Journal of Technology and System Information Vol: 3, No 2, 2026, Page: 48-73

Zero-Trust Network Access with Federated Learning for Privacy-Preserving Intrusion Detection in Distributed Communication Systems

Karar Talal

University of Al-Qadisiyah

DOI:
https://doi.org/10.47134/jtsi.v3i2.5746
*Correspondence: Malath Technical Kareem
Email: porteacher11@qu.edu.iq

Received: 30-05-2026
Accepted: 30-03-2026
Published: 30-04-2026

Abstract: The fast-growing distributed communication systems, such as cloud environment, Internet of Things (IoT) platform, and edge computing computers, have greatly compounded the threat of contemporary cybersecurity. The common traditional intrusion detection systems (IDS) are based on centralized collection and analysis of data, which initiates significant issues concerning the privacy of data, scale issues, and communication overheads. This paper will overcome these issues by developing a new Zero-Trust Network Access (ZTNA) model that combines Federated Learning (FL) with privacy-constrained intrusion detection in distributed communication setting. This suggested architecture will be made of three collaborative layers: edge nodes which process local data and train local models, a federated aggregation server which coordinates the global model update using the Federated Averaging (FedAvg) algorithm, and a zero-trust policy engine which dynamically assesses access control decisions based on user trust scores, and network risk assessments. Deep learning techniques, such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Transformer, are used to create local IDS models with which spatial and temporal patterns of attacks can be effectively detected. The experiments are carried out with well-known datasets of cybersecurity benchmarks that are UNSW-NB15, CSE-CIC-IDS2018 and TON IoT. The environment of implementation makes use of the TensorFlow federated, PyTorch, Docker based edge nodes, and a Kubernetes orchestration framework to recreate realistic distributed conditions. Experimental evaluation proves that the offered framework is much more effective in terms of increasing the accuracy of intrusion detection and decreasing false positive rates and maintaining data privacy. Moreover, federated learning combined with zero-trust policies eliminates centralized dependency of data and improves adaptive control access of network elements in dynamic network context. The findings illustrate how the suggested method has the potential of establishing scalable, privacy conscious, and robust intrusion detection systems in next generation distributed communication networks.

Keywords: Federated Learning, Intrusion Detection Systems, Privacy-Preserving Security, Zero-Trust Architecture, Zero-Trust Network Access.

Introduction

The swift development of distributed communication systems, such as cloud computing, Internet of Things (IoT), edge computing and the new 6G infrastructures, contributed significantly to the attack surface of current networks. With the implementation of highly interrelated systems in various areas of administration, the conventional models of perimeter security no longer suffice in securing sensitive digital resources. Cyber attackers are using the weaknesses of distributed environments more and more to create advanced intrusions that disregard traditional defense mechanisms. As a result, intelligent, scalable, and privacy-preserving intrusion detection mechanisms, which can be effectively used in the context of decentralized infrastructures, are increasingly needed (Aloqaily et al, 2025) (Alnaim & Alwakeel, 2025).

The Intrusion Detection Systems (IDS) are important in determining the presence of malicious activities and the security of communication networks. Nevertheless, much of the traditional IDS methods use the centralized data collection and processing, and the network traffic and security logs are pooled at a central location and analyzed through a central server. Although it makes model training and monitoring simpler, this architecture also brings with it a number of shortcomings such as privacy threats, excessive communication cost, and scalability in large distributed settings (Chandu et al, 2025) (Mazid et al, 2025). Organizational information can be sensitive and can be compromised during transmission or storage and centralized IDS frameworks cannot be applied to privacy sensitive domains like healthcare, finance and industrial systems.

Federated Learning (FL) has become the potential solution to these constraints, as it makes it possible to perform collaborative machine learning without sharing raw data. In FL, the local models are trained locally on local data and only model parameters or gradients are shared with an aggregation server in the central location, thus preserving privacy of data and allowing global model to be improved (Hossain et al, 2025) (Puviarasu & Sudha, 2026). It has been shown that this decentralized learning method has significant potential in the field of cybersecurity, especially in distributed intrusion detection systems, where data privacy and scalability are paramount factors (Javeed et al, 2024) (Mrabet, 2025).

Meanwhile, the Zero-Trust Security Model has recently become one of the most popular security models that is aimed at substituting the conventional implicit trust in the network setting. The principle of zero trust adheres to the philosophy of never trust, always verify and every access request has to be continuously authenticated, authorized, and validated irrespective of its source (Potluri, 2024) (Kokku, 2025). The Zero-Trust Network Access (ZTNA) mechanisms present adaptive risks considerations to contextual data to assess the risk based on the identity of the user and the device integrity, alongside the patterns of behavior, and then determine network access. This has worked especially well in the securing of distributed systems, edge computing settings, and next-generation communication systems (Asad & Otoum, 2024) (El-Hajj, 2025).

The recent research has investigated the implementation of federated learning and zero-trust architecture to improve the security of distributed systems. As an example, IoT and industrial settings are suggested to use FL-based systems of intrusion detection

powered by decentralized learning to enhance the accuracy of threat detection and maintain privacy (Al-Sharafi et al, 2025) (Laghari et al, 2025). Likewise, other papers have examined the model of zero-trust-based collaborative intrusion detection that integrates dynamic trust management with distributed machine learning methods (Wardana et al, 2024) (Ullah et al, 2025). Other methods also involve the use of blockchain or secure communication system to create trust and integrity in federated environments (Sharma et al, 2025) (Varadala & Xu, 2025). Regardless of these developments, several of the current solutions have issues connected to efficient incorporation of intrusion detection engines and zero-trust policy engines, scalability among heterogeneous edge devices, and efficient deployalties of enhanced deep learning designs in distributed threat detections (Abbas et al, 2025) (Zhou et al, 2025).

Despite the fact that both federated learning and zero-trust architectures have shown serious prospects of further improving network security, there is little integration of both in the intrusion detection systems. Conventional IDS models rely on the existence of central data repository points, which reveal the sensitive data and make them vulnerable to data breaches. Moreover, a lot of the distributed IDS models do not have dynamic access control that can adapt to the changing network threats. The modern distributed communication systems are susceptible to advanced cyberattacks without a detailed security framework that would both implement privacy-sensitive learning and incorporate adaptive trust assessment.

Moreover, the solutions currently available tend to be based on mono model machine learning and do not have the ability to learn more complex spatial and temporal patterns of attacks that are demonstrated by the modern network traffic. Because cyber threats are getting more sophisticated, it is required that more advanced hybrid deep learning architectures can be seen to analyze multi-dimensional network behaviors and can work effectively in decentralized environments (Chandu et al, 2025) (Mazid et al, 2025). Thus, learning on a single framework, incorporating federated learning, deep learning-based intrusion detection, and zero-trust network policies is necessary to protect next-generation distributed networks.

This study is mainly aimed at creating a privacy-conservative intrusion detection system, which incorporates federated learning and zero-trust network access schemes to distributed communication networks. The proposed solution will help to improve security, scalability, and privacy and decrease reliance on the centralized data collection.

The key achievements of this paper can be summarized as follows:

1. Federated Intrusion Detection Architecture: It presents a new three-layer architecture, which combines edge-based models of intrusion detection, a federated learning aggregation server, and a zero-trust policy engine to provide decentralized threat detection in distributed communication systems.
2. privacy preserving distributed learning: It has a framework that uses federated learning to learn intrusion detection models on many edge nodes without sharing raw data and, therefore, does not violate user privacy and minimizes communication overhead.

3. Deep Learning Hybrid IDS Models: The suggested system is based on several deep learning networks, such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Transformer systems, that allow capturing both spatial and temporal features of network traffic.
4. There should be a Zero-Trust Access Control Integration: The intrusion detection results are combined with a zero trust policy engine that dynamically determines the access decisions based on the trust scores and network risk analysis.
5. Extensive Experimental Evaluation: Detection accuracy, false positive, privacy preservation, communication overhead, and model convergence performance are assessed as the proposed framework is analyzed on benchmark cybersecurity datasets, such as UNSW-NB15, CSE-CIC-IDS2018 and TON IoT.

The originality of the presented study is that federated learning-based intrusion detection is closely combined with a framework of zero-trust network access decisions, which allows privacy preserving threat detection and dynamic security enforcement in distributed communication systems. The framework proposed is in contrast to conventional models of the IDS as it is distributed over edge nodes, unlike the traditional models that use centralized data gathering, collaborative model improvement is achieved via federated aggregation.

Moreover, the system enables the identification of complex attack patterns more efficiently than single-model systems, because the integration of multiple deep learning architectures (CNN, LSTM, and Transformer) into the federated learning process is efficient. Another layer of security is the zero-trust policy engine which enables intrusion detection results to be included in the dynamic access control decision-making to ensure that access to the network is provided based on satisfying predefined security limits, both of the user trust scores and network risk level.

The proposed solution will act as a scalable, privacy-sensitive, and responsive cybersecurity model that federated learning, hybrid deep learning models, and zero-trust access control tools will offer to next-generation distributed network, such as IoT ecosystems, edge computing infrastructures, and future 6G networking.

Literature Review

The blistering growth in the distributed computing environment, i.e., Internet of Things (IoT), edge computing, and next-generation wireless networks has drastically altered the cybersecurity scene. Conventional centralized security systems are becoming inefficient in dealing with highly distributed architectures where huge size of heterogeneous data is created across a large number of nodes. Therefore, scholars have looked into new paradigms that integrate federated learning (FL) and zero-trust security frameworks to enhance intrusion detection potentials without violating the privacy and scalability of the data. This part will examine the most pertinent research on the topic of federated intrusion detection, zero-trust networking, and hybrid systems that combine these technologies.

Zero-Trust Security Model has become an important paradigm in the context of protecting the current network infrastructures by removing implicit trust in internal networks. Rather, zero-trust ensures verification of identities, devices and behaviors, and then provides access to resources in a constant manner. Aloqaily et al. (2025) explain that zero-trust architectures are emerging as the baseline to ensure the security of the next-generation communication networks, especially in organizations that are moving towards the decentralized computing space. In the same vein, Alnaim and Alwakeel (2025) noted that zero-trust mechanisms are crucial to protecting edge and fog computing in new 6G networks, where massive populations of distributed devices and devices are needed to perform dynamic authentication and risk evaluation.

Some of the research studies have suggested frameworks that utilize the concept of zero-trust in network security designs. Potluri (2024) proposed a model of a zero-trust identity and access management that is applicable to cross-cloud federated settings and allows safe communication across two or more cloud domains. A further conceptualization of this idea is proposed by Kokku (2025) who combined dynamic trust management and federated learning to enhance the security of IoT infrastructure. Another concept proposed by Li et al. (2025) is the idea of zero-trust foundation models that involve artificial intelligence and collaborative learning to develop secure and scalable security frameworks of the IoT ecosystems.

The use of the zero-trust models in particular areas of the network has been examined in other studies. El-Hajj (2025) suggested a zero-trust and federated learning-based optimization models in Open Radio Access Networks (O-RAN) in the 6G conditions, and the critical role of dynamically adaptive trust checking was noted in extremely dynamic wireless networks. Equally, Varadala and Xu (2025) also designed a federation-based decentralized zero-trust architecture of satellite networks incorporating post-quantum cryptography mechanisms and federated learning to improve the security and detection of anomalies.

Federated learning is a type of machine learning that has attracted a lot of attention as a distributed paradigm that enables different devices to train models without exchanging raw data. The method is especially useful in cases of cybersecurity use where privacy and confidentiality of data are paramount. Chandu et al. (2025) introduced a federated intrusion detection architecture to distributed IoT networks and showed that decentralized model training can be useful in enhancing the accuracy of attack detection at the same time sensitive information can be stored at the local nodes.

In an equal measure, Mazid et al. (2025) presented the FL-IDPP model, which is a federated learning-based intrusion detection system that aims at offering privacy-respectful threat detection in distributed settings. They showed better results in detection with their framework and reduced the risks of data leakage with centralized training. Puviarasu and Sudha (2026) also designed a federated learning-based security solution that will provide the capability to detect intrusion in real-time across the IoT devices with a high detection rate and data privacy.

Moreover, Wardana et al. (2024) designed a lightweight collaborative intrusion detection system, which integrates the mechanisms of trust management to increase the reliability of distributed security models. Mrabet (2025) proposed a trust-based federated learning model that can be used to share cyber threat intelligence in a distributed organization. The paper highlighted the significance of trust assessment in cooperative intrusion detection systems so as to guarantee credible information sharing of threats.

The recent studies have concentrated on the combination of federated learning and zero-trust security architecture to overcome the shortcomings of both technologies. Asad and Otoum (2024) came up with a model that integrates federated learning and zero-trust in order to establish safe wireless communication systems. Their solution proved to be more secure in terms of the network protection as it would allow collaboration in intrusion detection and impose rigorous access control policies.

In a comparable way, Javeed et al. (2024) presented a federated learning-based zero-trust intrusion detection system to work with the IoT networks. Their model is a combination of distributed learning and zero-trust verification to identify cyber threats and maintain the privacy of data among devices. Hussain et al. (2024) advanced the given approach with the implementation of both differential privacy and the use of blockchain technologies in the framework of federated learning to gather the information on the different level to share it safely and without losing its privacy in the conditions of the IoT.

The Al-Sharafi et al. (2025) suggested a federated framework of attack detection based specifically on the consumer IoT setting and built on the principles of zero-trust security. Their design proved that it is possible to identify malicious activity of distributed devices without necessarily centralizing data. Laghari et al. (2025) proposed a zero-trust-based industrial IoT architecture intrusion detection using an artificial intelligence-assisted system, which indicated that AI-based security systems have the potential to achieve industrial infrastructure security.

Still, other works have presented new and enhanced architectures of combining and integrating several technologies with federated learning and zero-trust models. Shah et al. (2025) suggested a privacy-friendly federated system of software-defined networking (SDN) space that incorporates zero-trust blockchain systems and 6G terahertz networks to promote greater attack detection. Sharma et al. (2025) introduced a zero-trust network with blockchain to provide a federated transfer learning to achieve the security of Industry 5.0 IoT.

As next-generation networks (6G and large-scale IoT ecosystems) emerged, researchers considered more advanced security frameworks that involve the new technologies. A GDPR-compliant federated learning architecture proposed by Abbas et al. (2025) incorporates the concepts of the zero-trust in order to provide privacy-preserving collaborative learning. They are designed with the focus on the regulatory compliance and with the high security provisions.

To eliminate IoT-related cyber threats, such as power terminals, Al Shahrani et al. (2024) designed a federated learning model based on blockchain with an edge-based zero-trust structure to reduce cyber threats. On the same note, Alzahrani (2025) suggested a

quantum-enhanced federated learning framework that would be incorporated into zero-trust blockchain technologies to detect anomalies in a 6G IoT network.

Zhou et al. (2025) presented a decentralized federated graph learning system, which includes a lightweight zero-trust architecture of next-generation networking security. Their solution was found to be more scalable and performance based in detecting intrusion over the network. Another neurosymbolic AI-based model of zero-trust intrusion detection suggested by Ullah et al. (2025) is to apply federated meta-learning approaches to boost the detection accuracy of Internet of Vehicles (IoV) settings.

Moreover, Matam et al. (2026) investigated privacy-oriented cloud AI systems that combine federated learning and zero-trust technology to ensure the safe cooperation on various spheres. Mahamad (2024) offered a federated AI and cloud-based cybersecurity framework that is aimed at underpinning the concept of zero-trust security with regard to large-scale digital ecosystems.

Despite the fact that considerable efforts have been made in terms of combining federated learning with zero-trust architecture, there are still quite a few challenges to overcome. Firstly, most of the current frameworks are only concentrated on individual machine learning models which do not allow them to uncover complex spatial and temporal characteristics of network traffic. Second, some of the suggested systems depend extensively on blockchain or other infrastructure elements which can create computational load and scalability issues. Third, little research has been conducted on the idea of incorporating hybrid deep learning models (CNN, LSTM and Transformer models) in federated intrusion detection models.

Also, the current solutions tend to separate intrusion detection and access control, instead of incorporating them into a single security solution. Closely linked set of functions that integrate distributed intrusion detection with dynamic zero-trust policy can greatly improve the security and resiliency of distributed communication systems.

In order to overcome these drawbacks, the proposed study is a new federated learning-based intrusion detection system with a zero-trust network access policy engine. The suggested architecture utilizes hybrid deep learning models and decentralized training to enhance performance on detection and maintain privacy of data. Additionally, the system also combines the results of intrusion detection with zero-trust access decisions, and in this way, such capabilities promote adaptive intelligent enforcement of the security of distributed communication systems.

Methodology

This section provides a description of the proposed Zero-Trust Network Access with Federated Learning framework of Privacy-preserving Intrusion Detection in Distributed Communication Systems. The methodology incorporates federated deep learning models, distributed edge-based intrusion detection, and an engine based on a zero-trust policy to offer scalable and privacy-preservation cybersecurity protection. The suggested system will

be used to run in distributed settings like IoT networks, cloud-edge networks, and next-generation communication systems.
It comprises five major subsections of the methodology system architecture, dataset preparation, model development and federated learning process, zero-trust integration and experimental environment.

Overall System Architecture

The suggested framework is based on three-layer architecture that is meant to aid decentralized training and dynamically implemented security enforcement. The architecture includes:

1. Edge Nodes Layer
2. Federated Learning Aggregation Server
3. Zero-Trust Policy Engine

The different layers carry out certain functions to guarantee the preservation of privacy, effective model training and adaptive access control.

1. Edge Nodes Layer (Data Sources)

Edge nodes are distributed network elements which include IoT devices, routers, cloud gateways or enterprise servers. Data on the network traffic are also locally collected by each node and the intrusion detection model of the node is also trained.
The major functions of edge nodes are:

- Local network traffic monitoring
- Feature extraction
- Local IDS model training
- Transmission of model parameters to the federated server

Compared to the conventional centralized IDS models, raw data is not transferred to the edge nodes, which implies a high level of privacy protection.
Let:

$$D_i = \{ (x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\} \quad (1)$$

where:

- D_i = local data of edge node i.
- x = feature observation of network traffic.
- y = label (normal or attack)

Every node of the edges develops a local model on its dataset D_i.

2. Federated Learning Aggregation Server

The federated aggregation server is what it coordinates collaborative learning of many edge nodes, without traveling to their local datasets.
The process includes:

1. Getting the global model to contributing nodes.
2. Getting locally trained model parameters.
3. Combining parameters with the Federated Averaging (FedAvg) algorithm.

4. Updating the global model.

The FedAvg aggregation has the following definition:

$$w_{\{t+1\}} = \sum_{\{i=1\}}^{N} \left(\frac{n_i}{n}\right) w_{\{i\ t\}} \quad (2)$$

Where:

- w_{t+1} = global model parameters after updating.
- $w_{\{i\ t\}}$ = parameters of node i at round t.
- n_i = number of samples at node i
- n = total number of samples across all nodes
- N = number of participating nodes

This protocol allows collaborative learning and provides data locality and preservation of privacy.

3. Zero-Trust Policy Engine

The third tier is the Zero-Trust Policy Engine that makes dynamic decisions about access control to users considering the risk analysis.

The zero-trust engine is an assessment of:

- User trust score
- Device integrity
- Intrusion detection output
- Network risk level

The access decision functionality is as follows:

$$Access = f(T_u + R_n) \quad (3)$$

Where:

- T_u = user trust score
- R_n = score of network risk produced by IDS.
- f(·) = decision function

Access rules are defined as:

$$Access = \{ Allow\ if\ T_u - R_n > \theta \quad Deny\ otherwise \} \quad (4)$$

where θ signifies the level of security.

The given dynamic mechanism can be used to perform continuous authentication and risk-based authorization that is adaptive.

The suggested intrusion detection system is a three-layer architecture comprising of distributed edge nodes, a federated learning aggregation server, and a zero-trust policy engine. Edge nodes are locally trained on intrusion detection models with their own traffic data and the federated server consolidates model parameters without ever seeing raw data. The zero-trust engine scores the risk scores generated by the IDS models, and dynamically makes access decisions. Fig. 1 depicts the general structure of the suggested system.

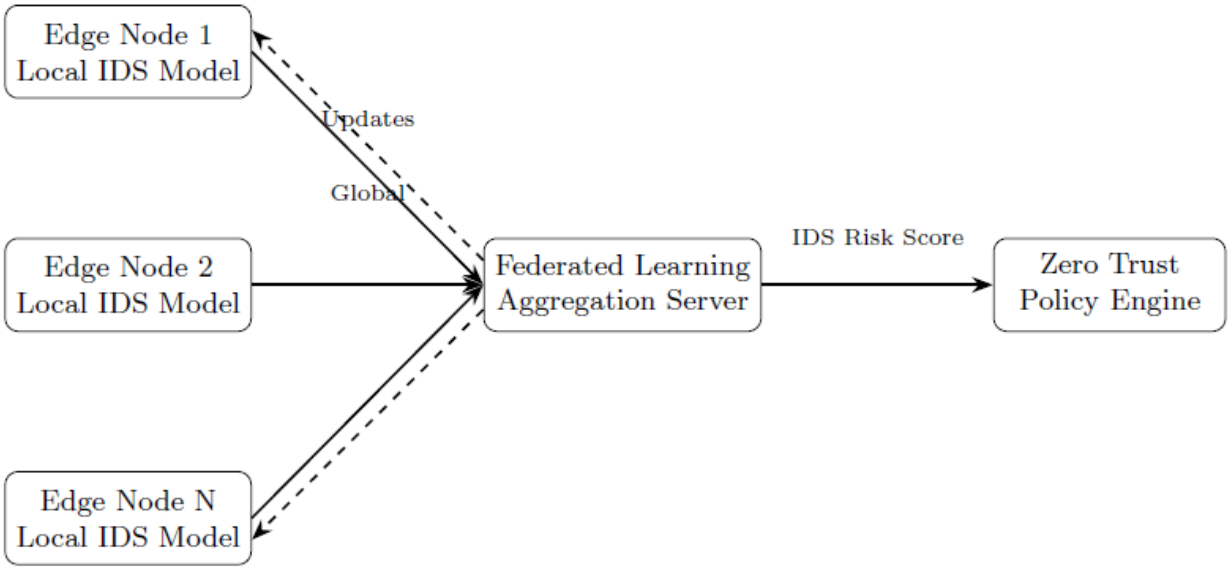

Figure 1. Architecture of the Proposed Zero-Trust Federated Intrusion Detection Framework

Dataset Description

To assess the efficiency of the proposed system, there are three datasets commonly used in cybersecurity that are employed:

1. UNSW-NB15 Dataset

The UNSW-NB15 data file is a contemporary artificial network traffic by utilizing the IXIA PerfectStorm simulator.

The characteristics of the data set are:

- 2.5 million network records
- 49 traffic features
- 9 attack categories

Attack types include:

- DoS
- Exploits
- Reconnaissance
- Worms
- Shellcode

This data is very popular in the testing of machine learning-based IDS systems.

2. CSE-CIC-IDS2018 Dataset

CSE-CIC-IDS2018 is one of the most extensive datasets of intrusion detection.

Key characteristics:

- real enterprise network traffic.
- multiple attack scenarios
- labeled traffic flows

Attack categories include:

- DDoS
- Botnet

- Brute force
- Web attacks
- Infiltration

The data allows to analyze the multi-stage attack in complicated conditions.

3. TON_IoT Dataset

The TON IoT data is concentrated on IoT and edge computing spaces.

Dataset features include:

- telemetry data
- network traffic logs
- IoT device activity

Attack types include:

- ransomware
- backdoor attacks
- scanning attacks
- data exfiltration

This set of data helps to test the framework in the environment of IoT and distributed devices.

Data Preprocessing and Feature Engineering

A number of preprocessing steps are undertaken before the training of the models.

1. Data Cleaning

The activities carried out are as follows:

- removal of missing values
- removal of records of duplications
- standardization of numerical variables

It is normalised using Min-Max:

$$x' = \frac{(x - x_{min})}{(x_{max} - x_{min})} \quad (5)$$

2. Feature Encoding

Categorical characteristics like the protocol type or service type are coded with:

- One-Hot Encoding
- Label Encoding

3. Feature Selection

The selection of features is done using:

- Mutual information
- Correlation filtering
- Principal Component Analysis (PCA)

This is a dimensionality-reduction step which enhances the performance of the model.

4. Intrusion Detection Model Development

The suggested framework applies three deep learning models to identify various trends in network traffic.

Convolutional Neural Network (CNN)

The CNN models are useful in eventuating spatial associations amid features.

Architecture:

- Input layer
- Convolution layers
- ReLU activation
- Max pooling
- Fully connected layer
- Softmax classifier

Convolution operation may be defined as follows:

$$y_{\{i,j\}} = \sum_m \sum_n x_{\{i+m,j+n\}} k_{\{m,n\}} \quad (6)$$

Where:

- x = input feature map
- k = convolution kernel

Long Short-Term Memory (LSTM)

The LSTM networks express time variation of network traffic through a sequence.

LSTM equations:

Forget gate:

$$f_t = \sigma\left(W_f \left[h_{\{t-1\}}, x_t \right] + b_f \right) \quad (7)$$

Input gate:

$$i_t = \sigma\left(W_i \left[h_{\{t-1\}}, x_t \right] + b_i \right) \quad (8)$$

Cell state update:

$$C_t = f_t * C_{\{t-1\}} + i_t * C\sim_t \quad (9)$$

Output gate:

$$o_t = \sigma\left(W_o \left[h_{\{t-1\}}, x_t \right] + b_o \right) \quad (10)$$

Hidden state:

$$h_t = o_t * tanh(C_t) \quad (11)$$

Transformer-Based Model

Transformers are able to gather long-range dependencies via self-attention mechanisms.

The self-attention is calculated as:

$$Attention(Q, K, V) = softmax\left(\frac{(Q\, K^T)}{\sqrt{d_k}} \right) V \quad (12)$$

Where:

- Q = query matrix
- K = key matrix
- V = value matrix

Transformer models are very effective in the complex network traffic analysis.

Federated Learning Training Procedure

The federated learning process is executed in series of communication rounds.

Step 1: Initialization of Global Model.

Initialization of model parameters: The parameters of the models are initialised at the central server:

$$w_0 \quad (13)$$

and disseminates them to all the involved nodes.

Step 2: Local Model Training

The models in each node are trained locally in a few epochs:

$$w_{\{i,t+1\}} = w_{\{i,t\}} - \eta \nabla L\left(w_{\{i,t\}}\right) \quad (14)$$

where:

- η = learning rate
- L = loss function

Step 3: Model Parameter Upload

Rather than raw data is shared, model updates are transmitted by each node to the server.

Step 4: Federated Aggregation

FedAvg is used to aggregate parameters by the server.

Step 5: Global Model Update

The new global model is reallocated to edge nodes.

This is repeated till convergence.

Federated learning training procedure is an iterative process in which edge nodes can only communicate model parameters with the central server. These parameters are aggregated by the aggregation server based on Federated Averaging algorithm and the revised global model is redistributed to the participating nodes. The general training process is depicted in Fig. 2.

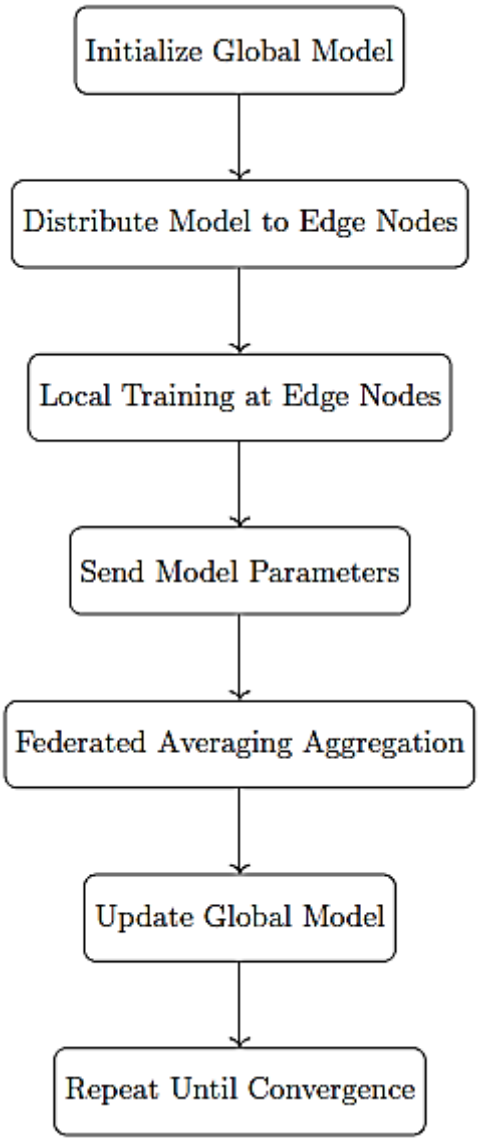

Figure 2. Federated Learning Training Workflow

Experimental Environment

The distributed computing infrastructure is used to implement the proposed system.

1. Software Tools

The following tools are used:

- TensorFlow Federated
- PyTorch
- Docker containers
- Kubernetes orchestration

The tools allow simulating large-scale distributed environments.

2. Hardware Configuration

In the experimental setup, it has:

- multi-node edge simulation
- Training with the help of GPU.
- distribution of containers deployment.

Typical configuration:

- CPU: Intel Xeon processors
- GPU: NVIDIA RTX series
- RAM: 64GB
- Storage: SSD clusters

Evaluation Metrics

In order to determine the success of the framework proposed, some evaluation metrics are applied.

Detection Accuracy

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (15)$$

False Positive Rate

$$FPR = \frac{FP}{(FP + TN)} \quad (16)$$

Precision

$$Precision = \frac{TP}{(TP + FP)} \quad (17)$$

Recall

$$Recall = \frac{TP}{(TP + FN)} \quad (18)$$

F1-Score

$$F1 = 2 \times \frac{(Precision \times Recall)}{(Precision + Recall)} \quad (19)$$

Privacy Leakage: The privacy is quantified by the exposure of information in the model update that is transmitted.

Communication Overhead: This is determined as the sum of the size of transmitted model parameters across all nodes and the central server.

Model Convergence Speed: It is a number used to measure the number of federated rounds that come to a stable performance.

Summary of the Method

The given methodology combines federated deep learning-based intrusion detection with zero-trust network access control to offer the scalable and privacy-preserving framework of cybersecurity. The architecture will allow training distributed models on the distributed edge nodes and coordinate centrally through federated aggregation. Using CNN, LSTM and Transformer models, the system completely understands network traffic patterns that are complicated. Moreover the incorporation of intrusion detection outputs into the zero-trust policy engine enables real-time access decisions by use of real risk assessment. This method largely improves the security, scalability and privacy of intrusion detection solutions in distributed communication system.

Results and Discussion

In this section, the experimental findings will be discussed based on testing the suggested Zero-Trust Network Access with Federated Learning (ZTNA-FL) intrusion detection system. The experiments evaluate the workability of the suggested system concerning detection capability, the preservation of privacy, communication effectiveness, and convergence of the model. These are determined by the three benchmark cybersecurity datasets, including UNSW-NB15, CSE-CIC-IDS2018, and TON_IoT. The effectiveness of the proposed hybrid federated IDS is compared to the use of a couple of baseline models to prove its performance.

The experiments have been performed in a simulated distributed environment by means of using Docker-based edge nodes which are coordinated by a Kubernetes cluster, and the federated learning models have been implemented with the help of TensorFlow Federated and PyTorch. All the edge nodes were training local IDS models with their own datasets partition and model parameters were aggregated by the federated learning server on the Federated Averaging (FedAvg) algorithm.

Experimental Setup

Ten distributed edge nodes are in the experimental configuration with each node holding a part of the training dataset. The system runs 50 communication rounds with each node training its local model five local epochs, per federated round.
The hybrid IDS model incorporates three deep learning models:

- Convolutional Neural Network (CNN)
- Long Short-Term Memory (LSTM)
- The intrusion detection model based on transformers.

The weighted ensemble strategy is used to obtain the final prediction and enhance the detection performance and resistance to various attack patterns. (See Table 1)

Table 1.
Training Hyperparameters

Parameter	Value
Learning rate	0.001
Batch size	64
Local training epochs	5
Federated rounds	50
Optimizer	Adam
Activation function	ReLU / Softmax
Edge nodes	10

Intrusion Detection Performance

The former group of experiments assesses the accuracy of intrusion detection of the proposed federated IDS system. There are various baseline methods where performance is compared:

- Centralized CNN IDS
- Federated CNN IDS
- Federated LSTM IDS
- Proposed CNN-LSTM-Transformer Federated IDS hybrid.

Table 2 shows the comparison between several models.

Table 2.
Detection Performance Comparison Across Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Centralized CNN	94.8	93.6	92.7	93.1
Federated CNN	95.6	94.9	94.1	94.5
Federated LSTM	96.4	95.8	95.2	95.5
Proposed Hybrid FL Model	98.1	97.5	97.3	97.4

The outcomes prove that hybrid federated IDS is to be significantly more effective than single deep learning models. The addition of CNN, LSTM and Transformer architecture allows the system to capture both spatial correlation of features and temporal patterns of traffic and this leads to better detection performance.

Transformer attention mechanism helps the model to capture long-range dependencies in the network traffic that would help to increase the rate of complex attacks recall.

A performance analysis was performed among a number of baseline methods and the proposed hybrid federated IDS model to compare their ability of detection in comparison to different intrusion detection models. Fig. 3 presents the comparison of accuracy in the detection of these models.

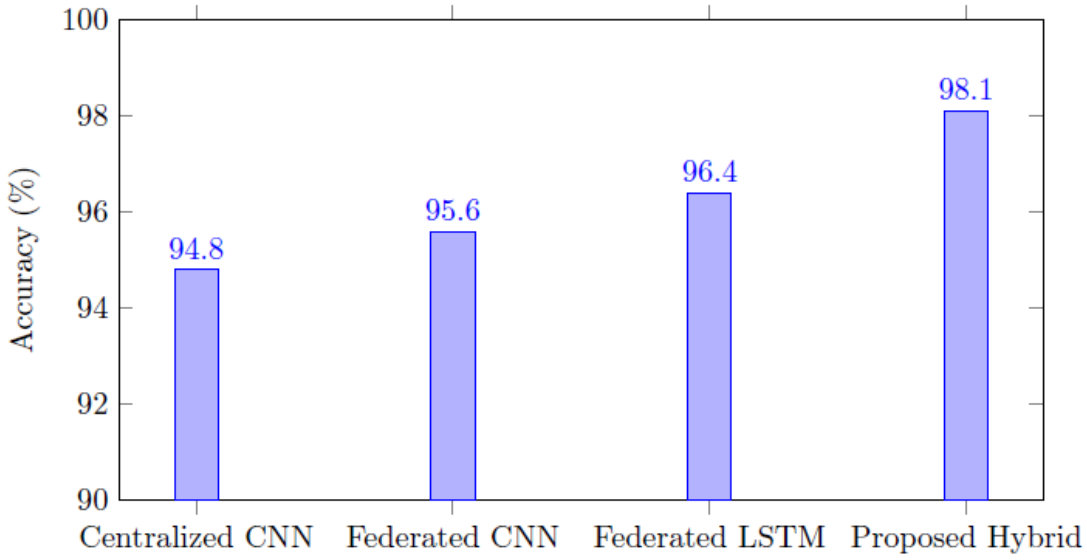

Figure 3. Detection Accuracy Comparison of Intrusion Detection Models

False Positive Rate Analysis

False alarm reduction is another crucial aspect of intrusion detection system since it can adversely affect the working conditions. (See Table 3)

Table 3.
False Positive Rate Comparison

Model	False Positive Rate (%)
Centralized CNN	5.4
Federated CNN	4.7
Federated LSTM	4.1
Proposed Hybrid FL Model	2.6

The lowest false positive rate is obtained with the proposed system, which proves the fact that the hybrid architecture enhances reliability in classifications. False alarms reduction is a mandatory requirement of zero-trust security settings where false alarms may inappropriately prevent valid users.

Dataset-Specific Performance

In order to test the robustness, the proposed model was applied to three benchmark cybersecurity datasets. (See Table 4)

Table 4.
Detection Accuracy on Different Datasets

Dataset	Accuracy (%)	Precision (%)	Recall (%)
UNSW-NB15	97.6	96.9	96.7
CSE-CIC-IDS2018	98.4	97.9	97.6
TON_IoT	97.3	96.5	96.2

The findings suggest that the suggested system remains on a level of high performance in various datasets of cybersecurity, which proves to be highly generalized. Maximum accuracy is obtained on CSE-CIC-IDS2018, which has various attack scenarios and realistic enterprise network traffic.

Privacy Preservation Analysis

The protection of data privacy is one of the key reasons that have driven the federated learning. The proposed framework does not exchange raw traffic data as centralized IDS systems do because it only exchanges model parameters among nodes. (See Table 5)

Table 5.
Privacy Leakage Comparison

Approach	Raw Data Sharing	Privacy Leakage Risk
Centralized IDS	Yes	High
Distributed IDS	Partial	Medium
Federated IDS	No	Low
Proposed ZTNA-FL Framework	No	Very Low

The framework suggested will dramatically minimize the chances of leaking privacy since sensitive traffic information is held locally at every edge node.

Communication Overhead Evaluation

Federated learning causes communication overheading because model parameters are being transferred between edge nodes and the central server. (See Table 6)

Table 6.
Communication Cost per Training Round

Method	Communication Overhead (MB)
Centralized Training	480
Federated CNN	220
Federated LSTM	235
Proposed Hybrid FL Model	248

The hybrid model has a small size addition to the parameters, but the total cost of communication is much lower than the centralized transmission of data.

Model Convergence Analysis

The number of federated rounds to convergence is another important evaluation measure. (See Table 7)

Table 7.
Convergence Speed Comparison

Model	Convergence Rounds
Federated CNN	45
Federated LSTM	38
Proposed Hybrid FL Model	32

The hybrid model is able to converge quicker because complementary capabilities of the CNN, LSTM and Transformer elements make it possible to complete the gradient updates with reduced time during the federated aggregation.

The convergence rate of the global model is another significant assessment criterion of federated learning systems. Increased speed of convergence leads to less communication overhead and better training. The cost of the evaluated models towards the convergence behavior is presented in Fig. 4.

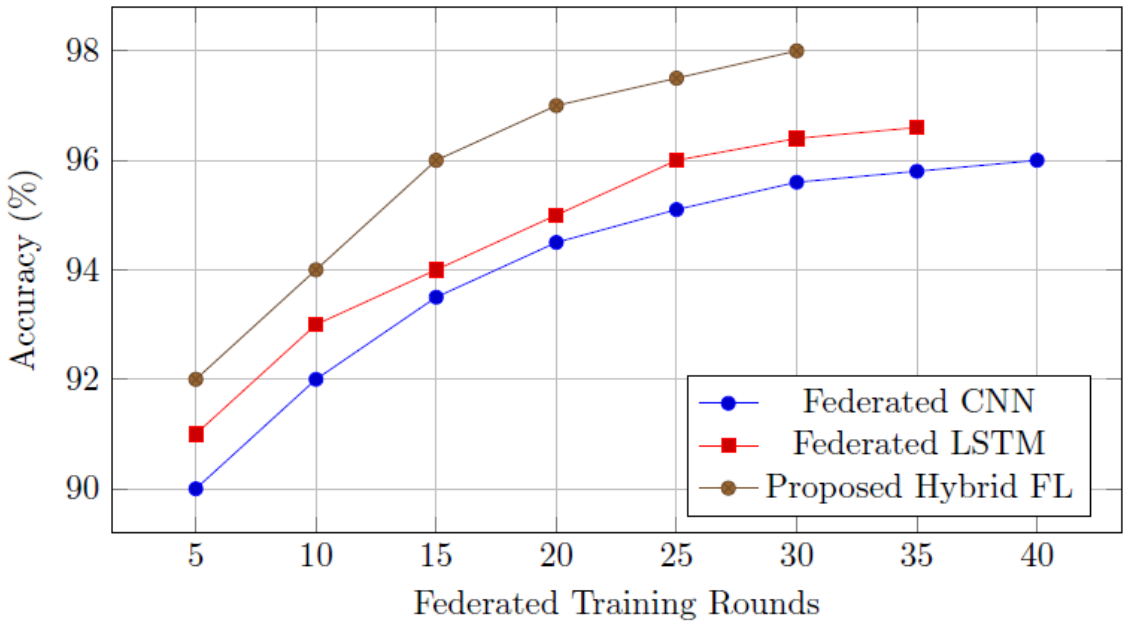

Figure 4. Convergence Performance of Federated Intrusion Detection Models

Zero-Trust Access Control Evaluation

The combination of the intrusion detection results with the Zero-Trust Policy Engine allows taking the dynamic access decisions toward the network risk level.
The risk score is computed as:

$$Risk = \alpha \times IDS_{Score} + \beta \times Network_{Anomaly} \quad (20)$$

Where:

- IDS_{Score} :This is the likelihood of the IDS to predict malicious behavior.
- $Network_{Anomaly}$ indicates the indicators of abnormal network activity.
- α, β are weighting parameters

Table 8 illustrates the evaluation.

Table 8.
Zero-Trust Access Decision Evaluation

Scenario	IDS Risk Score	Access Decision
Normal traffic	0.12	Allow
Suspicious activity	0.46	Monitor
High-risk attack	0.81	Deny

This mechanism identifies continuous authentication and adaptive access control which enhances the network security.

The proposed framework combines intrusion detection output and zero-trust access policy to dynamically decide whether a user or a device is to access the network. The choice is made based on a unified approach to the user trust score and network risk score provided by intrusion detection system. The mechanism used in decision-making is shown in Fig. 5.

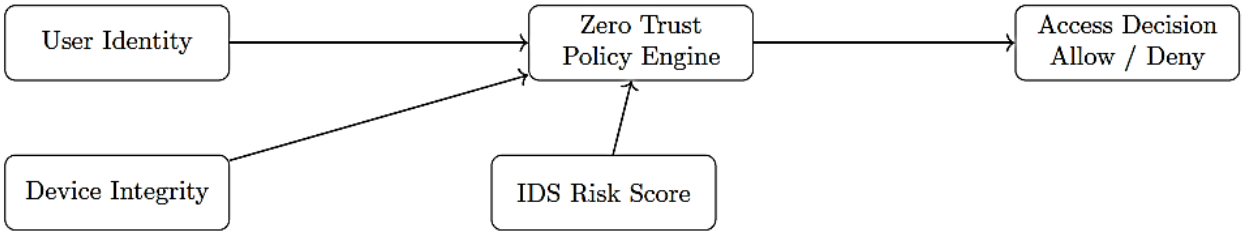

Figure 5. Zero-Trust Risk-Based Access Control Model

Discussion

The experiment findings illustrate that federated learning with the zero-trust network access control mechanisms is a reasonably effective approach to enhance security and scalability of intrusion detection systems. The suggested framework has a number of benefits compared to conventional IDS methods.

To start with, the hybrid deep learning model greatly increases the performance in detection since it integrates the CNN to extract spatial features, LSTM to identify temporal sequences, and Transformer attention to extract the long-range dependencies. This scenario enables the system to easily identify sophisticated multi-stage cyberattacks.

Second, the federated learning architecture provides a high level of privacy by removing the centralized data collection requirement. Network traffic data is sensitive, and it is not moved to central nodes in the network, thus minimizing the chances of data breach and regulatory violations.

Third, the combination with the zero-trust protection systems of access control improves the capacity of the system to react on the cyber threats on the ground. The system can automatically limit the network access by connecting the intrusion detection outputs to dynamic trust evaluation.

Lastly, the given framework is shown to perform efficiently in terms of communication and converge quicker, thus being applicable in large-scale distributed systems including IoT platforms, cloud-edge solutions, and the next-generation communication systems.

Altogether, the findings do support the idea that the suggested ZTNA-FL intrusion detection framework offers a scalable, privacy-saving, and very accurate cybersecurity concept to distributed communication systems.

Conclusion

The paper has introduced a new Zero-Trust Network Access with Federated Learning (ZTNA-FL) architecture that ensures privacy-enhancing intrusion detection in distributed communication systems. The suggested solution will overcome some of the important shortcomings of the conventional intrusion detection systems, especially their centralized approach to data collection, which creates privacy problems, scalability factors, and high communication costs. The proposed framework, which combines the principles of federated learning and zero-trust security, allows model training on both distributed edge nodes in collaboration, and on top of this, sensitive network traffic data is kept locally. Such

a decentralized learning model is much better in terms of privacy protection but at the same time, it offers high rates of intrusion detection.

The system proposed follows a three-layer architecture system) (edge nodes, federated learning aggregation server, and a zero-trust policy engine. Edge nodes locally train deep learning-based models of intrusion detection by using network traffic data and the federated server combines model updates with the Federated Averaging (FedAvg) algorithm to produce a global model. In addition, with the combination of the intrusion detection outputs and the engine of a zero-trust policy, it is possible to make dynamic and risk-aware access control decisions, depending on user trust scores and network risk levels. The architecture offers an all-encompassing security system that can safeguard distributed architectures like IoT networks, cloud-edge systems, and next-generation communication systems.

The performance of the proposed framework was evaluated through well-established cybersecurity datasets, such as UNSW-NB15, CSE-CIC-IDS2018, and TON_IoT, to examine the effectiveness of the proposed framework. The findings reveal that the hybrid federated learning framework using Convolutional Neural Networks (CNN), Long Short-Term memory (LSTM) networks, and Transformer models is more effective in the intrusion detection than the traditional centralized and single-model federated setup. The system proposed gave greater detection accuracy, low false positive rates, and faster model convergence speed with low privacy leakage rates. Moreover, the federated training resulted in a large reduction of centralized data dependency and, thus, made the system more scalable and adaptable to big distributed networks.

Another aspect that can make the framework more efficient in terms of security is the incorporation of zero-trust access control systems that provide the ability to conduct an ongoing authentication process and risk-based decision-making. The system will have the capability of enforcing network access policies in real time and mitigating possible cyber threats by correlating intrusion detection outputs with trust assessment measures. Such a federated learning-based intrusion detection and zero-trust policy enforcement would offer a highly effective defense system against complex cyberattack on distributed communication infrastructures.

On the whole, the proposed ZTNA-FL intrusion detection framework has a great potential of being used to secure contemporary distributed networks through integrating privacy saving machine learning and adaptable zero-trust security frameworks. The architecture provides an intelligent, privacy-aware, and scalable cybersecurity system with the potential to deal with the increasing challenges of decentralized digital ecosystems.

The future studies can be directed towards using blockchain-based trust management systems, adaptive federation optimization schemes and lightweight edge artificial intelligence schemes to even improve the scalability and resilience of a system. Furthermore, it can be of interest to investigate real use cases in the large-scale IoT and 6G communication networks and assess the feasibility of the proposed framework in practice.

References

Abbas, Z., Ahmad, S. F., Anjum, A., Syed, M. H., Malik, S. U. R., & Rehman, S. (2025). Ensuring Zero Trust in GDPR-Compliant Deep Federated Learning Architecture. Computers, 14(8), 317. https://doi.org/10.3390/computers14080317

Al Shahrani, A. M., Rizwan, A., Sánchez-Chero, M., Cornejo, L. L. C., & Shabaz, M. (2024). Blockchain-enabled federated learning for prevention of power terminals threats in IoT environment using edge zero-trust model. The Journal of Supercomputing, 80(6), 7849-7875. https://doi.org/10.1007/s11227-023-05763-6

Alnaim, A. K., & Alwakeel, A. M. (2025). Zero-trust mechanisms for securing distributed edge and fog computing in 6G networks. Mathematics, 13(8), 1239. https://doi.org/10.3390/math13081239

Aloqaily, M., Zhang, Q., Andreoni, M., Nogueira, M., Du, X., & Chen, A. (2025). Guest Editorial: Special Issue on Zero Trust for Next-Generation Networking. IEEE Journal on Selected Areas in Communications, 43(6), 1901-1907. https://doi.org/10.1109/JSAC.2025.3558644

Al-Sharafi, A. M., Alrayes, F. S., Alruwais, N., Maray, M., Alshuhail, A., Darem, A. A., ... & Al-Hagery, M. A. (2025). Ensuring Zero Trust Security in Consumer Internet of Things Using Federated Learningbased Attack Detection Model. IEEE Access. https://doi.org/10.1109/ACCESS.2025.3551212

Alzahrani, A. I. (2025, December). Quantum-Enhanced Federated Learning With Zerotrust Blockchain for Secure 6G IoT Anomaly Detection. In 2025 IEEE 17th International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 1015-1021). IEEE. https://doi.org/10.1109/CICN67655.2025.11368171

Asad, M., & Otoum, S. (2024). Integrative federated learning and zero-trust approach for secure wireless communications. IEEE wireless communications, 31(2), 14-20. https://doi.org/10.1109/MWC.001.2300355

Chandu, G., Karthik, T., & Parag, B. (2025). Federated learning for distributed IoT security: A privacy-preserving approach to intrusion detection. IEEE Access.

El-Hajj, M. (2025). Secure and trustworthy open radio access network (O-RAN) optimization: A zero-trust and federated learning framework for 6G networks. Future Internet, 17(6), 233. https://doi.org/10.3390/fi17060233

Hossain, A. A., Kumar, P. M., Amsaad, F., & Ahner, D. (2025, February). Secure and Privacy-Preserving AI: A Zero Trust Architecture for Federated Machine Learning. In 2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC) (pp. 1-7). IEEE. https://doi.org/10.1109/SATC65530.2025.11137026

Hussain, A., Akbar, W., Hussain, T., Bashir, A. K., Al Dabel, M. M., Ali, F., & Yang, B. (2024). Ensuring zero trust IoT data privacy: Differential privacy in blockchain using federated learning. IEEE Transactions on Consumer Electronics, 71(1), 1167-1179. https://doi.org/10.1109/TCE.2024.3444824

Javeed, D., Saeed, M. S., Adil, M., Kumar, P., & Jolfaei, A. (2024). A federated learning-based zero trust intrusion detection system for Internet of Things. Ad Hoc Networks, 162, 103540. https://doi.org/10.1016/j.adhoc.2024.103540

Kokku, V. K. (2025). Toward Secure IoT Infrastructure: Integrating Zero Trust, Federated Learning, and Dynamic Trust Management Models. Federated Learning, and Dynamic Trust Management Models (April 25, 2025). https://doi.org/10.2139/ssrn.5230237

Laghari, A. A., Khan, A. A., Ksibi, A., Hajjej, F., Kryvinska, N., Almadhor, A., ... & Alsubai, S. (2025). A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture. Scientific Reports, 15(1), 26843. https://doi.org/10.1038/s41598-025-11738-9

Li, K., Li, C., Yuan, X., Li, S., Zou, S., Ahmed, S. S., ... & Akan, Ö. B. (2025). Zero-trust foundation models: A new paradigm for secure and collaborative artificial intelligence for internet of things. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2025.3603957

Mahamad, H. (2024). Guardians of the Data Galaxy: A Federated AI and Cloud Synergy for Zero-trust Cybersecurity Models. International Journal of Education Humanities and Social Science, 7(06), 796-810. https://doi.org/10.54922/IJEHSS.2024.0746

Matam, P., Mittal, A., Pappu, K., & Jadav, V. (2026, February). Privacy-Driven Cloud AI: Federated Learning and Zero-Trust for Secure Multi-Domain Collaboration. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-8). IEEE. https://doi.org/10.1109/ICAIC67076.2026.11395751

Mazid, A., Kirmani, S., Manaullah, & Yadav, M. (2025). FL-IDPP: A Federated Learning Based Intrusion Detection Approach With Privacy Preservation. Transactions on Emerging Telecommunications Technologies, 36(1), e70039. https://doi.org/10.1002/ett.70039

Mrabet, M. (2025). TrustFed-CTI: A Trust-Aware Federated Learning Framework for Privacy-Preserving Cyber Threat Intelligence Sharing Across Distributed Organizations. Future Internet, 17(11), 512. https://doi.org/10.3390/fi17110512

Potluri, S. (2024). A Zero Trust-Based Identity and Access Management Framework for Cross-Cloud Federated Networks. International Journal of Emerging Research in Engineering and Technology, 5(2), 28-40. https://doi.org/10.63282/3050-922X.IJERET-V5I2P104

Puviarasu, A., & Sudha, V. K. (2026). Enhanced IoT security: privacy-preserving federated learning model for accurate, real-time intrusion detection across devices. Ain Shams Engineering Journal, 17(1), 103866. https://doi.org/10.1016/j.asej.2025.103866

Shah, K., Kumari, A., Solanki, B., Al-Humairi, S. N. S., & Al-Hakimi, A. M. H. (2025, July). ZTSec-FedSDN: A Privacy-Preserving Federated Framework for SDN Attack Detection Using Zero-Trust Blockchain and 6G Terahertz Networks. In 2025 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 1-6). IEEE. https://doi.org/10.1109/CITS65975.2025.11099386

Sharma, A., Rani, S., & Boulila, W. (2025). Blockchain-based zero trust networks with federated transfer learning for IoT security in industry 5.0. PLoS One, 20(6), e0323241. https://doi.org/10.1371/journal.pone.0323241

Ullah, F., Srivastava, G., Mostarda, L., & Raza, U. (2025). ZTID-IoV: Zero-Trust Intrusion Detection in IoV Using Neurosymbolic AI Approach with Federated Meta-Learning. IEEE Transactions on Consumer Electronics. https://doi.org/10.1109/TCE.2025.3625081

Varadala, S., & Xu, H. (2025). A Blockchain-Enabled Decentralized Zero-Trust Architecture for Anomaly Detection in Satellite Networks via Post-Quantum Cryptography and Federated Learning. Future Internet, 17(11), 516. https://doi.org/10.3390/fi17110516

Wardana, A. A., Kołaczek, G., & Sukarno, P. (2024). Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for internet of things. Applied Sciences, 14(10), 4109. https://doi.org/10.3390/app14104109

Zhou, X., Liang, W., Kevin, I., Wang, K., Yada, K., Yang, L. T., ... & Jin, Q. (2025). Decentralized federated graph learning with lightweight zero trust architecture for next-generation networking security. IEEE Journal on Selected Areas in Communications. https://doi.org/10.1109/JSAC.2025.3560012