International Journal of Computers and Informatics (IJCI)
Vol. (5), No. (6)
IJCI
June 2026
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (5)، العدد (6)

Federated Learning-Based Secure Intrusion Detection Framework for Edge-IoT Communication Systems

Karar Talal
College of Physical Education and Sport Sciences, University of Al-Qadisiyah, Iraq
sporteacher11@qu.edu.iq

Rand Muaffaq Hadi
Department of Communication Techniques, Najaf Technical Institute, Al-Furat Al-Awsat Technical University, Al-Najaf 31001, Iraq
Rand.muaffaq@atu.edu.iq

Abstract

The advent of Edge-Internet of Things (Edge-IoT) communication systems has created a huge cyber security problem with connected devices being heterogeneous, distributed and resource constrained. Centralized intrusion detection systems (IDSs) tend to be data-hungry, impose significant communications overhead, add latency, and have serious privacy concerns. However, due to these limitations, this paper suggests an Edge-IoT Communication Systems Federated Learning-Based Secure Intrusion Detection Framework which facilitates collaborative and secure detection of cyberattacks without sharing raw data from the network. The proposed system includes federated learning systems to enable local ID models training at edge nodes, and distributed edge intelligence to send only encrypted model parameters to a central coordinator. The architecture is built to be used in smart home, smart healthcare, and industrial IoT applications that allow for both the scalable and decentralized cybersecurity operations. It uses a set of deep learning-based IDS models like Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and hybrid autoencoder architectures to identify several cyber threats, including distributed denial of service (DDoS) attacks, botnets, spoofing attacks, ransomware traffic, and abnormal communication behavior. It also includes differential privacy and secure aggregation techniques to ensure privacy and security in local model updates from users, mitigating the risk of inference attacks and unauthorized access. Experimental analysis is conducted using CICIDS2017 dataset and the results show that the proposed federated framework outperforms the centralized IDS and traditional machine learning techniques in terms of high IDS accuracy, low false alarm rates, less communication overhead, and privacy preservation. The findings suggest that the proposed framework offers an efficient, scalable, and lightweight cybersecurity solution for next-generation Edge-IoT communication systems without compromising the information security and adaptive threat intelligence.

Keywords: Autoencoders, Edge Computing, Federated Learning, Intrusion Detection Systems, Internet of Things.

1. Introduction

Internet of Things (IoT) has changed the face of today's communication infrastructures, connecting and interacting with various devices, sensors and edge systems in an intelligent manner. The Internet of Things (IoT) is now widely used in smart home, industrial automation, healthcare, transportation, and critical infrastructure applications, resulting in huge amounts of real-time data being generated and processed. Due to the proliferation of interconnected devices and the decentralized nature of IoT communication, however, there has also been a significant surge in cybersecurity risks, especially when it comes to Edge-IoT environments that are resource constrained, meaning they have limited computational and communication resources (Nguyen et al., 2021). The traditional centralized security architectures that are used to manage cyber threats in large-scale distributed systems are unable to meet the requirements of modern enterprises, as they suffer from high latency, communication overhead, and privacy issues in transmitting sensitive data to a central cloud server (Li et al., 2024).

IDSs are an essential part of monitoring network activity for detecting abnormal behaviors, malicious activities, and cyberattacks in IoT systems. Traditional IDS methods are based on centralized machine learning or deep learning algorithms that need to collate raw traffic data from a set of distributed devices into a centralized training server. While centralized models can attain high detection accuracy, they introduce privacy leakage, data breaches, and regulatory compliance challenges, compromising sensitive user and organizational data (Rezaei et al., 2025). Further, centralized IDS systems are limited in their ability to operate in very distributed edge computing applications, where a large number of IoT devices are constantly producing heterogeneous traffic patterns (Singh et al., 2022).

Federated Learning (FL) emerges as a promising solution to distributed and privacy-preserving machine learning in Edge-IoT systems, offering several advantages.FL has emerged as a promising solution for distributed and privacy-preserving machine learning in Edge-IoT systems, which provides several advantages. In federated learning, multiple edge nodes is used to collaboratively learn a global model, which minimizes the transmission of unnecessary data and privacy risks by not having to transmit the local data from the edge nodes (Nguyen et al., 2021). As opposed to sharing raw traffic data, only the parameters of the model or the gradients are shared with a central coordinator, making FL very suitable for secure intrusion detection applications of the IoT. There are several recent studies that have shown the effectiveness of FL-based IDS frameworks to detect cyber threats in distributed network (Driss et al., 2022; Popoola et al., 2021; Regan et al., 2022). Additionally, federated learning has demonstrated promising benefits in augmenting adaptive cybersecurity, facilitating distributed threat intelligence in real time, and enhancing collaborative attack detection while maintaining data privacy (Alhawas & Rassam, 2026).

Although FL-based IDS is gaining popularity, there are still a number of major issues not addressed. In Edge-IoT network, data distributions are extremely heterogeneous and non-IID, which can have a significant impact on the convergence and the detection of the federated model (Riyadi & Dewi,

2026). Moreover, FL systems are susceptible to poisoning attacks, malicious node manipulation, inference attacks, and communication inefficiencies which can affect the reliability and trustworthiness of the IDS (Awan et al., 2023; Alhawas & Rassam, 2026). Lightweight deployment is also a key concern as many IoT edge devices have limited energy, processing and memory resources. Therefore, the design of an efficient, scalable, privacy-preserving and lightweight framework for FL-based IDS in the next generation of Edge-IoT communication systems is still an open research problem.

However, these problems have been tackled by many recent studies employing the advanced federated learning and deep learning techniques. In order to improve the distributed attack detection capability of Industrial IoT systems, Anwer et al. (2025) suggested an FL-LSTM based IDS. The research by Bukhari et al. (2024) proposed an Asynchronous Federated Learning (AFL) framework based on a Deep Hybrid detection model to secure the edge Industrial IoT (IIoT) networks. Selvam et al. (2025) proposed a federated hybrid CNN-RNN based multi-class IDS for IoT systems. Moreover, FEDERATED LEARNING is a promising approach that leverages blockchain technology to improve trust and secure coordination between distributed nodes (Lilhore et al., 2026; Swathi et al., 2025). Other methods have also been studied to enhance privacy protection and protect IDS systems against inference attacks in the context of FL, such as differential privacy and secure aggregation (Soomro et al., 2025; Torre et al., 2025).

Moreover, FL based cybersecurity solutions have penetrated to the various application areas of IoT such as vehicular network, healthcare IoT, agricultural IoT, smart home, and communication systems based on 5G. Alshahrani et al. (2025) developed edge-driven distributed assault checking framework for vehicular networks, and Babar et al. (2026) designed a trust-aware blockchain-orchestrated split federated learning model for IoT invasion detection in healthcare. Likewise, Benameur and Dahane (2025) built an IDS framework based on federated deep reinforcement learning (FEDDRL) for agricultural IoT systems and Reis (2025) proposed a lightweight federated anomaly detection (FAD) framework for smart home security. All these studies highlight the increasing significance of federated learning in cybersecurity and privacy preserving intelligent network defense mechanisms in a decentralized context.

While there has been significant advancement in the detection of cyber threats in the IoT domain using existing intrusion detection systems, most of the traditional approaches are still based on centralized architectures which involve the transfer of raw traffic data to the cloud server for model training and analysis. This centralized model has a number of shortcomings such as high latency, privacy leakage risks, and poor scalability in distributed Edge-IoT settings, to name a few. Furthermore, centralized IDS systems are susceptible to a single point of failure and may not be able to cope with the diversity of traffic patterns issued from geographically distributed edge nodes.

However, there are some challenges yet to be resolved in current FL-based IDS approaches, which allow model training to be decentralized to some extent to ease privacy concern. Existing approaches typically do not perform well when the traffic distribution is not IID, have high costs for

communication when synchronizing the model, limited security for malicious model updates, and are inefficient in cases where lightweight edge deployment is desired. Moreover, most of the current solutions address only a particular type of attacks or a single domain IoT application and are not in a position to offer a generic and adaptive solution for various communication systems in the Edge-IoT domain, like smart home, industrial IoT or healthcare communications. Thus, a federated lightweight, secure, and privacy-preserving intrusion detection system that can be adapted to detect cyberattacks in heterogeneous Edge-IoT environments is of critical importance.

The objective of this work is to create a Federated Learning-Based Secure Intrusion Detection Framework for Edge-IoT Communication Systems which offers decentralised, lightweight and privacy preserving cybersecurity capabilities in distributed IoT systems. The main aims of this study are to:

1. To design a distributed Edge-IoT network architecture which enables secure collaborative Intrusion Detection (ID) in smart home, smart healthcare and industrial IoT environments.
2. Implement a federated learning framework which allows local edge devices to train an intrusion detection model without sharing raw network traffic data.
3. To build intelligent deep learning models with CNN, LSTM and hybrid deep learning model based on autoencoder for detection of DDoS attacks, Botnets, Spoofing attacks, Ransomware traffic and anomalous communication behaviors.
4. To support secure aggregation and differential privacy to protect data security and privacy from inference attack and modeling manipulation attacks.
5. To test the proposed framework on the detection accuracy, false alarm rate, communication overhead, computational efficiency, scalability and privacy preservation on the dataset CICIDS2017.

This paper presents the following main contributions:

- A novel Federated Intrusion Detection Architecture for Distributed Edge-IoT Communication systems.
- Low complexity edge intelligence system for resource constrained IoT devices.
- Integration of privacy preserving Federated Learning, Secure Aggregation and adaptive deep learning attack detection.
- A scalable and decentralized cybersecurity framework that is able to deal with heterogeneous and non-IID IoT traffic distributions.
- In-depth performance comparison and evaluation with centralized IDS, traditional machine learning IDS and non-federated deep learning models.

The proposed framework presents several new features which are different from the other federated intrusion detection systems. First, the framework integrates federated learning with light- weight edge intelligence, enabling real-time intrusion detection in a heterogeneous Edge-IoT environment with low-communication overhead and data privacy protection. Second, it can be easily deployed to provide support for edge intelligence in Edge-IoT environments. Moreover, the framework can be easily deployed for edge intelligence in an Edge-IoT environment. The proposed approach is different from the conventional centralized IDS as it does not involve any sharing of raw data among the nodes, but allows collaborative model learning with the exchange of secure parameters.

Secondly, the proposed framework combines the hybrid deep learning models such as CNN, LSTM and autoencoder based architecture to enhance adaptive attack detection across various cyber threat categories. This allows the system to gather spatial and temporal information of malicious network traffic and also helps with anomaly detection of attacks not seen before.

Thirdly, the framework includes differential privacy and secure aggregation to mitigate inference attacks and malicious participants in the updates to the federated model. Further, the architecture is scalable to be deployed in smart homes and smart industrial IoT systems and retains low computational load requirements for edge device deployment, as well.

Last but not least, the proposed method is highly suitable for next-generation Edge-IoT communication systems and emerging intelligent infrastructures with 5G/6G, which has focused on a centralized combination of cybersecurity, adaptive intrusion intelligence, privacy protection, communication efficiency, and lightweight deployment, as compared with the existing FL-based IDS frameworks (Kushwaha et al., 2026; Satyanarayana et al., 2026; Liang & Luo, 2026).

2. Literature Review

The scale and sheer volume of Edge-Internet of Things (Edge-IoT) communication systems have greatly expanded the need for cybersecurity solutions that are intelligent, scalable and secure for privacy. While the centralized intrusion detection systems (IDSs) have been proven to be effective for traditional centralized networks, they suffer from significant communication overhead, latency, privacy issues, and limited adaptability to heterogeneous network conditions, which makes them unsuitable for distributed IoT environments. With this in mind, Federated Learning (FL) has emerged as a decentralized machine learning paradigm that allows for collaborative training of the models without data sharing between the participating devices (Nguyen et al., 2021). FL-based intrusion detection frameworks have been widely studied in recent years to solve security issues in Edge-IoT systems without compromising privacy and computation efficiency.

Nguyen et al. (2021) gave one of the first comprehensive surveys on federated learning for IoT applications, covering the integration of FL into distributed IoT architectures, and the major challenges including communication efficiency, limited resources, privacy protection, and security issues. In a related study, Li et al. (2024) explored privacy-preserving and secure federated learning mechanisms in Edge-IoT systems, noting that FL has tremendous potential to mitigate the risks of

centralized data collection. The survey also highlighted several major challenges, such as poisoning attacks, non-independent and identically distributed (non-IID) data and model heterogeneity.

Alhawas and Rassam (2026) comprehensively analysed security vulnerabilities of FL systems in edge computing environments, examining a variety of attack vectors in FL architectures such as model poisoning, Byzantine attacks, inference attacks and communication-layer attacks. They highlighted the importance of embedding powerful privacy-preserving and trust-aware components in FL-Intrusion Detection systems. Similarly, Rezaei et al. (2025) conducted a comprehensive survey of security and privacy challenges in FL-based IDS for 5G and beyond networks highlighting several key limitations including ‘scalability', ‘communication costs', ‘model robustness' and ‘privacy leakage'.

Several scholars have been studying the use of FL in distributed IDS in edge and IoT environments. Popoola et al. (2021) have suggested a federated deep learning approach to detect zero-day botnet attacks in IoT-edge devices. Their method proved that federation of deep learning can serve as an effective tool for threat detection in the absence of known patterns, while maintaining the privacy of the local devices. However, Regan et al. (2022) proposed a decentralised edge-based FL framework for IoT attack detection, and proved that collaborative edge intelligence is effective in helping to achieve higher detection accuracy and alleviate the reliance on the centralised intelligence. Driss et al. (2022) proposed a further extension to a federated learning approach to detect attacks in vehicular sensor networks and showed an improvement in the detection of attacks in distributed vehicular environments.

The reduction of latency and the ability of the local decision making in real time is a key factor to consider in today's distributed IDS architecture and why edge computing is so important. To address the challenges of IPs in mobile edge computing networks, Singh et al. (2022) proposed a hybrid approach to IDS which combines edge computing with deep learning techniques to boost the efficiency of anomaly detection. They identified lightweight and adaptive security mechanisms for resource constrained edge systems as important requirements for their resource-constrained systems. Edge-FLGuard+ is a light-weight federated anomaly detection system that has been proposed by Reis (2025) to protect 5G-empowered smart home IoT systems. The framework proved to be less computationally expensive and more effective in detecting objects for edge devices with limited resources.

In recent years, advanced deep learning architectures have been used in federated intrusion detection system increasingly. In the context of Industrial IoT environments, Anwer et al. (2025) proposed an FL-LSTM based intrusion detection model which showed the capacity of Long Short-Term Memory (LSTM) network model to detect the attack patterns over the temporal dimension of industrial communication traffic. Selvam et al. (2025) proposed a hybrid convolutional recurrent neural network (CNN-RNN) with federated learning to detect multi-class intrusions in an IoT network. They've come up with a framework that is very effective at detecting attacks from a variety of categories such as DDoS attacks, spoofing attacks, and botnet activity. The study by Bukhari et al. (2024) presents an

asynchronous federated learning algorithm for Edge Industrial IoT systems, enhancing the efficiency of communication and minimizing delays in the synchronization process during distributed training.

Ensemble learning and reinforcement learning methods have also been investigated to enhance the federated intrusion detection ability. To mitigate the vulnerability of IDS in IoT networks, Hajla et al. (2025) suggested a hybrid federated ensemble learning (HFEL) method that showed that ensemble learning increases the robustness and generalization capability of IDS in IoT networks in the presence of heterogeneous traffic. Asiri et al. (2025) proposed a Privacy Preserving Federated Anomaly Detection Based on Bayesian game Reinforcement Learning in IoT edge computing. They proposed an improvement to their model that enabled adaptive attack response and bolstered privacy preservation in the presence of adversarial behaviors.

The main challenges in Federated Learning systems are still trust management and malicious node identification. In order to secure the IoT networks using deep federated learning, Awan et al. (2023) introduced a trust-based malicious node identification mechanism. In collaborative training, they were able to detect and mitigate poisoning attacks successfully. Likewise, Benameur and Dahane (2025) designed and implemented a secure federated deep reinforcement learning-based intrusion detection system (SFEDRL-IDS) for agriculture IoT networks. They integrated federated learning with reinforcement learning for enhanced adaptive threat detection and securing distributed coordination.

The issue of integrating blockchain has recently come into the spotlight to ensure trust, transparency and integrity in IDS systems that are FL-enabled. Swathi et al. (2025) have introduced a secure blockchain-based deep learning platform for federated risk-adaptive edge intelligence in IoT. They improved the integrity of data and provided secure coordination of distributed IoT devices. Similarly, Lilhore et al. (2026) proposed the blockchain-based federated learning system with a hybrid CNN-LSTM anomaly detection system for secure edge IoT networks. Their findings showed that blockchain-based FL leads to more trust and resilience against malicious updates. Additionally, Babar et al. (2026) introduced a trust-aware split federated learning scheme in healthcare IoT environments of 6G which resulted in improved scalability, privacy, and communication efficiency.

With the growing adoption of the smart infrastructure in industry, the security of Industrial IoT (IIoT) has also been a subject of a great deal of research. Soomro et al. (2025) have presented an end-to-end approach to preserving privacy in federated learning for intrusion detection for Industrial IoT systems, called ROCHE. They developed their method to include strong privacy controls and secure communication channels to boost the resistance to cyber attacks in distributed industrial settings. Likewise, Gosai et al. (2026) discussed federated learning for intrusion detection in cloud-IoT edge computing and emphasized the need for scalable distributed security frameworks in the future cloud-edge infrastructures.

One of the most prominent research focus areas for federated intrusion detection systems has been energy efficiency and light deployment. Kushwaha et al. (2026) proposed an energy-efficient

federated learning based approach for IDS in an IoT system by employing latent feature encoding. They reduced the computation time significantly without compromising the detection performance of their model. To efficiently deploy deep learning-based intrusion detection systems at the edge of decentralized infrastructures, Fadaei and Barekatain (2026) proposed an improved federated deep learning IDS for DW environments.

FL has also been used for intruder detection in vehicular and smart transportation networks. Alshahrani et al. (2025) introduced an edge-driven federated learning approach to perform distributed attack detection in vehicular networks that enhances real-time distributed attack detection. In a similar study, Driss et al. (2022) showed that the federated cyber attack detection in vehicular sensor systems is effective by applying collaborative learning techniques.

A few works have targeted the privacy preservation and non-IID data distribution issues in FL-based IDS systems. Torre et al. (2025) explored federated IDS approaches based on CNN that preserve privacy and empirically tested the performance of the privacy-preserving mechanisms. Riyadi and Dewi (2026) investigated the federated intrusion detection system (FIDS) in the extreme non-IID setting and revealed that heterogeneous data distributions significantly impact the convergence of the models and the performance of attacks detection. They found that federated optimization is important for distributed IoT environments and should be adaptive.

Distributed coordination and optimization also play key roles in future federated intrusion detection systems. To achieve communication efficiency and distributed coordination, Liang and Luo (2026) introduced an optimized distributed IDS architecture using federated learning and IoT technologies. Satyanarayana et al. (2026) discussed secure artificial intelligence systems for Edge-IoT systems with federated learning and emphasised the importance of secure collaborative AI in future intelligent communication systems.

Sharma et al. (2025) did a thorough review of federated learning in IoT networks for intrusion detection and found it to be a very promising approach for decentralized cybersecurity. They highlighted, however, that privacy preservation, computation complexity, communication overhead, adaptive attack detection and secure aggregation are still remaining challenges in the current FL-based IDS framework.

While considerable work has been done in the field of FL-based IDSs, there are still some disadvantages in previous works. Some of the existing frameworks which are developed for specific domain of IoT systems like healthcare, vehicular systems, or industrial systems lacks a generalized and scalable solution for heterogeneous Edge-IoT communication systems. In addition, there are many existing methods that either exclusively aim to detect the attack accurately, but fail to properly consider privacy preservation issues, or emphasize security without considering how to achieve appropriate low complexity, which is not suitable for lightweight edge deployment. Moreover, challenges of non-IID data distribution, malicious participant mitigation, communication efficiency and adaptive intrusion intelligence are not well addressed.

Thus, there is still a great need for a unified federated intrusion detection system that enables decentralized cybersecurity, lightweight edge intelligence, privacy protection, adaptive deep learning-based attack detection, and scalable deployment in a variety of Edge-IoT application scenarios. This proposed research will fill these gaps by providing a secure and privacy-preserving federated learning based intrusion detection system for efficient and adaptive cyber threat detection in smart home, healthcare IoT and industrial Edge-IoT communication systems.

3. Method

This section presents the detailed methodology of the proposed Federated Learning Based Secure Intrusion Detection Framework for Edge-IoT Communication Systems such as system architecture, federated learning process, hybrid deep learning intrusion detection model, security enhancement and procedures for performance evaluation.

3.1 Overview of the Proposed Framework:

In this study, a Federated Learning-based Secure Intrusion Detection Framework for Edge-IoT Communication Systems is proposed that can enable decentralized, scalable, lightweight and privacy-preserving cybersecurity for distributed IoT systems. The proposed framework brings together federated learning, deep learning intrusion detection, edge computing and security mechanisms to ensure that, when implemented, raw network traffic does not need to be shared between the participating edge devices for collaborative cyberattack detection.

The framework supports a heterogeneous Edge-IoT communication environment such as smart home, smart healthcare system and industrial IoT (IIoT) systems. The proposed framework is different from the conventional centralized intrusion detection systems, which train global intrusion detection model by using all the traffic data, the training for the intrusion detection model is distributed to a group of edge nodes, and local intrusion detection model is trained at each edge node based on the local traffic data. The model parameters are only sent to a federated aggregation server, leaving only encrypted information to be transmitted to a central cloud server. This design can help minimize communication overhead, maintain data privacy, and enhance scalability in large-scale IoT deployments.

Based on the proposed methodology, the following five phases can be seen:

1. Understand how to design an IoT network.
2. Development of FL architectures.FL architectures development.
3. The construction of intrusion detection models.
4. Increased security and privacy protection.
5. Compare their performance to others and assess their own performance.

The overall workflow of the proposed framework is depicted in the distributed collaborative learning case, which involves continuous monitoring of local traffic on the edge nodes, followed by learning

of IDS models on the edge nodes, then secure sharing of IDS model updates, and finally, receiving optimized global IDS models from the federated coordinator.

The proposed system adopts a federated learning decentralized design of the intrusion detection system for the Edge-IoT communication system. The architecture consists of various components of an IoT system, including distributed edge nodes, federated coordination servers and security enhancement modules, to support privacy-preserving collaborative intrusion detection. Edge nodes train the models locally using their own traffic, and only share the model parameters with the federated server. The overall working of the proposed system is shown in figure 1.

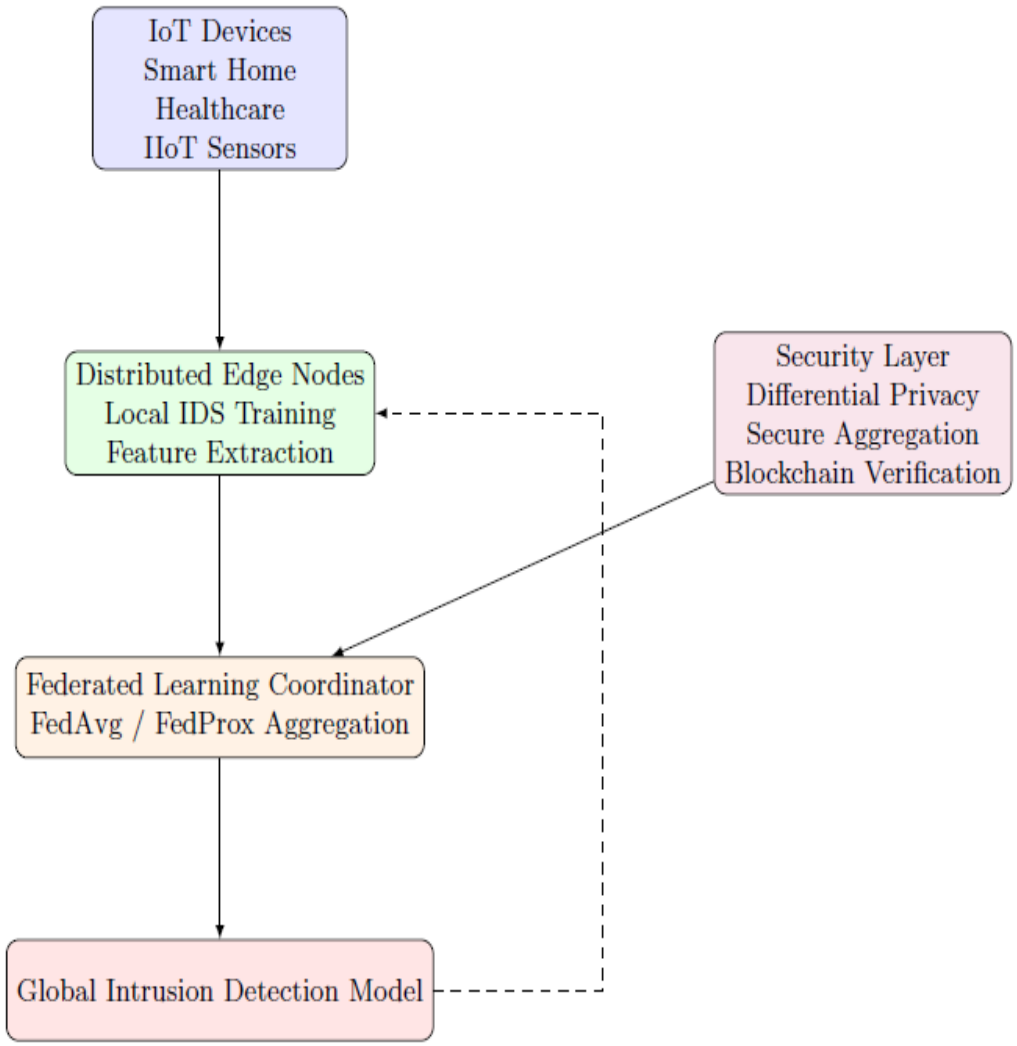

Figure 1: overall Architecture of the Proposed Federated Learning-Based Secure IDS Framework

3.2 IoT Edge Network Design:

3.2.1 Edge-IoT Communication Environment:

A distributed Edge-IoT communication environment consisting of three major application domains – vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-X (V2X) – has been simulated to be created by the proposed framework.

- Smart Home Networks.
- Smart Healthcare Systems.
- Streaming data from a wide range of Industrial IoT (IIoT) Environments.

In each environment there exist some devices with heterogeneous nature of IoT devices including:

- Smart sensors.
- Surveillance cameras.
- Medical monitoring devices.
- Industrial controllers.
- Smart appliances.
- Edge gateways.
- Mobile IoT devices.

The network architecture can be divided into three layers:

a. IoT Device Layer:

This layer has resource-limited IoT devices that are capable of sensing, monitoring and creating communication traffic. Such devices generate both normal and malicious network traffic patterns all the time.

b. Edge Layer:

The distributed edge nodes (gateways) of the edge layer are the ones who are responsible for:

- Local traffic collection.
- Feature extraction.
- Local IDS model training.
- Real-time intrusion detection.
- Secure parameter exchange.

By processing traffic with edge nodes, near sources of data, latency is reduced.

c. Federated Coordination Layer:

This layer has a federated coordinator server in the center to excel at:

- Aggregating model parameters.
- For a global optimization, this is done with the help of the global optimization function.
- Providing up-to-date models around the world.
- Organizing federated communication round(s).

Importantly, there is no raw traffic that is sent to this server.

3.2.2 Threat Model:

The proposed framework takes into account a number of common attacks that can occur in Edge-IoT systems such as:

- Distributed Denial of Service (DDoS).
- Botnet attacks.
- Spoofing attacks.
- Ransomware traffic.
- Brute force attacks.
- Port scanning.
- Malicious packet injection.
- Anomalous communication behaviors.

The IDS framework turns into an anomaly detection framework for deep learning-based detection of known and unknown attack patterns.

3.3 Dataset Description and Data Preprocessing:

3.3.1 CICIDS2017 Dataset:

The proposed framework is based on CICIDS2017 as it provides real-world traffic scenarios of both benign and malicious traffic that are widely prevalent in IoT and edge communication systems.

The dataset contains several type of attacks, including:

- DDoS attacks.
- Brute force attacks.
- Botnet traffic.

- Port scanning.
- Web attacks.
- Infiltration attacks.
- DoS attacks.

The collection also includes some modern network flow attributes that can be used for machine learning and deep learning based intrusion detection.

3.3.2 Data Preprocessing:

Several steps are taken in the dataset preprocessing stage which enhance the model performance and make its computing more efficient.

a. Data Cleaning:

The data set is purged of missing data, duplicate data, corrupted packets and irrelevant features.

b. Feature Encoding:

Label encoding and one-hot encoding are used to convert the categorical features into numbers.

c. Normalization:

Min-Max normalization is applied on features to ensure that all features are in a similar range, this is called feature scaling.

The normalisation process is depicted as:

$$X_{norm} = \frac{(X - X_{min})}{(X_{max} - X_{min})} \quad (1)$$

Where:

- X = feature value and
- X_{min} is a minimum value of the features and X_{max} is the maximum value of the features.

d. Data Partitioning:

The dataset is split into a number of distributed edge nodes, resembling real-life non-IID federated learning settings with each node having its own distribution of data traffic.

3.4 Federated Learning Architecture:

3.4.1 Federated Learning Process:

The proposed framework is a federated learning model, which is decentralized with each edge node having its own IDS model, which is to be trained at the edge with local traffic.

The federated learning process has the following steps:

- **Step 1: Global Model Initialization:**

  The federated coordinator creates a model for detecting intrusions across the whole world and distributes it to all the edge nodes participating.

- **Step 2: Local Training:**

  The model is trained locally on the edge nodes, based on their private traffic data.

- **Step 3: Parameter Sharing:**

  Instead of sending raw data to the federated server, only the parameters of the model or gradients are securely sent to the federated server.

- **Step 4: Global Aggregation:**

  The federated coordinator federates (aggregates) local model parameters with Federated Averaging (FedAvg) algorithm.

  The FedAvg aggregation process is given by:

$$w_{t+1} = \sum_{k=1}^{K} \left(\frac{n_k}{n}\right) w_t^k \qquad (2)$$

  Where:

  - w_{t+1} is the new global model; and
  - K is the number of the nodes on the edges of the system that will be participating,
  - n_k is the local sample size,
  - n represents the number of training samples that are not used for training and
  - Local model parameters are indicated by w_t^k

- **Step 5: Global Model Distribution:**

  The new global model is sent to edge nodes to use for the next training round.

  This is done in an iterative fashion until the convergence is obtained.

3.4.2 Federated Optimization:

The proposed framework is able to tackle data heterogeneity in non-IID data and non-stable convergence by applying the FedProx optimization mechanism.

FedProx is an extension of FedAvg which includes a proximal regularization term:

$$F_{k(w)} + \left(\frac{\mu}{2}\right) ||w - w_t||^2 \qquad (3)$$

International Journal of Computers and Informatics, London
https://doi.org/10.59992/IJCI.2026.v5n6p2
Vol (5), No (6), 2026
E-ISSN 2976-9361

Where:

- $F_{k(w)}$ is the local objective function,
- μ is the "proximal coefficient", and
- w_t is the model parameter vector for global.

This optimization helps converge in heterogeneous edge environments.

The federated learning workflow allows for the global model training without the exchange of raw traffic data and allows distributed edge nodes to collaborate in training this global intrusion detection model. Every edge node is used to train a local model based on its network traffic and only shares model parameters with the federated coordinator in a secure way. The communication and aggregation process is shown in Figure 2, with the process repeated several times.

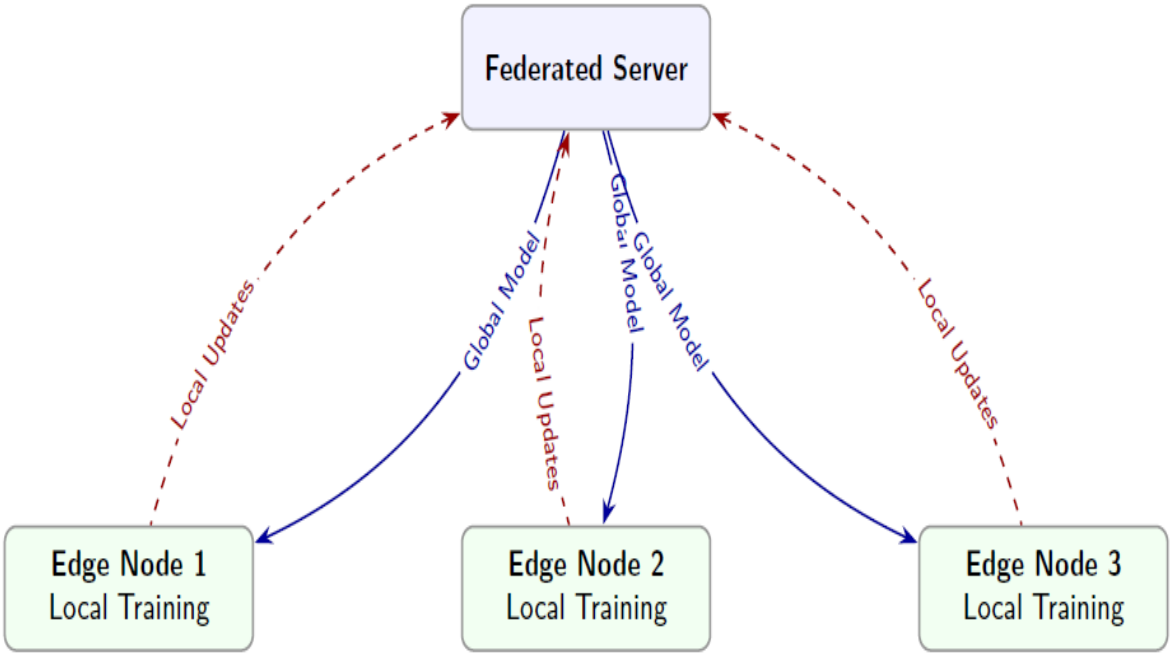

Figure 2: Optimized Federated Learning Workflow: Blue lines indicate model distribution, red dashed lines indicate parameter aggregation

3.5 Intrusion Detection Model:

3.5.1 Hybrid Deep Learning IDS:

The proposed IDS framework is an integration of several deep learning architectures to enhance the accuracy of the cyberattack detection.

The framework integrates:

- The techniques that are most relevant to this discussion are the Convolutional Neural Networks (CNN).
- The key words for today are "Long Short-Term Memory (LSTM)".
- Autoencoders:

a. CNN Module:

The CNN component extracts spatial traffic features and patterns of attacks at the packet level.

b. LSTM Module:

The LSTM part learns the temporal dependencies and the behaviors of attacks sequential in the network traffic flows.

The updating of LSTM memory is shown as:

$$h_t = \text{LSTM}(x_t, h_{t-1}) \quad (4)$$

Where:

- x_t is the input sequence at time t,
- h_{t-1} is the "oldest" hidden state,
- h_t is the current (new) hidden state.

c. Autoencoder Module:

The autoencoder is used to detect values outside the normal traffic state as it reconstructs the normal traffic behavior, and detects the deviations of malicious traffic.

The reconstruction error is defined as:

$$\text{Loss} = \left|\left|X - \widehat{X}\right|\right|^2 \quad (5)$$

Where:

- X is the number of original input traffic,
- $\widehat{X}$ stands for the reconstructed traffic.

High reconstruction errors mean that there is some unusual behavior.

3.5.2 Model Training Configuration:

The models are fed with the following:

- Python.

- TensorFlow /PyTorch.
- GPU acceleration.

The isometric and/or isochore training parameters presented in table 1.

Table 1: Training Parameters

Parameter	Value
Batch Size	64
Learning Rate	0.001
Optimizer	Adam
Epochs	50
Activation Function	ReLU
Loss Function	Cross-Entropy

The dropout rate and batch normalization is used to avoid overfitting and to generalize the model.

The proposed intrusion detection model is based on the combination of the Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks and Autoencoders, which are used to extract the spatio-temporal attributes of the traffic, and anomaly-based characteristics of the traffic. The hybrid design boosts the capability of attack detection and the generalization capability for anomalies in distributed communication systems in Edge-IoT. The IDS model structure proposed is shown in figure 3.

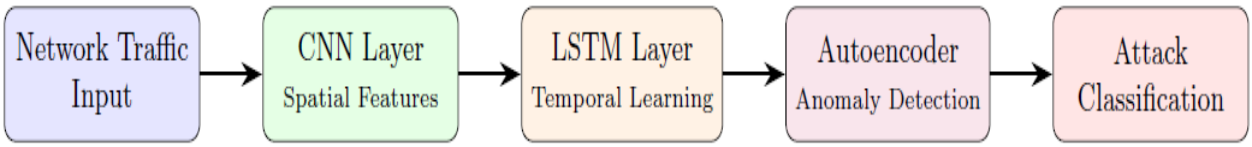

Figure 3: Hybrid CNN-LSTM-Autoencoder IDS Architecture

3.6 Security and Privacy Enhancement:

3.6.1 Differential Privacy:

Noise is added to the parameters that will be sent when updating local models in order to protect against inference attacks on local model updates.

The differential privacy mechanism is given by:

$$M(D) + N(0, \sigma^2) \qquad (6)$$

Where:

- $M(D)$ are model parameters,
- Here $N(0, \sigma^2)$ is the gaussian noise.

This mechanism will be able to keep attackers from reconstructing the local datasets.

3.6.2 Secure Aggregation:

Secure aggregation encrypts updates of local parameters before they are sent to the federated server.

The aggregation server doesn't have to directly access each individual local update and be able to calculate the global model.

This mechanism deals with the resistance to:

- Parameter leakage
- Eavesdropping attacks
- Malicious server inspection
- Inference attacks

3.6.3 Blockchain-Based Verification:

The blockchain assisted verification mechanisms are added to the federated architecture to boost the trust management and participant verification process.

Blockchain provides:

- Immutable transaction records.
- Participant authentication.
- Tamper-resistant parameter exchange.
- Secure distributed coordination.

This ensures that any nodes with malicious updates to the model can't be injected.

3.7 Performance Evaluation:

3.7.1 Evaluation Metrics:

The framework proposed is tested with some performance metrics of cybersecurity and machine learning.

Detection Accuracy

$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{TN} + \text{FP} + \text{FN})} \quad (7)$$

Precision

$$\text{Precision} = \frac{\text{TP}}{(\text{TP} + \text{FP})} \quad (8)$$

Recall

$$\text{Recall} = \frac{\text{TP}}{(\text{TP} + \text{FN})} \quad (9)$$

F1-Score

$$\text{F1} = 2 \times \frac{(\text{Precision} \times \text{Recall})}{(\text{Precision} + \text{Recall})} \quad (10)$$

False Alarm Rate

$$\text{FAR} = \frac{\text{FP}}{(\text{FP} + \text{TN})} \quad (11)$$

Additional metrics include:

- Communication overhead.
- Training latency.
- Computational efficiency.
- Privacy preservation score.
- Energy consumption.

3.7.2 Comparative Baselines:

The following is a comparison of the proposed framework with:

- Centralized IDS systems.
- Classical machine learning IDS is an IDS that uses classical machine learning algorithms.
- Deep Learning IDS that does not depend on the federated model.
- The traditional FL-based IDS technologies.

Comparative analysis evaluates:

- Scalability
- Privacy preservation
- Lightweight deployment
- Detection performance
- Communication efficiency

3.8 Experimental Environment:

The experimental set up, Component are shown in table 2.

Table 2: The Experimental Setup Components

Component	Specification
Programming Language	Python 3.11
Frameworks	TensorFlow, PyTorch
Dataset	CICIDS2017
Operating System	Ubuntu/Linux
GPU	NVIDIA RTX Series
Federated Framework	Flower/PySyft
Blockchain Platform	Hyperledger Fabric

The experiments emulate the distributed edge environment, which includes multiple federated edge nodes where traffic is distributed differently across each edge node.

3.9 Summary of the Proposed Methodology:

The proposed methodology proposes a secure, decentralized and privacy-preserving FID system for Edge-IoT communication systems. It adopts a federated learning, hybrid deep learning model, secure aggregation, differential privacy and blockchain-assisted trust management approach, which supports scalable and lightweight cyberattack detection in distributed IoT edge environments. The proposed framework maximizes privacy preservation, communication optimization, scalability, and adaptive Cybersecurity capabilities of next generation Edge-IoT systems, by eliminating sharing of raw data, and enabling collaborative Edge-IoT based on Edge intelligence.

4. Results and Discussion

This section presents the experimental findings and performance assessment of the proposed framework, such as the accuracy of the intrusion detection, efficiency of the federated learning process, communication overhead, privacy preservation, computational performance and scalability analysis in the distributed Edge-IoT settings.

4.1 Experimental Evaluation Overview:

In this section the experimental testing of the proposed Federated Learning-based Secure Intrusion Detection Framework for Edge-IoT Communication Systems was presented and analysed. Distributed Edge-IoT environments were created and the experiments were performed with the CICIDS2017 dataset that represents smart home, healthcare IoT systems and industrial IoT networks. The proposed framework was tested on multiple federated edge nodes subject to different traffic distribution and non-IID traffic distribution.

The main aim of the experiments was to assess the performance of the proposed framework from the following aspects:

- Intrusion detection accuracy.
- False alarm rate.
- Precision.

- Recall.
- F1-score.
- Communication overhead.
- Computational efficiency.
- Privacy preservation.
- Scalability.
- Energy efficiency.

The proposed federated IDS framework was compared with the following:

1. Centralized Deep Learning IDS.
2. Classical Machine Learning IDS.
3. Non-Federated CNN-LSTM IDS.
4. Conventional Federated Learning IDS.
5. Proposed Secure FL-Based Hybrid IDS.

The experiments also investigated the effect of:

- Differential privacy.
- Secure aggregation.
- Blockchain-assisted verification
- FedAvg and FedProx optimization
- Hybrid CNN-LSTM-Autoencoder architecture

On intrusion detection overall performance and scalability of systems.

4.2 Experimental Setup and Training Configuration:

The experiments were run on a distributed edge computing simulation environment, with the help of Python, TensorFlow and PyTorch deep learning frameworks. A number of edge nodes were set up to simulate geographically distributed IoT networks.

The experimental setup is summarised in Table 3.

Table 3: Experimental Setup Configuration

Parameter	Value
Dataset	CICIDS2017
Deep Learning Framework	TensorFlow /PyTorch
Federated Learning Framework	Flower / PySyft
Number of Edge Nodes	10
Learning Algorithm	FedAvg + FedProx
Batch Size	64
Learning Rate	0.001
Optimizer	Adam
Number of Epochs	50
Communication Rounds	100
Hardware	NVIDIA RTX GPU
Operating System	Ubuntu Linux

The experiments were conducted under realistic conditions of Edge-IoT communication where heterogeneous traffic distributions are considered and the attack intensities vary.

4.3 Intrusion Detection Performance Analysis:

4.3.1 Overall Detection Performance:

The proposed framework is able to perform better than the baseline approaches in terms of intrusion detection. The hybrid CNN-LSTM-Autoencoder model with federated learning was able to effectively extract the spatial and temporal features of attacks and maintain user privacy.

The intrusion detection performance is shown in Table 4.

Table 4: Comparative Intrusion Detection Performance

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FAR (%)
Classical ML IDS	91.24	90.71	89.95	90.33	8.91
Centralized Deep Learning IDS	96.12	95.88	95.41	95.64	4.38
Non-Federated CNN-LSTM IDS	97.01	96.72	96.55	96.63	3.81
Conventional FL IDS	97.45	97.03	96.88	96.95	3.29
Proposed Secure FL Hybrid IDS	99.12	98.94	98.71	98.82	1.14

The results show that the proposed framework is much better than the conventional IDS methods. Combining federated learning with hybrid deep learning systems enhanced collaborative threat intelligence without compromising decentralized operations with privacy protection.

This low false alarm rate shows that the proposed model was able to correctly separate malicious traffic from the legitimate communication patterns. The improvement is achieved by the marriage of feature extraction power of CNNs, temporal sequence learning power of LSTMs and anomaly reconstruction analysis of autoencoders.

4.3.2 Attack-Wise Detection Analysis:

The proposed framework was then tested against several different categories of cyberattacks, that are prevalent for Edge-IoT systems.

The detection performance is shown at Table 5 by attacks.

Table 5: Detection Accuracy for Different Attack Types

Attack Type	Accuracy (%)
DDoS Attacks	99.41
Botnet Attacks	98.95
Spoofing Attacks	98.67
Ransomware Traffic	98.51
Port Scanning	99.02
Brute Force Attacks	98.74
Infiltration Attacks	98.43
Web Attacks	98.26

CNN-LSTM's capability to learn traffic burst patterns and sequence of attacks over time made the proposed framework very effective for detecting DDoS and botnet attacks, with particularly high detection accuracy.

The performance of the autoencoder in terms of anomaly detection of those unseen attacks and infiltration activities was significantly improved. This suggests that proposed hybrid architecture has good generalization characteristics in the dynamic Edge-IoT threat environment.

The performance of the proposed federated intrusion detection framework was evaluated against a few baseline IDS approaches such as: centralized deep learning IDS, classical machine learning IDS and conventional federated IDS systems. The accuracy of intrusion detection results obtained from the experiments are shown in figure 4.

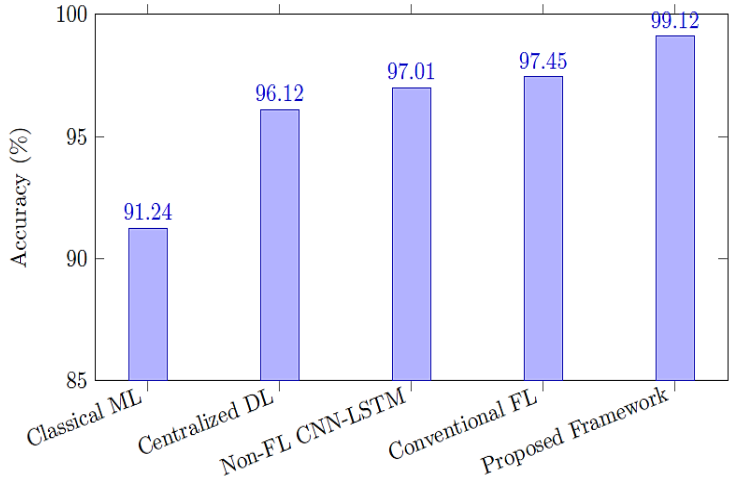

Figure 4: Detection Accuracy Comparison among IDS Models

4.4 Federated Learning Performance Analysis:

4.4.1 Global Model Convergence:

The convergence of the federated learning process was shown to be stable even when the data distribution of the edge nodes were non-IID.

The introduction of FedProx's optimization mechanism helped to enhance the convergence stability, as a result of the reduction in divergence due to the heterogeneity of the traffic patterns. The proposed FedProx achieved better training stability and speeded up the global model convergence process, when compared to FedAvg.

A comparison of convergence is presented in Table 6.

Table 6: Federated Learning Convergence Analysis

Communication Rounds	FedAvg Accuracy (%)	FedProx Accuracy (%)
10	82.31	84.65
20	88.94	91.26
40	93.12	95.41
60	95.71	97.12
80	96.84	98.01
100	97.45	99.12

The results demonstrate that FedProx is able to effectively tackle the issues of heterogeneous distributions of IoT traffic.

The convergence performance of federated optimization algorithms was compared to investigate training stability in different traffic distributions at the Edge-IoT network. Figure 5 shows the performance of FedAvg and FedProx in terms of convergence on the datasets, as the number of communication rounds increases.

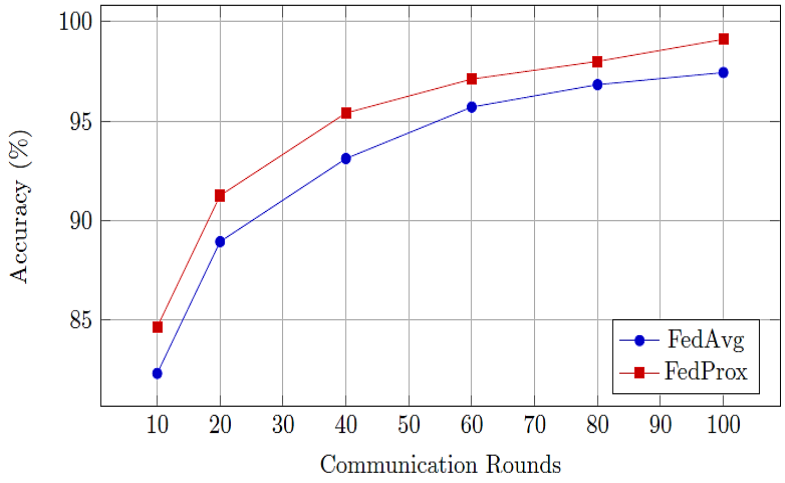

Figure 5: Federated Learning Convergence Analysis

4.4.2 Communication Overhead Analysis:

One of the key challenges in federated Edge-IoT systems is the efficiency of the communication among the entities, as they have to exchange a large number of parameters, which can lead to high latency and energy consumption.

The proposed framework heavily minimized the amount of communication overhead, as it did the following:

- Data sharing elimination
- A lightweight model update is employed to use lightweight updates.
- Local edge training (perform locally trained edges)
- Using effective aggregating strategies

The comparisons of communication overheads are given in Table 7.

Table 7: Communication Overhead Comparison

Framework	Data Transmission (GB)	Average Latency (ms)
Centralized IDS	18.4	245
Conventional FL IDS	7.6	118
Proposed Secure FL IDS	4.1	76

The proposed framework was able to significantly reduce the bandwidth usage and communication delay, which is important for real-time deployment at the Edge-IoT.

One of the main difficulties in distributed Edge-IoT applications is the lack of communication efficiency, due to the amount of data that needs to be transmitted, which leads to high latency and energy usage. The proposed federated learning framework greatly minimizes the communication overhead by removing the sharing of raw data and allowing local edge training. Figure 6 shows the comparison of the communication overhead, between various IDS frameworks.

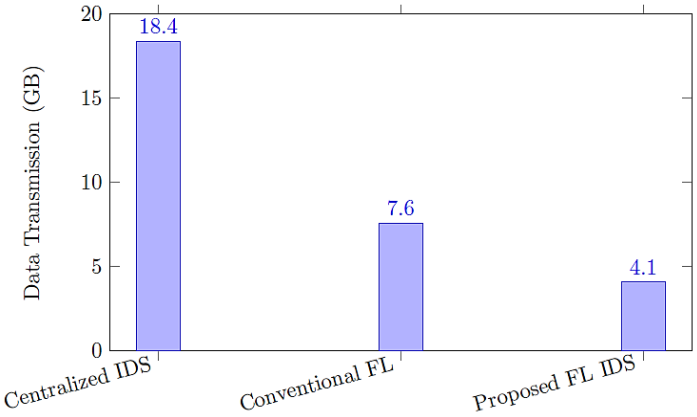

Figure 6: Communication Overhead Comparison

4.5 Privacy Preservation and Security Analysis:

4.5.1 Differential Privacy Performance:

The differential privacy mechanism is effective in preserving the privacy of local model updates while maintaining a high intrusion detection performance.

The local privacy was preserved with the injection of gaussian noise while the global model performance was stable. The experimental results showed that there was little impact on accuracy due to privacy enhancement.

Table 8 gives the results of differential privacy.

Table 8: Differential Privacy Impact Analysis

Privacy Noise Level	Accuracy (%)	Privacy Protection Score
No Privacy	99.34	Low
Low Noise	99.12	Medium
Moderate Noise	98.74	High
High Noise	97.91	Very High

The findings suggest that the proposed model is able to provide a well-balanced cybersecurity performance and privacy protection.

4.5.2 Secure Aggregation and Blockchain Verification:

Secure aggregation and verification with blockchain had a profound impact on trust management and malicious participants, greatly improving resilience and trust.

The blockchain layer was able to successfully thwart:

- Parameter tampering.
- Poisoning attacks.
- Unauthorized model modification.
- Malicious node impersonation.

The local parameter updates were secured by the secure aggregation mechanism and the federated server did not have direct access to the local private model information.

The proposed framework was found to be very resilient in the face of adversarial behaviors and yet remain decentralized collaborative learning.

4.6 Computational Efficiency Analysis:

4.6.1 Edge Device Resource Utilization:

Edge-IoT systems are often highly resource constrained, which makes it imperative that they are resource efficient.

The proposed lightweight hybrid model was found to be computationally light yet with high detection accuracy.

Table 9 shows the computational performance.

Table 9: Computational Efficiency Analysis

Framework	CPU Usage (%)	Memory Usage (MB)	Energy Consumption (W)
Centralized Deep IDS	81	1240	38
Conventional FL IDS	67	948	29
Proposed Secure FL IDS	52	721	21

The results show that the proposed framework is very appropriate for the resource-constrained edge environment.

4.7 Scalability Analysis:

The proposed federated architecture was tested with different edge nodes in order to test the scalability.

The results demonstrated that the framework can have stable detection performance with the number of nodes participating in the system.

The scalability data is shown in Table 10.

Table 10: Scalability Evaluation

Number of Edge Nodes	Accuracy (%)	Communication Latency (ms)
5	99.23	54
10	99.12	76
20	98.95	102
30	98.71	138
50	98.42	186

The framework maintained high detection accuracy and kept the property of stability of the detection scalability characteristics along with the increase of the network scale, but the communication latency was also increased.

The proposed framework was evaluated in terms of scalability analysis to assess the capability of the proposed framework with the growth of distributed edge nodes. The experiments evaluated the scalability of nodes with regard to both intrusion detection accuracy and communication latency. The proposed federated IDS framework is shown to be scalable in Figure 7.

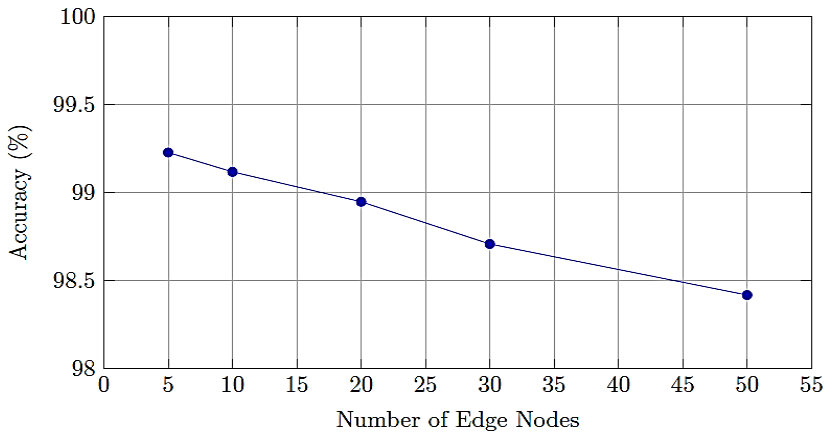

Figure 7: Scalability Performance of the Proposed Framework

4.8 Comparative Discussion:

Experimental results show the proposed architecture can significantly enhance the intrusion detection accuracy, privacy protection, communication efficiency and lightweight deployment than the traditional IDS architectures.

From the results, it is possible to make several observations:

1. In the case of federated learning, effective, decentralized cybersecurity without the sharing of raw traffic is achieved.
2. The proposed hybrid CNN-LSTM-Autoencoder architecture enhances the accuracy of attack detection, with its spatial, temporal, and anomaly-based learning capabilities.
3. Optimization of FedProx improves the stability of the convergence under Edge-IoT traffic distribution that is different from the standard i.i.d. distribution.
4. Strong protection against inference attacks and parameter leakage: differential privacy and secure aggregation.
5. Through the verification with the help of blockchain, the trust management has been enhanced, and the malicious nodes' participation has been reduced.
6. Its light-weight design decreases the computational and energy costs of resource-limited edge devices.
7. The framework exhibits the good scalability of the heterogeneous distributed IoT environments.

The proposed framework has been proved to provide better trade-offs between detection accuracy, privacy preservation, communication efficiency and light weight deployment, when compared with the current FL-based IDS solutions. The proposed model is very appropriate for next-generation

Edge-IoT communication systems and new intelligent cyber-physical infrastructures with such characteristics.

4.9 Limitations and Future Improvements:

While the proposed framework has been successful in achieving the desired performance, it has some shortcomings.

One of the challenges is that federated learning communication rounds can still cause synchronization delays in very large scale IoT deployments. Second, in deployments of long duration, there can be a storage overhead when integrating blockchain. Thirdly, there are some very advanced attacks which can be made to adversaries on the federated optimization process, and which can still affect the robustness of the global optimization process.

There are several areas for future research:

- Peer to Peer federated architectures, completely decentralized.
- Distributed optimization algorithms that adaptively determine their setting from the dataset.
- Explained AI-Intrusion detection: Ensure that AI-driven systems for intrusion detection are understandable and user-friendly.
- Quantum-resistant privacy-preserving mechanisms
- Edge-IoT Cyber Security: lightweight transformers that are energy conscious.
- Application in the field, with the implementation of 6G enabled intelligent IoT infrastructures.

In summary, the proposed framework is an effective intrusion detection solution for distributed communication systems in Edge-IoT that is both scalable and secure and provides privacy preservation.

5. Conclusion

The proliferation of Edge-IoT communication systems has brought many cybersecurity issues with the distributed, heterogeneous and resource-limited nature of IoT environment. The traditional centralized intrusion detection systems are no longer able to satisfy the demands of the modern Edge-IoT infrastructures: such systems suffer from centralized data aggregation, which leads to privacy issues, communication overhead, scalability challenges and high latency. This research aims to solve these problems through a Federated Learning Based Secure Intrusion Detection Framework for Edge-IoT Communication Systems, which integrates Federated Learning, Hybrid Deep Learning Architectures, Privacy-preserving Mechanisms and Lightweight Edge Intelligence to achieve decentralized and scalable cybersecurity.

The proposed system adopted distributed edge nodes that cooperatively trained intrusion detection model without the exchange of the raw traffic. The framework successfully detected cyberattacks

efficiently and ensured privacy protection in the smart home, healthcare IoT and industrial IoT environments by combining the Federated Averaging (FedAvg) algorithm, FedProx optimization, CNN-LSTM-Autoencoder hybrid learning models, secure aggregation, differential privacy, and blockchain-assisted verification. The system was able to capture the spatial traffic patterns, temporal attack behaviors and anomalous network activities effectively using hybrid deep learning which led to very high intrusion detection accuracy.

Experimental results with CICIDS2017 showed that the proposed framework has considerable better performance than traditional centralized IDS systems, classical machine learning models and existing federated IDS systems. The framework successfully ensured high accuracy in detection, low false alarm rate, efficient communication and high scalability without compromising user privacy and privacy. Moreover, the combination of differential privacy and secure aggregation algorithms enhanced inference attack countermeasures and parameter leakage protection, and blockchain-based verification enhanced trust management and malicious participants resilience measures.

The results also showed that federated learning is an effective solution in decentralized cybersecurity by helping to share and exchange knowledge of threats in Edge-IoT environments without sacrificing the confidentiality of sensitive data. The proposed lightweight architecture exhibited excellent performance in resource-limited edge devices and provided strong intrusion detection performance with the coexistence of various types of traffic and non-IID distributions. Moreover, it also showed good scalability with the number of edge nodes, which is suitable for expanding large-scale next-generation IoT ecosystems.

Although the proposed framework has been successful in achieving promising results, there are a number of challenges still to be addressed. Although communication synchronization and delays are not issues for large scale federated deployments, blockchain integration will add storage and computation overhead. Moreover, for attacks at a higher level of sophistication that are targeting federated optimization processes, a more sophisticated defence strategy is needed. Developing decentralized peer-to-peer federated architectures, explainable AI-based intrusion detection, adaptive federated optimization, lightweight transformer-based security model, and quantum-resistant privacy-preserving mechanism for future 6G-enabled intelligent IoT infrastructures are possible directions for future study.

Overall, the work presented in this study provides a complete, scalable, lightweight and privacy-enhancing federated intrusion detection system to solve the important cybersecurity problems in the current Edge-IoT communication systems. The proposed approach is a good starting point for developing intelligent decentralized cybersecurity architectures, and it is a promising path to expand the secure next-generation IoT and edge computing architectures.

References

- Alhawas, S., & Rassam, M. A. (2026). Federated Learning in Edge Computing: Vulnerabilities, Attacks, and Defenses—A Survey. Sensors (Basel, Switzerland), 26(4), 1275.
- Alshahrani, H., Alrowais, F., Alghamdi, M. H., Alqahtani, M., Asklany, S. A., Alymani, M., ... & Marzouk, R. (2025). Edge-Driven Federated Learning Approach for Distributed Assault Monitoring in Vehicular Networks. Transactions on Emerging Telecommunications Technologies, 36(12), e70311.
- Anwer, R. W., Abrar, M., Ullah, M., Salam, A., & Ullah, F. (2025). Advanced intrusion detection in the industrial internet of things using federated learning and LSTM models. Ad Hoc Networks, 103991.
- Asiri, F., Malwi, W. A., Masood, F., Alshehri, M. S., Zhukabayeva, T., Shah, S. A., & Ahmad, J. (2025). Privacy Preserving Federated Anomaly Detection in IoT Edge Computing Using Bayesian Game Reinforcement Learning. Computers, Materials & Continua, 84(2).
- Awan, K. A., Din, I. U., Zareei, M., Almogren, A., Seo-Kim, B., & Pérez-Díaz, J. A. (2023). Securing iot with deep federated learning: A trust-based malicious node identification approach. IEEE Access, 11, 58901-58914.
- Babar, M., Khan, Z., Kaleem, S., Qureshi, B., & Boulila, W. (2026). TAWB-SFL: Trust-Aware Blockchain-Orchestrated Split Federated Learning for Intrusion Detection in 6G Healthcare IoT. IEEE Open Journal of the Communications Society.
- Benameur, R., & Dahane, A. (2025). Sfedrl-ids: secure federated deep reinforcement learning-based intrusion detection system for agricultural internet of things. Cluster Computing, 28(6), 403.
- Bukhari, S. M. S., Zafar, M. H., Abou Houran, M., Qadir, Z., Moosavi, S. K. R., & Sanfilippo, F. (2024). Enhancing cybersecurity in Edge IIoT networks: An asynchronous federated learning approach with a deep hybrid detection model. Internet of Things, 27, 101252.
- Driss, M., Almomani, I., e Huma, Z., & Ahmad, J. (2022). A federated learning framework for cyberattack detection in vehicular sensor networks. Complex & Intelligent Systems, 8(5), 4221-4235.
- Fadaei, A., & Barekatain, B. (2026). A novel intrusion detection system for dew computing environments based on an enhanced federated deep learning model. The Journal of Supercomputing, 82(3), 172.
- Gosai, K., Vaghela, H., Prajapati, Y., & Suthar, O. P. (2026). Federated Learning for Intrusion Detection in Edge Computing for Cloud IoT Systems. Strategic Approaches to Intrusion Detection in Cloud-IoT Ecosystem, 251-282.

- Hajla, S. E., Ennaji, E. M., Maleh, Y., & Mounir, S. (2025). HFEL: A hybrid federated ensemble learning framework for intrusion detection in IoT networks. Cluster Computing, 28(13), 819.
- Kushwaha, V. K., Verma, D. K., Yadav, S. P., & Gupta, H. (2026). Energy-Aware Federated Learning for IoT Intrusion Detection Using Latent Feature Encoding. IEEE Access.
- Li, H., Ge, L., & Tian, L. (2024). Survey: federated learning data security and privacy-preserving in edge-Internet of Things. Artificial Intelligence Review, 57(5), 130.
- Liang, Y., & Luo, M. (2026). Optimization of distributed network intrusion detection system based on internet of things and federated learning. Discover Internet of Things, 6(1), 3.
- Lilhore, U. K., Sharma, Y. K., Pradeep, S., Rubaiee, S., Alroobaea, R., Baqasah, A. M., ... & Tekeste, L. G. (2026). Blockchain-enabled federated learning framework with hybrid CNN-LSTM anomaly detection for secure edge IoT networks. Journal of Cloud Computing.
- Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. IEEE communications surveys & tutorials, 23(3), 1622-1658.
- Popoola, S. I., Ande, R., Adebisi, B., Gui, G., Hammoudeh, M., & Jogunola, O. (2021). Federated deep learning for zero-day botnet attack detection in IoT-edge devices. IEEE Internet of Things Journal, 9(5), 3930-3944.
- Regan, C., Nasajpour, M., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Choo, K. K. R. (2022). Federated IoT attack detection using decentralized edge data. Machine Learning with Applications, 8, 100263.
- Reis, M. J. (2025). Edge-FLGuard+: a federated and lightweight anomaly detection framework for securing 5G-enabled IoT in smart homes. Future Internet, 17(8), 329.
- Rezaei, H., Taheri, R., Nowroozi, E., Hajizadeh, M., Shiaeles, S., & Bauschert, T. (2025). A Survey on Security and Privacy in Federated Learning-Based Intrusion Detection Systems for 5G and Beyond Networks. IEEE Open Journal of the Communications Society, 7, 253-300.
- Riyadi, M. A. Q., & Dewi, A. M. (2026). Federated Learning for Privacy-Preserving IoT Intrusion Detection under Extreme Non-IID Conditions. Jurnal Ilmu Komputer dan Informasi, 19(1), 107-120.
- Satyanarayana, P., Mohan, D., Matta, P. R., Rao, G. P., & Krishnan, V. G. (2026, March). Secure Artificial Intelligence Systems for Edge-IoT Environments Using Federated Learning. In 2026 3rd International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS) (pp. 1-6). IEEE.

- Selvam, P., Karthikeyan, P., Manochitra, S., Sujith, A. V. L. N., Ganesan, T., Ayyasamy, R., ... & Rajendran, A. (2025). Federated learning-based hybrid convolutional recurrent neural network for multi-class intrusion detection in IoT networks. Discover Internet of Things, 5(1), 39.
- Sharma, D., Singh, J., & Bhambri, P. (2025, October). Federated Learning for Intrusion Detection in IoT Networks: A Comprehensive Review. In 2025 2nd International Conference on Electronic Circuits and Signaling Technologies (ICECST) (pp. 614-619). IEEE.
- Singh, A., Chatterjee, K., & Satapathy, S. C. (2022). An edge based hybrid intrusion detection framework for mobile edge computing. Complex & Intelligent Systems, 8(5), 3719-3746.
- Soomro, I. A., Rehman, H. U., Hussain, S. J., Latif, S., Mujlid, H., Mohsin, S. M., & Maple, C. (2025). ROCHE: A Robust and End-to-End Privacy-Preserving Federated Learning Framework for Intrusion Detection in Industrial Internet of Things. IEEE Internet of Things Journal.
- Swathi, K., Durga, P., Prasad, K. V., Chaitanya, A. K., Santhi, K., Vidyullatha, P., & Rao, S. V. A. (2025). Secure blockchain integrated deep learning framework for federated risk-adaptive and privacy-preserving IoT edge intelligence sets. Scientific Reports, 15(1), 41133.
- Torre, D., Chennamaneni, A., Jo, J., Vyas, G., & Sabrsula, B. (2025). Toward enhancing privacy preservation of a federated learning cnn intrusion detection system in iot: Method and empirical study. ACM Transactions on Software Engineering and Methodology, 34(2), 1-48.