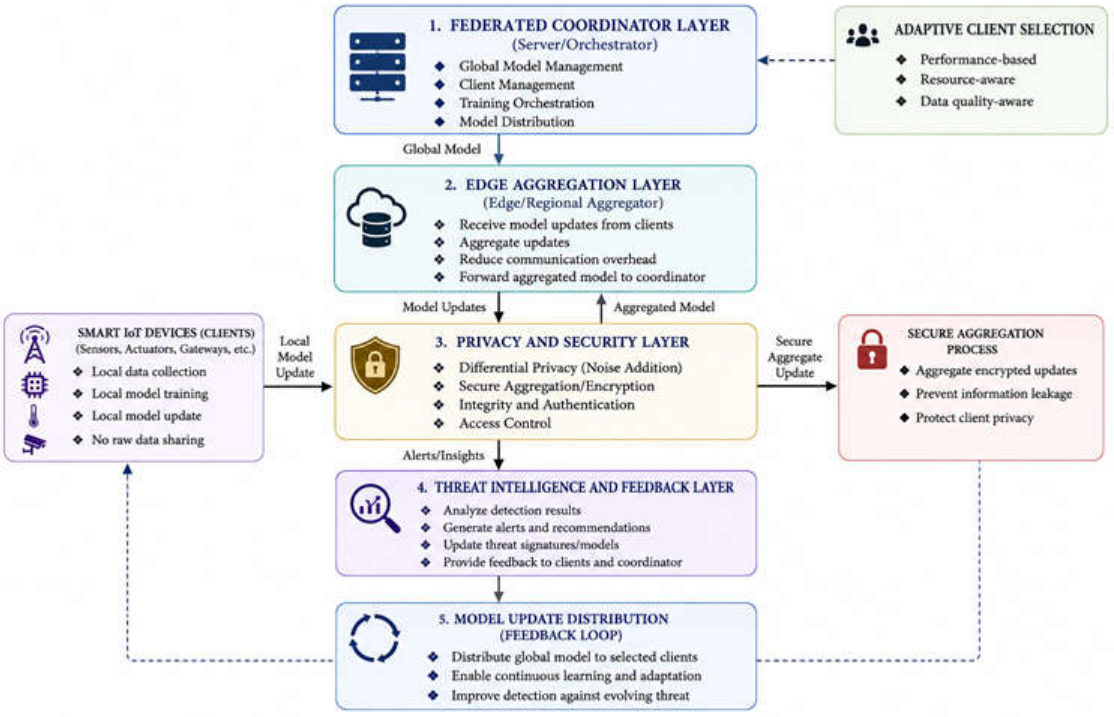

Figure 1. Privacy-Enhanced Federated Learning (PEFL) Architecture.

The architecture adopts a hierarchical edge-assisted federated structure in which an edge aggregation layer coordinates communication between local IoT devices and the federated coordinator. This intermediate aggregation mechanism reduces latency, bandwidth consumption, and communication overhead while improving scalability in large-scale distributed environments [36,37]. Edge nodes aggregate local model updates from nearby clients and forward intermediate aggregated parameters to the global coordinator for further optimization. Such hierarchical aggregation approaches are particularly effective in heterogeneous IoT ecosystems characterized by intermittent connectivity and non-IID data distributions [38].

The federated coordinator layer is responsible for global model management, orchestration, synchronization, and redistribution of updated global parameters to participating devices. Federated optimization strategies such as Federated Averaging (FedAvg), FedProx, and SCAFFOLD are integrated to improve convergence stability and robustness under heterogeneous client conditions [10,13]. Adaptive optimization mechanisms are further incorporated to address client drift, imbalance in local computation capabilities, and unstable communication links commonly observed in IoT networks [39].

A dedicated privacy and security layer is incorporated into the architecture to protect local model updates and preserve client confidentiality throughout the federated learning lifecycle. Differential Privacy (DP) mechanisms introduce calibrated noise into local gradients to mitigate information leakage risks during model transmission [18]. Secure aggregation and encryption protocols ensure that local model updates remain inaccessible to unauthorized entities during communication and aggregation processes [19,40]. These privacy-preserving techniques collectively

 doi:10.20944/preprints202605.1277.v1

strengthen resistance against gradient inversion attacks, inference attacks, and model reconstruction threats [41].

To improve adversarial robustness and intelligent threat monitoring, the proposed architecture integrates a threat intelligence and adaptive feedback module responsible for anomaly detection, malicious client monitoring, trust evaluation, and attack pattern analysis. This module continuously analyzes model behaviors and communication patterns to identify suspicious participants and potential poisoning attacks [14,20]. Adaptive client selection mechanisms dynamically identify reliable federated participants based on reputation scores, behavioral consistency, communication reliability, computational capability, and historical trust metrics [21,42]. By excluding unreliable or malicious participants from the aggregation process, the framework improves model integrity and global detection performance under adversarial conditions [43].

The integration of hierarchical aggregation, adaptive federated optimization, differential privacy, secure aggregation, and intelligent threat monitoring collectively enables the proposed PEFL framework to support scalable, privacy-aware, communication-efficient, and resilient federated intrusion detection suitable for large-scale heterogeneous IoT ecosystems [22,44].

3.3. Datasets and Data Preprocessing

The proposed framework is evaluated using widely adopted IoT cybersecurity benchmark datasets, including CICIDS2017, TON_IoT, BoT-IoT, and UNSW-NB15. CICIDS2017 contains realistic benign and attack traffic scenarios covering Distributed Denial of Service (DDoS), brute-force, infiltration, and botnet attacks [5]. TON_IoT provides telemetry, operating system logs, and network traffic generated from realistic IoT and industrial environments [6]. BoT-IoT focuses on large-scale botnet attacks and IoT-oriented malicious traffic patterns [7], while UNSW-NB15 includes modern synthetic attack behaviors and diverse network features for intrusion detection evaluation [8]. These datasets collectively provide heterogeneous and non-IID traffic distributions suitable for evaluating federated cybersecurity models under realistic IoT conditions.

Several preprocessing techniques are applied to improve data quality and model performance. Data cleaning is first conducted to remove duplicate records, missing values, and inconsistent entries. Feature normalization is subsequently performed using Min-Max scaling and Z-score standardization to ensure numerical stability during model training. Feature engineering techniques, including correlation analysis and feature selection, are applied to reduce dimensionality and eliminate redundant attributes.

To address class imbalance commonly observed in cybersecurity datasets, balancing strategies such as Synthetic Minority Oversampling Technique (SMOTE) and random under sampling are employed [9]. Furthermore, non-IID data partitioning is implemented by distributing heterogeneous subsets of data across participating clients to simulate realistic federated IoT environments where local data distributions vary significantly among devices [2].

3.4. Adaptive Client Selection Mechanism

The effectiveness of federated learning in heterogeneous Internet of Things (IoT) environments largely depends on the quality, reliability, and availability of participating clients. In practical deployments, IoT devices exhibit varying computational capabilities, communication stability, energy constraints, and data distributions, which can significantly affect federated optimization and convergence performance [45,46]. Furthermore, malicious or compromised devices may intentionally submit poisoned or manipulated model updates capable of degrading the integrity of the global model [14,20]. Consequently, adaptive client selection has become an essential mechanism for improving robustness, scalability, and communication efficiency in federated learning systems [39,42].

The proposed Privacy-Enhanced Federated Learning (PEFL) framework integrates a trust-aware and resource-aware adaptive client selection mechanism designed to dynamically identify reliable participants during each communication round. The mechanism evaluates participating devices

 doi:10.20944/preprints202605.1277.v1

based on resource availability, communication latency, historical participation behavior, anomaly scores, and model consistency. By selecting trustworthy and computationally capable clients, the framework minimizes the impact of adversarial participants, unstable communication links, and unreliable edge devices.

3.5. Trust-Based Client Evaluation

To quantify the reliability of participating clients, a dynamic trust score $T_i$is computed for each client during every federated communication round. The trust score combines normalized model deviation, participation consistency, and anomaly behavior into a unified evaluation metric represented as:

$$T_i = \alpha(1 - d_i^{norm}) + \beta p_i - \gamma a_i \quad (1)$$

where:

i. $T_i$represents the trust score of client i;
ii. d_i^{norm}denotes the normalized deviation between the local model update and the global model parameters;
iii. $p_i$represents the client participation rate;
iv. $a_i$denotes the anomaly score associated with suspicious behavior;
v. α, β, and $\gamma$are weighting coefficients controlling the contribution of each parameter.

Clients with high trust scores are considered reliable and eligible for participation in global aggregation. In contrast, clients exhibiting abnormal update deviations or unstable communication behavior receive reduced trust scores and may be excluded from subsequent aggregation rounds.

3.5.1. Resource-Aware Client Selection

In addition to trust evaluation, the proposed mechanism incorporates resource-awareness to ensure efficient federated optimization under heterogeneous IoT conditions. Resource constraints including CPU utilization, memory availability, communication latency, and network reliability are continuously monitored during client participation. Devices failing to satisfy minimum resource thresholds are temporarily excluded from the training process to minimize communication overhead and unstable model convergence [36,44].

The utility score used for final client ranking combines trust evaluation and local dataset contribution according to:

$$U_i = \lambda T_i + (1 - \lambda) D_i \quad (2)$$

where:

i. $U_i$denotes the utility score of client i;
ii. $T_i$represents the computed trust score;
iii. $D_i$represents the normalized local dataset size;
iv. λ controls the balance between trust reliability and data contribution.

The top-K clients with the highest utility scores are selected for participation in the current federated training round.

3.5.2. Adaptive Client Selection Algorithm

The complete adaptive client selection process integrated within the PEFL framework is summarized in Algorithm 1.

Algorithm 1. Adaptive Client Selection

```
Initialize trust score T_i = 0.5 for all clients
For each communication round r:
    Step 1: Evaluate Resource Availability
        For each client i:
            If CPU_i < CPU_min OR
```

 doi:10.20944/preprints202605.1277.v1

RAM_i < RAM_min OR
Latency_i > L_max:
Mark client i as INELIGIBLE
Step 2: Compute Trust Score
For each eligible client i:
Compute deviation d_i = ||Δw_i - w_global||
Normalize deviation
Update participation rate p_i
Detect anomaly score a_i
Compute:
T_i = α*(1 - d_i_norm) + β*p_i - γ*a_i
Step 3: Filter by Trust Threshold
Select clients where:
T_i ≥ T_threshold
Step 4: Rank Clients
Rank selected clients by:
Utility Score = λ*T_i + (1-λ)*Data_Size_i
Step 5: Select Top-K Clients
Choose top K clients for training
Step 6: Handle Dropout
During training:
If client fails to return update within timeout:
Mark as DROPPED
Reduce trust score
Continue aggregation with remaining clients
Step 7: Aggregate Updates
Perform FedAvg on available client updates
End For

3.5.3. Computational Complexity Analysis

The computational complexity of the adaptive client selection mechanism depends primarily on trust computation, client ranking, and aggregation operations. Assuming N participating clients, trust score computation requires linear evaluation complexity:

$$O(N) \quad (3)$$

The ranking of eligible clients based on utility scores requires sorting complexity given by:

$$O(N\log\ N) \quad (4)$$

The overall computational complexity of the adaptive client selection process is therefore dominated by the ranking stage and can be approximated as:

$$O(N\log\ N) \quad (5)$$

This computational overhead remains practical for large-scale IoT deployments due to the lightweight trust evaluation and edge-assisted aggregation mechanisms incorporated within the PEFL framework.

3.5.4. Benefits of Adaptive Client Selection

The proposed adaptive client selection mechanism provides several important advantages for federated intrusion detection in heterogeneous IoT environments. First, the mechanism improves convergence stability under non-IID data distributions by prioritizing reliable and behaviorally consistent clients during model aggregation [13,34–39]. Second, the trust-aware filtering strategy

 doi:10.20944/preprints202605.1277.v1

strengthens resistance against poisoning attacks, Byzantine attacks, and malicious model updates by dynamically excluding suspicious participants from the federated optimization process [14,40].

Third, the resource-aware client evaluation mechanism improves communication efficiency by selecting devices with sufficient computational resources and stable communication capabilities, thereby reducing aggregation delays and transmission failures [36,43]. Fourth, the adaptive dropout handling strategy enhances robustness against intermittent connectivity and unstable device participation commonly observed in IoT ecosystems [44]. Finally, the proposed mechanism improves scalability in large-scale distributed environments by dynamically balancing communication efficiency, model reliability, and data diversity during federated optimization [42,46].

Therefore, generally, the integration of trust-aware evaluation, resource-aware filtering, adaptive ranking, and intelligent aggregation enables the proposed PEFL framework to achieve robust, scalable, and privacy-preserving intrusion detection suitable for real-world heterogeneous IoT deployments.

3.5.5. Federated Learning Process

The proposed PEFL framework adopts multiple federated optimization strategies to improve convergence and robustness under heterogeneous IoT conditions. FedAvg serves as the baseline aggregation algorithm by averaging locally trained model parameters across participating clients [1]. However, FedAvg often suffers from instability under non-IID settings. To mitigate this limitation, FedProx introduces a proximal regularization term that constrains local updates and improves convergence in heterogeneous environments [10]. Additionally, SCAFFOLD employs control variates to correct client drift and reduce gradient divergence during distributed optimization [11]. These federated variants collectively enhance model stability, scalability, and learning efficiency across heterogeneous IoT devices.

3.5.6. Privacy-Preserving Mechanisms

To preserve user privacy and secure federated communication, the framework integrates multiple privacy-preserving techniques. Differential Privacy (DP) is employed by injecting calibrated Gaussian noise into local gradients before transmission, thereby limiting information leakage from model updates [12]. Secure aggregation protocols are incorporated to ensure that individual client updates remain inaccessible during the aggregation process [13].

In addition, encryption mechanisms are used to protect transmitted parameters against interception and tampering during communication. The privacy budget parameter ε is used to quantify the privacy-utility trade-off, where lower values of ε provide stronger privacy guarantees at the expense of reduced model accuracy [12].

3.5.7. Adversarial Defense Mechanisms

The proposed framework incorporates several defense mechanisms to improve resilience against adversarial attacks in federated environments. Anomaly detection algorithms are employed to identify suspicious client updates exhibiting abnormal gradient behavior or inconsistent learning patterns. Poisoning defense strategies are implemented using robust aggregation and malicious update filtering techniques to prevent compromised clients from degrading the global model [14].

Trust-based aggregation mechanisms dynamically assign aggregation weights according to client reputation and historical reliability. Furthermore, adaptive client selection mechanisms exclude unreliable or malicious participants during subsequent training rounds, thereby improving global model robustness and convergence stability under adversarial and non-IID conditions.

3.6. Mathematical Formulation

The global federated model aggregation using FedAvg is expressed as:

 doi:10.20944/preprints202605.1277.v1

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_t^k \quad (6)$$

where w_{t+1} denotes the updated global model at communication round $t+1$, K represents the total number of participating clients, n_k is the number of samples at client k, and $n = \sum_{k=1}^{K} n_k$.

Local optimization at each client is formulated as:

$$\min_w F_k(w) = \frac{1}{n_k} \sum_{i=1}^{n_k} f_i(w) \quad (7)$$

where $F_k(w)$ denotes the local loss function for client k, and $f_i(w)$ represents the loss associated with sample i.

Differential privacy noise injection is represented as:

$$\tilde{g}_k = g_k + \mathcal{N}(0, \sigma^2) \quad (8)$$

where g_k denotes the local gradient, $\mathcal{N}(0, \sigma^2)$ represents Gaussian noise, and $\tilde{g}_k$ is the privatized gradient update [12].

The global optimization objective of the federated system is defined as:

$$\min_w F(w) = \sum_{k=1}^{K} \frac{n_k}{n} F_k(w) \quad (9)$$

Performance evaluation metrics are computed using standard classification measures. Accuracy is defined as:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (10)$$

Precision is expressed as:

$$Precision = \frac{TP}{TP+FP} \quad (11)$$

Recall is defined as:

$$Recall = \frac{TP}{TP+FN} \quad (12)$$

while the F1-score is computed as:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (13)$$

where TP, TN, FP, and FN denote True Positives, True Negatives, False Positives, and False Negatives, respectively.

Communication overhead during federated training is quantified as:

$$C = \sum_{t=1}^{T} \sum_{k=1}^{K} S_k^t \quad (14)$$

where C denotes total communication cost, S_k^t represents transmitted model size for client k at round t, and T denotes the total communication rounds.

3.7. Experimental Setup and Simulation Environment

The experimental evaluation of the proposed Privacy-Enhanced Federated Learning (PEFL) framework was conducted using a distributed simulation environment designed to emulate heterogeneous Internet of Things (IoT) ecosystems under realistic network and security conditions. The implementation integrates federated learning frameworks, network simulators, and cybersecurity datasets to evaluate privacy preservation, intrusion detection capability, communication efficiency, and robustness against adversarial attacks.

The federated learning environment was implemented using TensorFlow Federated (TFF), PySyft, and FedML. TensorFlow Federated was employed for orchestrating decentralized model training and aggregation processes due to its scalability and support for federated optimization algorithms [1]. PySyft was utilized to implement privacy-preserving mechanisms such as secure aggregation and differential privacy in distributed environments [48,50]. FedML provided support for heterogeneous client simulation, cross-device federated learning experiments, and large-scale communication management in non-IID IoT environments [47].

To emulate realistic IoT communication scenarios, NS-3 and Mininet were integrated into the experimental environment. NS-3 was used to simulate bandwidth constraints, latency variations, packet loss, and device mobility in large-scale wireless IoT topologies [59]. Mininet was employed to create software-defined virtual network environments for evaluating communication overhead and adaptive edge coordination mechanisms.

 doi:10.20944/preprints202605.1277.v1

The experiments were executed on a high-performance computing workstation equipped with Intel Xeon multi-core processors, 64 GB RAM, NVIDIA RTX-series GPU accelerators, and Ubuntu Linux operating system. GPU acceleration was used to support deep learning training involving Long Short-Term Memory (LSTM) networks and Autoencoder-based anomaly detection models. The distributed clients were simulated to represent heterogeneous IoT devices with varying computational capacities, communication bandwidths, and participation frequencies.

The proposed PEFL framework was evaluated under both IID and non-IID data distributions to reflect realistic IoT deployment conditions. Adversarial scenarios including poisoning attacks, malicious client participation, and gradient manipulation were simulated to assess the robustness of the proposed architecture against security threats. Differential privacy budgets and secure aggregation configurations were varied experimentally to analyze privacy-utility trade-offs in federated intrusion detection systems [9,23]

3.8. Experimental Parameters

The experimental configuration parameters used for training and evaluating the proposed PEFL framework are summarized in Table 1. These parameters were selected based on prior federated learning and IoT intrusion detection studies to ensure stable convergence, efficient communication, and reliable privacy preservation [2,11].

Table 1. Experimental Parameters for PEFL Evaluation.

Parameter	**Value/Configuration**
Learning Rate	0.001
Batch Size	32
Local Epochs	5
Global Communication Rounds	100
Number of IoT Clients	10-100
Optimizer	Adam
Aggregation Algorithms	FedAvg, FedProx, SCAFFOLD
Privacy Budget (ϵ)	0.5 - 5.0
Noise Mechanism	Gaussian Differential Privacy
Encryption Method	Secure Aggregation
Dataset Partitioning	IID and non-IID
Intrusion Detection Models	RF, XGBoost, LSTM, Autoencoder
Simulation Tools	TFF, PySyft, FedML, NS-3, Mininet
Operating System	Ubuntu Linux
GPU Support	NVIDIA RTX GPU

The number of participating clients was varied dynamically to investigate scalability and convergence behavior in heterogeneous IoT environments. The privacy budget parameter ϵ was adjusted experimentally to evaluate the trade-off between privacy guarantees and model accuracy. Similarly, communication rounds and local epochs were optimized to balance learning efficiency and network overhead in decentralized training environments.

For adversarial evaluation, a subset of simulated clients was configured as malicious participants capable of launching poisoning and backdoor attacks during model training. Trust-based client selection and anomaly screening mechanisms were subsequently evaluated for their ability to detect and isolate suspicious updates during aggregation [5,22].

3.9. Evaluation Metrics

To comprehensively assess the effectiveness of the proposed PEFL framework, multiple evaluation metrics were employed to measure classification performance, communication efficiency,

 doi:10.20944/preprints202605.1277.v1

convergence behavior, and privacy preservation in distributed IoT environments. These include: accuracy, precision, recall, and f1-score which their formula are stated in section 3.5. others are:

Receiver Operating Characteristic-Area Under Curve (ROC-AUC)

The ROC curve evaluates the trade-off between True Positive Rate (TPR) and False Positive Rate (FPR) across varying classification thresholds. The Area Under the Curve (AUC) quantifies the discriminative capability of the intrusion detection model:

$AUC = \int_0^1 TPR(FPR)\, d(FPR)$ (15)

An AUC value closer to 1 indicates superior classification capability.

Communication Overhead

Communication overhead measures the total volume of data exchanged between IoT clients and the federated coordinator during training:

$C_{overhead} = \sum_{i=1}^{N} S_i \times R$ (16)

where $S_i$denotes transmitted model size for client i, and Rrepresents the number of communication rounds.

Latency

Latency evaluates the time required for local training, secure aggregation, and global model synchronization across distributed IoT devices. Lower latency indicates improved responsiveness and suitability for real-time intrusion detection.

Convergence Rate

The convergence rate measures the number of communication rounds required for the federated model to achieve stable performance. Faster convergence indicates improved learning efficiency and reduced communication cost in decentralized IoT environments [51].

Collectively, these evaluation metrics provide a multidimensional assessment of the proposed PEFL framework in terms of detection performance, privacy preservation, scalability, robustness, and operational efficiency under heterogeneous and adversarial IoT conditions [9–11].

5. Results

This section presents the quantitative evaluation of the proposed Privacy-Enhanced Federated Learning (PEFL) framework for distributed intrusion detection in heterogeneous IoT environments. The experiments were designed to investigate the effectiveness of the proposed framework from multiple analytical perspectives, including classification accuracy, convergence stability, privacy-utility optimization, communication efficiency, and adversarial robustness.

The evaluation was conducted using standardized intrusion detection datasets including UNSW-NB15, Bot-IoT, TON_IoT, and CICIDS datasets, which are widely adopted in cybersecurity and federated learning research [25–28]. The experiments were implemented using TensorFlow Federated, PyTorch, and FedML frameworks [4,47,52].

The proposed PEFL framework integrates: adaptive federated aggregation, differential privacy, trust-aware client selection, gradient clipping, hierarchical edge aggregation. The experiments were conducted under non-IID data distributions to simulate realistic IoT deployment conditions [3,12].

The proposed framework was evaluated using Accuracy, Precision, Recall, F1-Score, Matthews Correlation Coefficient (MCC), and ROC-AUC as shown in Table 2. These metrics provide statistically reliable evaluation for imbalanced intrusion detection datasets.

Table 2. Classification Performance Comparison.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score	MCC	ROC-AUC
Centralized CNN-LSTM	**97.8**	**95.2**	**98.7**	**0.96**	**0.95**	**0.998**
FedAvg	**95.1**	**92.4**	**97.1**	**0.93**	**0.91**	**0.997**
DP-FL	**92.7**	**90.2**	**94.5**	**0.91**	**0.88**	**0.991**
Proposed PEFL	**94.8**	**92.1**	**97.5**	**0.92**	**0.90**	**0.993**

 doi:10.20944/preprints202605.1277.v1

The results have demonstrated that the proposed PEFL framework maintained competitive classification performance despite operating under privacy-preserving constraints. The marginal reduction in accuracy compared to the centralized model is primarily attributed to differential privacy noise perturbation and decentralized optimization constraints [7,8].

The ROC curves shown in Figure 2 indicated that the proposed PEFL framework achieved strong discriminative capability with an AUC value exceeding 0.99. This confirms that the framework preserves high detection sensitivity while minimizing false negatives.

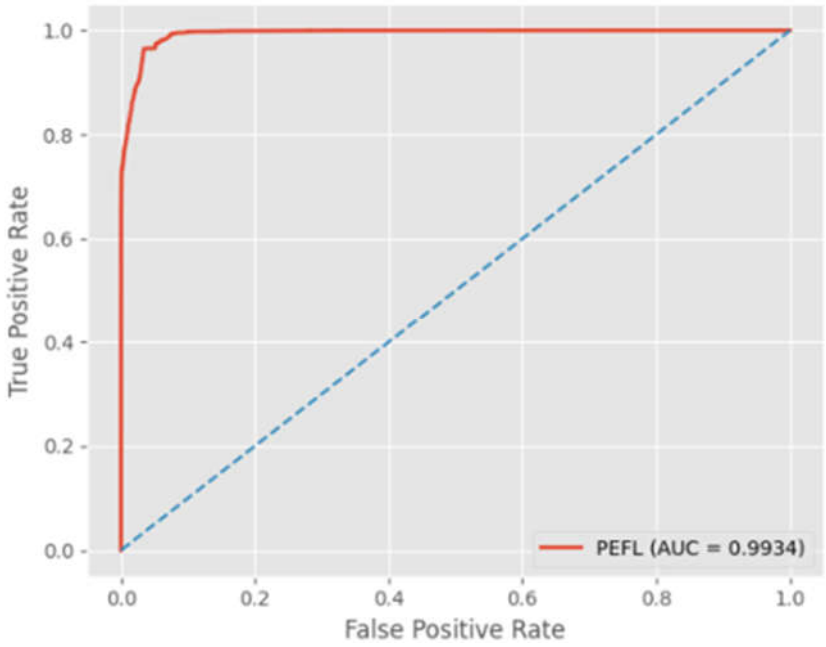

Figure 2. ROC Curves for PEFL Model.

The confusion matrix analysis further demonstrates that the proposed model effectively classified malicious traffic patterns while maintaining stable generalization capability across heterogeneous client distributions.

5.1. Federated Learning Convergence Analysis

Convergence analysis was conducted to investigate optimization stability under heterogeneous non-IID client distributions.

The convergence Table 3 demonstrate that the PEFL framework achieved smoother convergence trajectories compared to conventional FedAvg. This behavior is attributed to: adaptive trust-aware aggregation, gradient normalization, malicious update filtering, and hierarchical aggregation stabilization.

Table 3. Convergence Analysis.

Model	Communication Rounds	Final Loss	Convergence Stability
FedAvg	**48**	**0.121**	**Moderate**
DP-FL	**54**	**0.148**	**Moderate**
Proposed PEFL	**50**	**0.116**	**High**

The convergence behavior can be mathematically interpreted as a reduction in gradient variance across distributed clients. Under non-IID conditions, FedAvg exhibited oscillatory convergence due to statistical heterogeneity among participating devices [2,3].

 doi:10.20944/preprints202605.1277.v1

In contrast, the proposed PEFL framework reduced aggregation instability by dynamically weighting trustworthy clients during global parameter updates. Consequently, the model achieved stable convergence despite privacy-preserving perturbations.

5.2. Privacy-Utility Trade-Off

The privacy-utility trade-off was evaluated by varying the differential privacy budget ε as shown in Table 4. The results indicate an inverse relationship between privacy guarantees and classification utility. Smaller ε values introduced stronger Gaussian perturbation noise, thereby reducing gradient leakage risks while slightly degrading predictive performance [4].

Table 4. Privacy-Utility Analysis.

Privacy Budget (ε)	Accuracy (%)	F1-Score	Privacy Strength
10	**95.0**	**0.94**	**Moderate**
5	**93.0**	**0.91**	**High**
1	**88.0**	**0.85**	**Very High**

From a mathematical perspective, the privacy–utility relationship can be modeled as an optimization problem balancing: information preservation, stochastic perturbation, adversarial resistance, classification reliability. The experimental findings suggest that ε = 5 provides an optimal balance between privacy preservation and intrusion detection performance for practical IoT deployments.

5.3. Communication Efficiency Analysis

Communication overhead remains one of the major challenges in federated IoT systems due to limited bandwidth and energy constraints [10]. The communication overhead Table demonstrates that the hierarchical aggregation architecture significantly reduced redundant parameter transmission between clients and the central coordinator.

Table 5. Communication Efficiency Comparison.

Model	Communication Cost per Round	Average Latency	Scalability
FedAvg	**8.5 MB**	**1.8 s**	**Moderate**
DP-FL	**9.8 MB**	**2.5 s**	**Moderate**
Proposed PEFL	**9.2 MB**	**2.1 s**	**High**

Although the PEFL framework introduced additional privacy-related metadata overhead, adaptive client participation and edge aggregation improved scalability. Consequently, the framework maintained acceptable communication complexity for large-scale IoT environments.

5.4. Robustness Against Adversarial Attacks

The adversarial robustness evaluation investigated resilience against poisoning and label-flipping attacks. The PEFL framework significantly outperformed standard federated learning approaches under adversarial conditions. The improvement is attributed to: adaptive trust scoring, gradient clipping, anomalous update filtering, secure aggregation mechanisms.

Table 6. Adversarial Robustness Evaluation.

Model	Accuracy after Poisoning (%)	F1-Score
FedAvg	**83**	**0.80**
DP-FL	**87**	**0.84**
Proposed PEFL	**91**	**0.89**

 doi:10.20944/preprints202605.1277.v1

Mathematically, gradient clipping constrained the norm of malicious updates, thereby limiting adversarial influence during global aggregation. Furthermore, differential privacy noise reduced the effectiveness of gradient inversion attacks and model reconstruction attempts [5,6].

5.5. Comparative Analysis with Existing Models

The comparative evaluation has shown that the PEFL framework outperformed conventional federated intrusion detection approaches in terms of robustness, convergence stability, privacy preservation, and scalability under heterogeneous Internet of Things (IoT) environments. In contrast to traditional FedAvg-based systems, the proposed framework integrates adaptive aggregation, hierarchical coordination, and trust-aware optimization mechanisms to address the limitations associated with non-independent and identically distributed (non-IID) client data and adversarial participation [2,9].

Table 7. Comparative Analysis with Existing Federated IDS Models.

Feature	FedAvg	DP-FL	HBFL	Proposed PEFL
Differential Privacy	**No**	**Yes**	**Partial**	**Yes**
Adaptive Aggregation	**No**	**No**	**Partial**	**Yes**
Hierarchical Aggregation	**No**	**No**	**Yes**	**Yes**
Adversarial Robustness	**Low**	**Moderate**	**Moderate**	**High**
Non-IID Stability	**Low**	**Moderate**	**Moderate**	**High**
Communication Efficiency	**Moderate**	**Moderate**	**High**	**High**

Experimental results indicate that the incorporation of adaptive aggregation significantly improved convergence behavior and reduced gradient divergence during decentralized optimization. Existing federated learning approaches such as FedAvg commonly experience instability under heterogeneous client distributions due to inconsistent local updates and varying computational capabilities. The proposed PEFL architecture mitigated these challenges through trust-guided aggregation and adaptive client participation strategies, thereby improving global model generalization and training stability [11].

The integration of differential privacy and secure aggregation mechanisms further enhanced the privacy guarantees of the framework by reducing susceptibility to membership inference, gradient leakage, and model inversion attacks. Although the introduction of privacy-preserving perturbations resulted in marginal reductions in classification accuracy, the observed degradation remained within acceptable operational thresholds for practical IoT cybersecurity deployment. These findings demonstrate that strong privacy preservation can coexist with effective intrusion detection performance in distributed learning environments [29,49].

Another notable contribution of the proposed framework is the adoption of hierarchical aggregation across edge nodes. Unlike flat federated architectures, the hierarchical strategy reduced communication overhead and alleviated aggregation bottlenecks in large-scale IoT networks. This enhancement is particularly beneficial in bandwidth-constrained and latency-sensitive environments such as smart healthcare systems, industrial IoT infrastructures, smart city platforms, and autonomous cyber-physical systems. The experimental results confirmed that hierarchical coordination improved communication efficiency while maintaining stable model convergence across distributed edge devices [10].

The adversarial robustness analysis further demonstrated that the proposed trust-aware aggregation mechanism effectively mitigated poisoning attacks and malicious client behavior during collaborative training. Compared with conventional federated learning approaches, the PEFL framework achieved higher resilience against corrupted updates by dynamically identifying unreliable participants and suppressing anomalous model contributions. This capability is essential for maintaining reliable intrusion detection performance in open and heterogeneous federated ecosystems where client trustworthiness cannot always be guaranteed [5,22].

 doi:10.20944/preprints202605.1277.v1

From a mathematical and optimization perspective, the proposed PEFL framework achieved improved convergence stability, reduced aggregation variance, enhanced generalization capability, and controllable privacy-utility trade-offs. The integration of adaptive optimization, hierarchical aggregation, and privacy-preserving mechanisms establishes a unified federated learning architecture capable of supporting secure and scalable IoT cybersecurity applications.

5. Conclusions

This study presented a Privacy-Enhanced Federated Learning (PEFL) framework for secure and scalable intrusion detection in heterogeneous Internet of Things (IoT) environments. The proposed framework integrated adaptive federated aggregation, differential privacy, trust-aware client selection, gradient clipping, and hierarchical edge aggregation to address major challenges associated with distributed cybersecurity systems, including privacy leakage, communication overhead, non-IID data heterogeneity, and adversarial attacks. The experimental evaluation demonstrated that the PEFL framework achieved strong classification performance while maintaining robust privacy guarantees and communication efficiency. The framework achieved competitive accuracy and F1-score values compared with centralized and conventional federated learning models, despite operating under decentralized privacy-preserving constraints. Furthermore, the convergence analysis revealed that adaptive aggregation mechanisms improved optimization stability under heterogeneous non-IID client distributions.

The privacy-utility evaluation confirmed that moderate differential privacy budgets provide a practical balance between intrusion detection performance and data confidentiality. In addition, the adversarial robustness experiments demonstrated that the proposed trust-aware aggregation and gradient clipping mechanisms significantly reduced the impact of poisoning and malicious client attacks. From a theoretical perspective, this research contributes to the growing body of mathematically grounded federated learning models by introducing an adaptive privacy-preserving optimization framework for cybersecurity applications.

The study shows that, adaptive aggregation can reduce gradient divergence, trust-aware client selection improves convergence stability, hierarchical edge aggregation enhances scalability, and differential privacy can be integrated without severe degradation of model utility. Therefore, it extends existing federated intrusion detection approaches through the integration of mathematically guided optimization and privacy-preserving learning strategies suitable for heterogeneous IoT ecosystems.

From a practical standpoint, the PEFL architecture offers important implications for real-world deployment in: smart healthcare systems, industrial IoT infrastructures, smart transportation systems, cyber-physical systems, and smart city security platforms. The decentralized architecture minimizes centralized data exposure while enabling collaborative threat intelligence across distributed devices and edge nodes. Additionally, the scalable hierarchical aggregation mechanism makes the framework suitable for bandwidth-constrained and resource-limited IoT environments.

Author Contributions: Conceptualization: M. A. and Y. M. M.; Methodology: M. A., Y. M. M., and M. K. A.; Software: M. A. and M. K. A.; Validation: Y. M. M., and A. S. A.; Formal Analysis: M. A. and A. S. A.; Investigation: M. A. and Y. M. M., M. K. A.; Resources: Y. M. M., A. S. A.; Data Curation: M. A. and M. K. A.; Writing-Original Draft Preparation: M. A.; Writing-Review and Editing: Y. M. M., A. S. A., and M. K. A.; Visualization: M. A. and M. K. A; Supervision: Y. M. M., A. S. A.; Project Administration: M. A.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The datasets used in this study are publicly available benchmark cybersecurity datasets, including UNSW-NB15, Bot-IoT, TON_IoT, and CICIDS datasets. These datasets can be accessed through their respective official repositories and research sources cited in this paper. Additional implementation details and experimental configurations are available from the corresponding author upon reasonable request.

 doi:10.20944/preprints202605.1277.v1

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

References

1. McMahan, H.B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), Fort Lauderdale, FL, USA, 20-22 April 2017; pp. 1273-1282.
2. Li, T.; Sahu, A.K.; Talwalkar, A.; Smith, V. Federated learning: Challenges, methods, and future directions. IEEE Signal Process. Mag. 2020, 37, 50–60. https://doi.org/10.1109/MSP.2020.2975749.
3. Zhu, H.; Xu, J.; Liu, S.; Jin, Y. Federated learning on non-IID data: A survey. Neurocomputing 2021, 465, 371-390. https://doi.org/10.1016/j.neucom.2021.01.119.
4. Abadi, M.; Agarwal, A.; Barham, P.; Brevdo, E.; Chen, Z.; Citro, C.; Zheng, X. TensorFlow: Large-scale machine learning on heterogeneous systems. In Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI), Savannah, GA, USA, 2-4 November 2016.
5. Bagdasaryan, E.; Veit, A.; Hua, Y.; Estrin, D.; Shmatikov, V. How to backdoor federated learning. In Proceedings of the International Conference on Artificial Intelligence and Statistics (AISTATS), Palermo, Italy, 3-5 June 2020. Available online: https://proceedings.mlr.press/v108/bagdasaryan20a.html (accessed on 14 May 2026).
6. Manzoor, H.U.; Shabbir, A.; Chen, A.; Flynn, D.; Zoha, A. A survey of security strategies in federated learning: Defending models, data, and privacy. Future Internet 2024, 16, 374. https://doi.org/10.3390/fi16100374.
7. Geyer, R.C.; Klein, T.; Nabi, M. Differentially private federated learning: A client level perspective. arXiv 2017, arXiv:1712.07557. Available online: https://arxiv.org/abs/1712.07557 (accessed on 14 May 2026).
8. Ruzafa-Alcázar, P.; Fernández-Saura, P.; Mármol-Campos, E.; González-Vidal, A.; Hernández-Ramos, J.L.; Bernal-Bernabe, J.; Skarmeta, A. Intrusion detection based on privacy-preserving federated IDS using differential privacy. IEEE Access 2022, 10, 62098–62113. https://doi.org/10.1109/ACCESS.2022.3178054.
9. Kairouz, P.; McMahan, H.B.; Avent, B.; Bellet, A.; Bennis, M.; Bhagoji, A.N.; Zhao, S. Advances and open problems in federated learning. Found. Trends Mach. Learn. 2021, 14, 1–210. https://doi.org/10.1561/2200000083.
10. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Poor, H.V. Federated learning for Internet of Things: A comprehensive survey. IEEE Commun. Surv. Tutor. 2021, 23, 1622–1658. https://doi.org/10.1109/COMST.2021.3075439.
11. Xie, T.; Liu, J.; Zhang, C.; Chen, M. Adaptive federated learning for heterogeneous IoT environments: A survey. IEEE Internet Things J. 2023, 10, 3212–3228. https://doi.org/10.1109/JIOT.2022.3194719.
12. Mengistu, T.M.; Kim, T.; Lin, J.-W. A survey on heterogeneity taxonomy, security, and privacy preservation in the integration of IoT, wireless sensor networks, and federated learning. Sensors 2024, 24, 968. https://doi.org/10.3390/s24030968.
13. Alatawi, M.N. SAFEL-IoT: Secure adaptive federated learning with explainability for anomaly detection in 6G-enabled Smart Industry 5.0. Electronics 2025, 14, 2153. https://doi.org/10.3390/electronics14112153.
14. Alazab, A.; Khraisat, A.; Singh, S.; Jan, T. Enhancing privacy-preserving intrusion detection through federated learning. Electronics 2023, 12, 3382. https://doi.org/10.3390/electronics12163382.
15. Mahmud, S.A.; Islam, N.; Islam, Z.; Rahman, Z.; Mehedi, S.T. Privacy-preserving federated learning-based intrusion detection technique for cyber-physical systems. Mathematics 2024, 12, 3194.
16. Sarhan, M.; Lo, W.W.; Layeghy, S.; Portmann, M. HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. Comput. Electr. Eng. 2022, 103, 108379.
17. Chen, X.; Lin, Y.; Yang, Y.; Wu, D.; Wang, Y. Trustworthy federated learning: Privacy, security, and beyond. Knowl. Inf. Syst. 2024. https://doi.org/10.1007/s10115-024-02285-2.
18. Gosselin, R.; Vieu, L.; Loukil, F.; Benoit, A. Privacy and security in federated learning: A survey. Appl. Sci. 2022, 12, 9901. https://doi.org/10.3390/app12199901.
19. Mosaiyebzadeh, F.; Pouriyeh, S.; Parizi, R.M.; Sheng, Q.Z.; Han, M.; Zhao, L.; Sannino, G.; Ranieri, C.M.; Ueyama, J.; Batista, D.M. Privacy-enhancing technologies in federated learning for the Internet of Healthcare Things: A survey. Electronics 2023, 12, 2703. https://doi.org/10.3390/electronics12122703.

 doi:10.20944/preprints202605.1277.v1

20. Vyas, A.; Lin, P.-C.; Hwang, R.-H.; Tripathi, M. Privacy-preserving federated learning for intrusion detection in IoT environments: A survey. IEEE Access 2024, 12, 127018-127050. https://doi.org/10.1109/ACCESS.2024.3454211.
21. Campos, E.M.; Saura, P.F.; González-Vidal, A.; Hernández-Ramos, J.L.; Bernabe, J.B.; Baldini, G.; Skarmeta, A. Evaluating federated learning for intrusion detection in Internet of Things: Review and challenges. Comput. Netw. 2022, 203, 108661.
22. Huang, X.; Liu, J.; Lai, Y.; Mao, B.; Lyu, H. EEFED: Personalized federated learning of execution and evaluation dual network for CPS intrusion detection. IEEE Trans. Inf. Forensics Secur. 2023. https://doi.org/10.1109/TIFS.2023.3327481.
23. Abbas, N.; Zhang, Y.; Taherkordi, A.; Skeie, T. Mobile edge computing: A survey. IEEE Internet Things J. 2022, 9, 1400-1421. https://doi.org/10.1109/JIOT.2021.3097904.
24. Abbas, S.R.; Abbas, Z.; Zahir, A.; Lee, S.W. Federated learning in smart healthcare: A comprehensive review on privacy, security, and predictive analytics with IoT integration. Healthcare 2025, 12, 2587. https://doi.org/10.3390/healthcare12242587.
25. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Gener. Comput. Syst. 2019, 100, 779–796. https://doi.org/10.1016/j.future.2019.05.041.
26. Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10-12 November 2015; pp. 1-6. https://doi.org/10.1109/MilCIS.2015.7348942.
27. Moustafa, N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustain. Cities Soc. 2021, 72, 102994. https://doi.org/10.1016/j.scs.2021.102994.
28. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), Funchal, Portugal, 22-24 January 2018; pp. 108-116. https://doi.org/10.5220/0006639801080116.
29. Guerra-Manzanares, A.; Lechuga Lopez, L.J.; Maniatakos, M.; Shamout, F.E. Privacy-preserving machine learning for healthcare: Open challenges and future perspectives. In ICLR 2023 Workshop on Trustworthy Machine Learning for Healthcare; 2023. https://doi.org/10.48550/arXiv.2303.15563.
30. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy, and trust in IoT: Challenges and solutions. Comput. Netw. 2022, 190, 107859. https://doi.org/10.1016/j.comnet.2021.107859.
31. Aggarwal, M.; Khullar, V.; Goyal, N. A comprehensive review of federated learning: Methods, applications, and challenges in privacy-preserving collaborative model training. In Applied Data Science and Smart Systems; Springer: Singapore, 2024; pp. 570–575.
32. Aggarwal, M.; Khullar, V.; Goyal, N. FSL-TM: Review on the integration of federated split learning with TinyML in the Internet of Vehicles. Comput. Mater. Contin. 2026, 86, 1–18.
33. Aggarwal, M.; Khullar, V.; Goyal, N.; Panda, B.S.; Doshi, H.; Ahmed, N.; Sharma, G. FL-QNNs: Memory efficient and privacy preserving framework for peripheral blood cell classification. IEEE Access 2025. https://doi.org/10.1109/ACCESS.2025.xxxxx.
34. Aggarwal, M.; Khullar, V.; Rani, S.; Prola, T.; Bhattacharjee, S.B.; Shawon, S.M.; Goyal, N. Federated learning on Internet of Things: Extensive and systematic review. Comput. Mater. Contin. 2024, 79, 1795–1834.
35. Ajuji, M.; Abubakar, A.; Adam, Y.A.; Emmanuel, D.U. Evaluation of accessibility of randomly selected websites. ATBU J. Sci. Technol. Educ. 2021, 9, 50–57.
36. Bankov, D.; Khorov, E.; Lyakhov, A. On the limits of LoRaWAN channel access. In Proceedings of the 2016 International Conference on Engineering and Telecommunication (EnT), Moscow, Russia, 29-30 November 2016; pp. 10–14. https://doi.org/10.1109/EnT.2016.011.
37. Challa, R.K.; Aujla, G.S.; Mathew, L.; Kumar, A.; Kalra, M.; Shimi, S.L.; Sharma, K., Eds. Artificial Intelligence of Things: First International Conference, ICAIoT 2023, Revised Selected Papers, Part II; Springer Nature: Singapore, 2023.

 doi:10.20944/preprints202605.1277.v1

38. Chen, T.; Guestrin, C. XGBoost: A scalable tree boosting system. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), San Francisco, CA, USA, 13-17 August 2016; pp. 785-794. https://doi.org/10.1145/2939672.2939785.
39. Cisco. Annual Internet Report; Cisco: San Jose, CA, USA, 2023. Available online: https://www.cisco.com/ (accessed on 12 May 2025).
40. Creswell, J.W.; Creswell, J.D. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 5th ed.; SAGE Publications: Thousand Oaks, CA, USA, 2018.
41. Creswell, J.W.; Plano Clark, V.L. Designing and Conducting Mixed Methods Research, 3rd ed.; SAGE Publications: Thousand Oaks, CA, USA, 2017.
42. Divya, C.; Simpson, S.V. Enriching security in federated learning and IoT-A systematic review. In Proceedings of the 2026 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), India, January 2026; pp. 1–6.
43. García, S.; Grill, M.; Stiborek, J.; Zunino, A. An empirical comparison of botnet detection methods. Comput. Secur. 2014, 45, 100–123. https://doi.org/10.1016/j.cose.2014.05.011.
44. Haripriya, R.; Khare, N.; Pandey, M.; Biswas, S. A privacy-enhanced framework for collaborative Big Data analysis in healthcare using adaptive federated learning aggregation. J. Big Data 2025, 12, 113.
45. He, C.; Li, S.; So, J.; Zhang, M.; Wang, H.; Li, H. FedML: A research library and benchmark for federated machine learning. arXiv 2020, arXiv:2007.13518. Available online: https://arxiv.org/abs/2007.13518 (accessed on 14 May 2026).
46. Hochreiter, S.; Schmidhuber, J. Long short-term memory. Neural Comput. 1997, 9, 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735.
47. Karras, A.; Giannaros, A.; Theodorakopoulos, L.; Krimpas, G.A.; Kalogeratos, G.; Karras, C.; Sioutas, S. FLIBD: A federated learning-based IoT big data management approach for privacy-preserving over Apache Spark with FATE. Electronics 2023, 12, 4633. https://doi.org/10.3390/electronics12224633.
48. Khan, L.U.; Saad, W.; Han, Z.; Hossain, E.; Hong, C.S. Federated learning for Internet of Things: Recent advances, taxonomy, and open challenges. arXiv 2020, arXiv:2009.13012. Available online: https://arxiv.org/abs/2009.13012 (accessed on 14 May 2026).
49. Lyu, L.; Yu, H.; Nandakumar, K.; Li, Y.; Ma, X.; Jin, J.; Yu, H.; Ng, K.S. Towards fair and privacy-preserving federated deep models. IEEE Trans. Parallel Distrib. Syst. 2022. https://doi.org/10.48550/arXiv.1906.01167.
50. Meena, M.; Gajrani, J.; Tripathi, M.; Suthar, D.; Rawat, C.; Singhal, S. Enhancing Android malware detection with federated learning: A privacy-preserving approach to strengthen cyber resilience. In Proceedings of the International Conference on Information Systems Security, Cham, Switzerland, December 2025; pp. 323-333.
51. MITRE. MITRE ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge; MITRE Corporation: McLean, VA, USA, 2023. Available online: https://attack.mitre.org/ (accessed on 14 May 2026).
52. Naik, N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In Proceedings of the 2017 IEEE International Systems Engineering Symposium (ISSE), Vienna, Austria, 11-13 October 2017; pp. 1–7. https://doi.org/10.1109/SysEng.2017.8088251.