I. J. Engineering and Manufacturing, 2026, 4, 324-343
Published Online on August 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijem.2026.04.22

FL-EZTF: A Privacy-Preserving Federated Deep Learning Framework with Enhanced Zero Trust for Healthcare IoT Security

Urvashi
Department of Computer Science and Engineering, Jamia Hamdard University, Hamdard Nagar, New Delhi, Delhi 110062, India
E-mail: urvi.bhanu@gmail.com
ORCID iD: https://orcid.org/0009-0005-2859-604X

Parul Agarwal*
Department of Computer Science and Engineering, School of Engineering Sciences and Technology (SEST), Jamia Hamdard University, Hamdard Nagar, New Delhi, Delhi 110062, India
E-mail: pagarwal@jamiahamdard.ac.in
ORCID iD: https://orcid.org/0000-0002-7297-335X
*Corresponding Author

Kamlesh Kumar Raghuvanshi
Department of Computer Science, University of Delhi, New Delhi, Delhi, India
E-mail: mailto.kamlesh@ramanujan.du.ac.in
ORCID iD: https://orcid.org/0000-0001-9887-3392

Jawed Ahmed
Department of Computer Science and Engineering, Jamia Hamdard University, Hamdard Nagar, New Delhi, Delhi 110062, India
E-mail: jahmed2047@jamiahamdard.ac.in
ORCID iD: https://orcid.org/0000-0002-8852-8234

Received: April 12, 2026; Revised: April 27, 2026; Accepted: June 17, 2026; Published: August 8, 2026

Abstract: Smart healthcare IoT systems are vulnerable to cyber threats as they deal with sensitive patient information. Problems such as privacy, scalability, and delayed response to threats in distributed healthcare environments challenge centralized security approaches. To mitigate the security challenges of cloud-edge healthcare IoT systems, this paper presents FL-EZTF, a privacy-preserving, Federated Deep Learning and Enhanced Zero Trust Framework. The framework combines federated learning, Enhanced Zero Trust Architecture (E-ZTA), and Secure Access Service Edge (SASE). In this framework, lightweight deep learning models are developed locally at hospitals and various edge nodes without the need to transfer sensitive medical data. In place of raw data, model updates are sent conveniently through a trust-aware federated learning process. Simultaneously, E-ZTA performs continuous authentication, micro-segmentation, and access control to rapidly contain threats. The framework is assessed using CIC-IoT-2023, IoT-23, and WESAD datasets. The experimental results show improved accuracy in detection, lower rates of false positives, a significant reduction in the latency of decisions, and enhanced containment as compared to centralized and traditional federated learning.

Index Terms: Federated Learning, Zero Trust, SASE, Healthcare IoT, Intrusion Detection, Edge Computing, Privacy preserving

1. Introduction

The Internet of Things (IoT) enables advanced communication that can be automated, interconnected, and simplified using sensors and technologies [1]. These systems can collect and communicate data in real-time, work continuously, and interact with other IoT infrastructures by collecting data and using communication protocols to transfer data [2]. There is

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

a growing trend to utilize IoT infrastructures in smart industries [3], smart energy systems [4], intelligent surveillance [5], as well as transportation, farming, and health ecosystems [6]. In healthcare, IoT systems range from wearable sensors
This work is open access and licensed under the Creative Commons CC BY 4.0 License. Volume 12 (2022), Issue 6 to monitoring systems to infusion systems and even telemedicine. These systems rapidly change and exchange protected health information to facilitate remote diagnosis and telehealth services. The growth of the IoT systems has expanded the range of possible attacks on an IoT system and created numerous possible security exploits, including, but not limited to, spoofing, distribution of malware, phishing, routing manipulation, data leakage, and distributed denial-of-service attacks [7].

The unique characteristics of IoT ecosystems make centralized security mechanisms ineffective. IoT environments, like healthcare, are the most impacted by this challenge. Ransomware, botnet attacks, and Man-in-the-Middle (MitM) attacks are among the various vulnerabilities targeting IoT systems and their infrastructure [8]. To mitigate security challenges, the adoption of the Zero Trust model is becoming popular. The Zero Trust model shifts from perimeter-based security. More specifically, Zero Trust entails that no user, device, or entity should be trusted by default, even after authentication. Contrarily, security mechanisms should be implemented to consistently evaluate requests. Zero Trust increases security by removing concerns regarding threats from both outside and within [8].

Similarly, to address these challenges, IoT networks rely on AI-based intrusion detection systems. The main areas of focus within AI-based intrusion detection systems for IoT networks include Federated Learning (FL). FL has received a lot of consideration for IoT networks because of the data privacy concerns surrounding the systems [9, 10]. Within an FL framework, local models are trained with private datasets at each node, and only model updates are transmitted to a centralized server. The server updates the global model, and the distributed model is sent back to the nodes to continue local learning [11]. Because of the distributed nature of FL, a global model is continuously updated based on the networked data [12].

The use of federated learning (FL) in intrusion detection systems has two primary benefits. The first is that devices only send information for model updates, and the raw data is not sent, which mitigates privacy and data exposure risks in distributed systems [13]. The second benefit is that the lightweight model updates significantly decrease the volume of communications when compared to centralized learning [14]. Moreover, learning in a distributed manner increases the system's flexibility, responsiveness, and robustness in the always-changing nature of IoT ecosystems [15]. From a security standpoint, federated learning complements the Zero Trust model since it is assumed that no participating node is fully trusted and that all model updates should be validated and then aggregated.

It is noted that many of the security IoT solutions in healthcare have some of the same limitations. Many of the federated learning frameworks assume some form of intrusion detection with privacy protection but focus less on trust evaluation, access control, and threat containment. In the same way, many Zero Trust architectures focus on authentication and policy control but do not incorporate threat detection. Scalability, the efficiency of communications, and the heterogeneity of IoT frameworks are other challenges that exist. Also, it is noted that there is a lack of integration of federated intrusion detection systems and security enforcement constructs such as Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE) in the context of the healthcare domain IoT systems.

In response to these issues, we propose FL-EZTF, a Federated Deep Learning and Enhanced Zero Trust Framework combining privacy and security for cloud-edge healthcare IoT systems. This framework combines federated deep learning, Enhanced Zero Trust Architecture (E-ZTA), and SASE-based policy enforcement within a single security architecture. At the healthcare edge, lightweight deep learning models are built, and trust-aware aggregation, continuous authentication, micro-segmentation, and adaptive containment are employed to enhance security. The framework combines intelligent intrusion detection, trust enforcement, and edge-based policy to offer flexible and privacy-preserving protection in real time for advanced healthcare IoT systems.

1.1. Motivation and Challenges

Healthcare IoT system development technologies quickly compromise system security and usability. Conventional security measures cannot ensure privacy, scalability, or low latency for resource-constrained healthcare devices. One of the key issues is the privacy of the centralized storage of sensitive patient data. While federated learning minimizes data sharing, existing federated learning systems are still susceptible to adversarial model updates and poisoning. Moreover, the diverse and dynamic nature of IoT systems creates challenges for effective centralized monitoring and increased detection latency. Current Zero Trust implementation focuses mainly on authentication and access control, while most federated learning-based IDSs do not offer a continuous trust and adaptive response. Integration of Federated Intelligence, Zero Trust, and SASE Managed Healthcare Policy remains low. Based on these issues, this research proposes a comprehensive and integrated healthcare IoT security framework, combining privacy-preserving federated learning, continuous trust verification, and policy protection at the cloud-edge for resilient security.

1.2. Contributions

- Developed FL-EZTF based on FL, E-ZTA, and SASE.
- Proposed trust-aware federated aggregation for secure healthcare IoT.
- Developed adaptive containment and micro-segmentation on edge nodes.

- Evaluated framework on CIC-IoT-2023, IoT-23, and WESAD datasets.
- Achieved better accuracy with less latency and greater robustness.

1.3. Contributions

- We propose FL-EZTF, a federated anomaly-detection + E-ZTA + SASE architecture for healthcare IoT.
- We design lightweight local DL models (e.g., CNN-LSTM or LSTM-AE) suitable for edge nodes and federated aggregation.
- We simulate a multi-hospital federated setup and quantify privacy, accuracy, latency, and containment time compared to baselines.

2. Related Work

2.1. FL-Based Intrusion Detection Systems for IoT

Due to privacy concerns, securing IoT environments using Federated Learning (FL) based intrusion detection systems, has gained a lot of interest. The authors of [16] developed an FL based intrusion detection framework with the capability of monitoring IoT communications over the MQTT protocol. The framework was tested on the MQTT-IoT-IDS2020 dataset that contains almost 2 million instance of attacks and obtained over 80% detection accuracy. Although, additional communication latency was introduced by the framework, there was no adaptive trust validation mechanism to validate compromised devices.

To study the adversarial effects on FL systems, the authors of [17] studied the effects of model poisoning, by using Generative Adversarial Networks (GANs). Among the many effects of including malicious clients, the authors observed that FL based intrusion detection systems suffer from biased predictions, increased false positives, and decreased detection trust. To construct a better balance between trust and security in a collaborative context, the authors proposed a trust-aware relationship based social intrusion detection system (SIDS). Although the framework improved the trust in social systems, the framework increased the trust in social systems, but worsened the computational burden, and failed to perform real time containment.

The study in [18] proposed a federated CNN-based intrusion detection framework, using the CSE-CICIDS2018 dataset, to detect multiple types of attacks, including DoS-Slowloris, DoS-HOIC, and brute-force attacks. Although the framework indicated good performance, it was mainly focused on attack classification and did not incorporate attack response adaptively or trust continuously enforced. In [19], a semi-supervised FL-based framework for anomaly detection in large-scale IoT environments using the N-BaIoT dataset was introduced. Communication overhead in the federated training rounds was a limitation of the framework, despite successfully detecting novel attacks. The study in [20], which used the IoT-23 dataset, presented a decentralized FL-based CNN framework. The model achieved high detection accuracy, but the high number of false positives limited its usability in real environments.

The study in [21] proposed a GRU-based federated threat classification model, using the ToN-IoT dataset to classify query flooding, SYN flooding, and distributed denial-of-service attacks. Although the framework was able to classify attacks effectively, the training times were long, and a scalability analysis for large healthcare IoT deployments was not presented.

2.2. Privacy-Preserving FL Models

Multiple attempts have been made to enhance distributed learning and privacy preservation in IoT intrusion detection systems. In [22], the authors introduced FEDGAN-IDS, a combination of federated learning with added privacy preserving techniques. The proposed framework detected 24 types of attacks on the NSL-KDD, KDD-CUP99, and UNSW-NB15 datasets. However, the complexity added to the model increased communication delays and decreased the efficiency of deployment in the real world.

In [23], the authors also proposed an FL-based intrusion detection framework for edge-assisted IoT systems. The framework implemented local learning in edge nodes in order to decrease the exposure of centralized data, and the framework was able to identify denial-of-service and unauthorized probing attacks. The detection performance of the framework was satisfactory; however, the design had a strong focus on the identification of attacks, and there was no design of adaptive trust management and automated containment

In the contribution in [24], the authors proposed a multi-view federated intrusion detection framework which integrated Random Forest classification and Grey Wolf Optimization (GWO) based feature extraction. The approach enabled the analysis of network traffic using uniflow, biflow and packet-level traffic, thus improving the reliability of detection. However, the framework had a high false-positive rate and did not offer defense mechanisms for malicious federated participants.

The authors of [25] proposed a framework for anomaly detection in the Modbus traffic data, centered on GRU models, based on FL. Despite strong detection accuracy and recall, the framework has limited applicability in latency-sensitive IoT environments due to time-intensive training and testing. Similarly, in [26], an FL-based unsupervised intrusion detection framework demonstrated effective detection of botnet, denial-of-service, and port-scanning attacks

based on the CICIDS2017 dataset. However, the framework lacks the incorporation of active resilience mechanisms to counter adversarial conduct in the large-scale distributed IoT environments as well as the Byzantine attacks.

2.3. Robustness of FL and Model Poisoning Attacks

The application of federated learning (FL) in IoT intrusion detection is still new and comes with challenges. One of the primary challenges is the effect of malicious participants in federated learning, especially in an IoT environment. In the work referenced as [17], it was shown that FL-based intrusion detection systems are subject to poisoning-based attacks when malicious participants are allowed to perform updates on the to-be Federated global model. Some of the problems highlighted were biased predictions, high false positive rates, and instability in the collaborative learning process. The trust-based collaborative IoT framework (SIDS) proposed by the authors addressed some of the problems but still does not have passive client validation and real-time adversarial mitigation. In the same way, the multi-view FL framework proposed in [24] introduced improvements in threat and attack detection via RFs and GWO. As is, the primary focus of the framework was on the improvement of detection capabilities and the issues of Byzantine-resilient aggregation, malicious clients, and adaptive trust ratings were not addressed. As such, most of the offered research focuses on privacy-preserving algorithms and the classification of attacks with the least focus on the adversarial attacks framework and poisoning in the distributed healthcare IoT system.

2.4. Gap Analysis

Table 1 summarizes the notable drawbacks of current FL-based intrusion detection systems and juxtaposes them with the FL-EZTF framework. While earlier works have made significant strides in enhancing privacy by not directly exchanging raw data, the majority of these frameworks are still lacking in shielding against malicious clients and attacks, including poisoning attacks and Byzantine behavior. Moreover, most approaches exhibit a communication burden and higher rates of false positives along with low scalability in the context of heterogeneous IoT deployments. It is also apparent that the current solutions incorporating Zero Trust and FL-based systems, do not offer adaptive trust scoring, realtime response and containment, or integrated security enforcement on the cloud and the edge. The FL-EZTF framework, on the other hand, employs trust-aware federated learning, Enhanced Zero Trust Architecture (E-ZTA), and SASE-based orchestration, and presents an innovative solution that is scalable, privacy-preserving, and real-time for secure healthcare IoT ecosystems.

3. Proposed Framework (FL-EZTF)

The FL-EZTF framework utilizes a three-layer cloud-edge IoT architecture for healthcare: device, edge, and cloudedge coordination layers. The architecture supports privacy-preserving intrusion detection, continuous trust verification, and adaptive security enforcement in distributed healthcare settings.

At the device layer, the healthcare IoT ecosystem includes hospitals and clinics, as well as devices such as wearable sensors, patient monitoring systems, infusion pumps, and telehealth and telemedicine devices. These devices collect both physiological and network data. Lightweight deep learning models, like LSTM Autoencoders and CNN-LSTM networks, operate at the device layer to detect anomalous/suspicious behaviors. To enhance patient privacy and reduce exposure of sensitive healthcare data, the aforementioned models (and data collected by these devices) remain in the local healthcare facility. The only external data shared in the federated learning framework comprises locally updated model parameters and encrypted updates.

The edge layer is implemented at the hospital gateways, acting as a federated learning and security enforcement layer. Within this layer, local model updates from healthcare devices are pre-processed and sent to the global aggregation server. The edge layer incorporates the Enhanced Zero Trust Architecture (E-ZTA) and continuous validation of device identity, user behavior, and context requests. Continuous authentication, trust scoring, and reauthentication are employed. Micro-segmentation and quarantine of devices, along with policy-based threat containment mechanisms are implemented to provide a rapid response at the edge. The cloud–edge coordination layer integrates the centralized federated learning server and SASE-enabled security orchestration services. The global federated server is responsible for the trust-aware aggregation of model updates and the dissemination of global model updates to the edge nodes. The SASE component integrates the SWG, CASB, FWaaS, and ZTNA, to provide consolidated policy-driven and automated cross-domain security and traffic management. The framework leverages an iterative cycle of federated learning, in which healthcare devices train the model locally, edge nodes validate and aggregate the model updates, and the cloud server processes the global model for redistribution. The integration of federated learning, E-ZTA, and SASE-based orchestration enables the FL-EZTF framework to deliver scalable, privacy-preserving, and real-time security for emerging healthcare IoT ecosystems.

Table 1. Gap Analysis between Existing FL-Based IoT IDS Approaches and the Proposed FL-EZTF Framework

Research Aspect	Limitations of Existing Works (Refs. [18]–[28])	FL-EZTF Improvements
Privacy Preservation	Existing studies focus mainly on preventing raw data sharing but provide limited protection against compromised clients and malicious model updates.	Introduces privacy-preserving federated learning with trust-aware aggregation and continuous validation at edge nodes.
Model Poisoningand Byzantine Defense	Most existing frameworks do not address Byzantine-resilient aggregation or malicious client filtering during federated learning.	Incorporates trust-aware validation and adaptive filtering of suspicious model updates before global aggregation.
Detection Accuracy	Several approaches achieve high detection accuracy but suffer from increased false positives and poor generalization across heterogeneous IoT environments.	Provides balanced intrusion detection with improved accuracy and reduced false-positive rates across diverse healthcare IoT scenarios.
Communication Overhead	Many FL-based systems experience excessive communication latency and computational overhead during federated training rounds.	Employs lightweight deep learning models and optimized federated communication for edge-assisted healthcare environments.
Trust Management	Existing works mainly focus on attack detection while lacking continuous trust evaluation and contextual risk assessment.	Integrates Enhanced Zero Trust Architecture (E-ZTA) for continuous authentication, adaptive trust scoring, and behavioral verification.
Real-Time Threat Containment	Detection outcomes are rarely connected with automated response and containment mechanisms.	Enables real-time threat containment through micro-segmentation, device quarantine, and adaptive access control.
Edge–Cloud Coordination	Most studies provide limited coordination between cloud security and edgelevel enforcement.	Combines federated learning, edge intelligence, and SASE-based policy orchestration for unified cloud–edge security management.
Scalability	Existing systems show performance degradation with increasing federated clients and large-scale IoT deployments.	Designed for scalable healthcare IoT environments using distributed edge processing and hierarchical federated learning.
Healthcare IoT Applica-bility	Most existing approaches target generic IoT environments without considering healthcare-specific privacy and latency requirements.	Specifically designed for healthcare IoT systems with privacy preservation, low-latency response, and secure medical data handling.

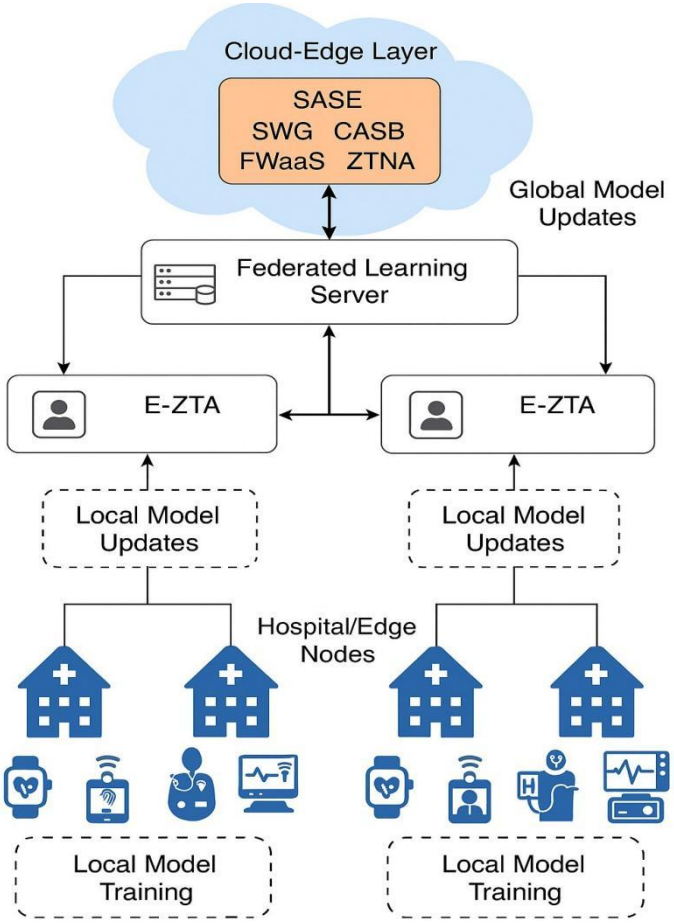


Fig. 1. High-level architecture of FL-EZTF: federated learning across hospital/edge nodes, E-ZTA modules at edge, and SASE policy enforcement at cloud-edge layer.

3.1. Federated Deep Learning Module

The Federated Deep Learning module in the proposed FL-EZTF framework enables intrusion detection that preserves the privacy of medical and network data against unauthorized access. Participating healthcare organizations, hospital gateways, and edge nodes can train deep learning models on IoT traffic data and device data without sending this data beyond the edge node. This enables organizations to cooperate and share information regarding threats and protect valuable data at the same time. The FL-EZTF framework is designed to address the multi-faceted and non-stationary nature of IoT data. It uses deep learning frameworks for LSTM Autoencoders, hybrid CNN-LSTM models, and 1D-CNN models. LSTM Autoencoders, part of the deep learning framework, are used for anomaly detection and reconstruction to identify abnormal behavior in healthcare IoT systems. The hybrid CNN-LSTM model combines spatial and temporal domains to identify Denial-of-Service (DoS) attacks, as well as intrusion activities that occur in multiple steps. The 1DCNN model is an intrusion detection model for resource-constrained healthcare devices that allows for low latency and low-power consumption. IoT traffic data is preprocessed to normalize, reduce the number of dimensions using PCA, and segment time before the locals models are trained. Each federated client is required to train the model on a given number of epochs using the Adam optimizer. The clients share only the trained model parameters and gradients to the aggregating server which performs the model updates. To enhance resilience against untrustworthy or adversarial participants, the framework introduces an aggregation mechanism under the concept of trust federated aggregation, which is a variant of the Federated Averaging (FedAvg). For this model, a client's local model parameter is denoted as w_k^t where k is the index of the client and t is the global communication round. T_k is the trust score of the k-th client derived from behavioral confirmation and anomaly assessment. The global aggregation is described as follows:

$$wt+1=\mathrm{X}\alpha_k \overset{K_w}{\underset{k=1}{}} {}_{kt} \tag{1}$$

where the aggregation weight α_k is computed as:

$$\alpha_k=\frac{T_k\times D_k}{\sum_{i=1}^{K} T_i\times D_i} \tag{2}$$

Here, D_k refers to the size of the local dataset belonging to client k. Trust-based aggregation methods effectively decrease the impact of problematic or malicious clients, increasing the level of consistency and trust in the global federated model. The federated learning algorithm is executed in iterations, which are divided into several global communication rounds. For every round, local models are built and validated at healthcare edge nodes, and the improved global model is sent back to the institutional users. To minimize the amount of data sent and the delay in healthcare networks that are federated, methods such as gradient compression, sparse updates, and weight quantization are used. The global model, once spread to every institutional user, functions as the basis for real-time anomaly detection and the adaptation of countermeasures to continuously changing cyber threats, all without compromising the integrity of the data.

3.2. Enhanced Zero Trust Architecture (E-ZTA) at the Edge

The enhanced zero trust architecture (E-ZTA) module works at the healthcare edge layer to implement continuous trust evaluation, adaptive access control, and adaptive threat containment at the healthcare edge layer for distributed IoT environments. As opposed to conventional zero trust systems, which heavily depend on static authentication policies, behavioral analytics, contextual risk assessment, and adaptive policy enforcement are emphasized to increase the security resilience of the healthcare IoT ecosystem.

1. Continuous Behavioral Verification

The framework under consideration for implementation focuses on continuous verification rather than on a reliance of one-time authentication methods. This involves observing user behavior, device behavior and network traffic patterns. At edge nodes, lightweight anomaly detection models are used to identify suspicious behavior by analyzing access and traffic patterns and deviations. An example may include a spectrum of communication behavior, and access and device posture. Communication patterns may also include patient monitoring and affinity grouping over a spectrum of infusion devices. Continuous verification extends beyond anomalous behavior, allowing for early detection of threats, while maintaining barriers of unauthorized access within a healthcare environment.

2. Micro-Segmentation and Adaptive Isolation

To mitigate cyberattack spread, the structure of healthcare IoT environments is split into different logical microsegments. IoT wearable devices, patient and imaging monitoring systems, telemedicine devices, and administrative systems fall into different micro-segments. The E-ZTA framework proposed here isolates faulty or high-risk entities using adaptive segmentation policies. By restricting the lateral propagation of malware, insider threats, and other forms of

attacks, the framework addresses the critical concern posed to integrated systems within the healthcare ecosystem. The framework fulfills this concern while reducing the impact of a cyber incident and retaining the continuity of healthcare services.

Algorithm 1 Trust-Aware Federated Training and Aggregation in FL-EZTF

Require: Global communication rounds T, local epochs E, participating clients K, trust threshold τ, local datasets D_k

1: Initialize global model parameters w^0
2: for t =0 to T −1 do
3: Server selects a subset S_t of available healthcare clients
4: for all k $\in S_t$ in parallel do
5: Client k receives global model w^t
6: Preprocess local healthcare IoT data
7: Train local model for E epochs using dataset D_k 8: Compute local model update:

$$\Delta\omega_k^t=\omega_k^t-\omega^t$$

9: Compute anomaly score A_k from local behavioral analysis
10: Compute trust score:

$$T_k=\frac{1}{1+A_k}$$

11: if $T_k < \tau$ then
12: Reject suspicious client update
13: else
14: Compress and encrypt $\Delta^{w}{}_k^t$
15: Transmit validated update to edge aggregator
16: end if 17: end for
18: Edge aggregators validate received updates
19: Compute trust-aware aggregation weights:

$$\alpha_k=\frac{T_k\times D_k}{\sum_{i=1}^{K} T_i\times D_i}$$

20:Update global federated model:

$$=X\alpha_k^{\,w_{kt}} \quad \begin{matrix} K\ wt+1 \\ k=1 \end{matrix}$$

21:Perform secure aggregation and integrity validation
22:Redistribute updated global model to participating clients
23:Update E-ZTA and SASE policies using global threat analytics
24: end for
25: return Final global model w^T

Algorithm 2 E-ZTA Risk Evaluation and Adaptive Threat Containment

Require: Risk threshold T_{risk}, escalation threshold T_{esc}, monitoring window W

1: while system is active do
2: Receive device activity and network events
3: Generate anomaly score s using local intrusion detection model
4: Compute behavioral deviation score b 5: Compute device posture score p 6: Calculate composite risk score:

$$R = \alpha s+\beta b+\gamma p$$

7: if $R < T_{risk}$ then

```
8:      Allow normal activity and continue monitoring
9:     else if T_risk ≤ R < T_esc then
10:    Trigger adaptive authentication
11:    Restrict device privileges
12:    Enable micro-segmentation
13:    Log suspicious activity
14:     if multiple violations detected within window W then
15:         Notify administrator and security operations center
16:              end if
17:               else
18:    Initiate threat containment
19:    Quarantine compromised device
20:    Revoke active sessions and access tokens
21:    Collect forensic logs and attack traces
22:    Notify SASE control plane for global policy enforcement
23:    Apply cross-site blocking and isolation policies
24: end if
25:Update local trust profile using feedback analytics
26:if false positive confirmed then
27:    Adjust thresholds and retrain local detection model
28:  end if 29: end while
```

3. Risk Scoring and Decision Enforcement

The E-ZTA module calculates a composite risk score combining results from anomaly detection, device posture verification, and behavioral deviation assessment. The risk assessment procedure is defined as follows:

$$R = \alpha s + \beta b + \gamma p \tag{3}$$

where s is the indicator of the anomaly score output by the intrusion detection model; b stands for behavioral deviation; and p means the posture score for the device. The weighting coefficients α, β, and γ determine the level of impact of each security factor. Depending on the ascertained risk score, the framework implements adaptive decision enforcement. By default, low-risk entities are granted access; mid-risk entities are subjected to step-up authentication or controlled access; and high-risk entities are subjected to automatic quarantining or isolation. This process of adaptive decision making not only enables the swift containment of threats, but also ensures that critical system functionality is not impacted to a large extent.

3.3. SASE Integration

For the integration of Secure Access Service Edge (SASE) with the proposed FL-EZTF framework, SASE interprets the results of anomaly detection and applies adaptive security mechanisms across the distributed healthcare IoT environment. The federated learning module is capable of performing Intrusion Detection and Risk Assessment at the edge, while the SASE layer implements cloud-edge unified policy and orchestrated response to threats.

Within the proposed framework, each component of SASE implements a specific security function based on the risk score and anomaly alerts generated by FL-EZTF. The SASE solution, Secure Web Gateway, prohibits access to malicious

Table 2. Roles of SASE Components and Their Integration with FL-EZTF

SASE Compo-nent		Primary Function	Integration with FL-EZTF
SWG		Filters malicious web traffic and suspicious sessions.	Blocks anomalous outbound traffic detected by FL-EZTF.
CASB		Controls access to healthcare cloud applications.	Restricts abnormal access to EHR and telemedicine services.
FWaaS		Performs distributed firewall policy enforcement.	Updates firewall rules based on detected attack patterns.
ZTNA		Provides identityaware and adaptive access control.	Adjusts authentication and quarantine policies using risk scores.

URLs and blocks suspicious outbound traffic. The SASE solution, Cloud Access Security Broker, within the SASE framework, blocks anomalous access to the healthcare cloud services, including access to the Electronic Health Record (EHR) and the telemedicine platform. In a similar fashion, Firewall as a Service (FWaaS) employs an adaptive and context

aware access control based on risk score, which controls the extent to which an attack can spread across the healthcare network. Zero Trust Network Access (ZTNA) employs adaptive access control and context based control, based on risk score, which is generated by the E-ZTA module.

To support dynamic policy enforcement, the framework adjusts security policies based on the evolving threat situation using:

$$P_t = P_{t-1} + \lambda R_t \quad (4)$$

where P_t is the revised security policy, R_t is the risk score from FL-EZTF, and λ is the factor for policy adaptation.

Integration of federated learning, E-ZTA, and SASE provides privacy-preserving intrusion detection and adaptive trust enforcement and quick threat containment for large scale health care IoT systems.

3.4. Workflow Summary

The sequential workflow of the FL-EZTF framework is shown in Figure 2. The starting point involves the collection of data from IoT healthcare devices, along with local data preprocessing steps of normalization and feature extraction. Each device or hospital node implements local training and inference using lightweight deep learning models and performs real-time anomaly detection. Local nodes send only federated model updates to the global server rather than the raw data, thus maintaining privacy. At the edge, the Enhanced Zero Trust Architecture (E-ZTA) performs continuous and real-time risk score assessments through device posture and user behavior monitoring. Depending on the results, containment enforcement policies are applied: low-risk situations allow free access, medium-risk situations initiate step-up authentication, and privilege restrictions are applied; high-risk situations cause total containment. At the final step, the SASE layer makes these security controls cloud-level decisions, applying the same controls and policies to all distributed healthcare environments.

4. Experimental Setup

This section outlines the experimental methodology used to validate the proposed FL-EZTF framework under realistic deployment conditions. The evaluation focuses on measuring intrusion detection effectiveness, privacy preservation, trust enforcement, and policy response behavior within distributed healthcare IoT environments. Details regarding the datasets, preprocessing pipeline, federated simulation settings, model architectures and hyperparameters, baseline configurations, and evaluation metrics are presented. Collectively, these components define a comprehensive and reproducible experimental framework that enables fair and meaningful comparison with existing approaches.

4.1. Datasets

Table 4 contains a summary of the datasets developed to evaluate the proposed FL-EZTF framework. CIC-IoT2023 is used as the primary dataset for federated intrusion detection because it contains a rich variety of IoT traffic profiles, attack categories, and diverse behavioral patterns of IoT devices. To evaluate the framework's robustness and generalization capability, some unseen attack traffic patterns are considered using IoT-23, which consists of multiple botnets and malicious IoT framework traffic. Unlike the other datasets, WESAD is not used for intrusion detection. It is used as a dataset to model the normal behavioral and physiological patterns of healthcare devices. The use of this collection of datasets achieves an adequate and balanced assessment of intrusion detection, behavioral verification, and contextual trust enforcement in a distributed healthcare IoT system.

Table 3. Workflow Summary of FL-EZTF Framework

Step	Process Description
1	Data Collection: IoT devices and medical sensors generate traffic and telemetry data at hospital or home environments.
2	Local Preprocessing: Features are normalized, reduced (e.g., PCA), and encoded at device/edge nodes for consistency.
3	Local Training & Inference: Lightweight DL models (LSTM-AE, CNN-LSTM, 1DCNN) perform anomaly detection and generate local alerts.
4	Federated Update Sharing: Model updates (not raw data) are transmitted securely to the edge/global aggregator for FedAvg.
5	Global Aggregation: Central server aggregates updates, validates the model, and redistributes improved weights to all nodes.
6	E-ZTA Verification: Local risk scoring combines anomaly score, user behavior, and device posture to evaluate trust level.
7	Decision Enforcement: Low-risk → normal access; Medium-risk → step-up authentication/privilege reduction; High-risk → containment/quarantine.
8	SASE Policy Enforcement: SWG, CASB, FWaaS, and ZTNA modules enforce global access rules and block suspicious sessions.
9	Continuous Feedback: Logs, alerts, and outcomes are fed back into federated models for retraining and adaptive policy refinement.

Table 4. Datasets Used in FL-EZTF Framework Experiments

Dataset	Description	Purpose in FL-EZTF	Stage of Use
CIC-IoT-2023	Large-scale IoT intrusion detection dataset containing diverse IoT traffic and 33 attack categories including DoS, DDoS, reconnaissance, and brute-force attacks.	Used as the primary benchmark for federated intrusion detection and anomaly classification in healthcare IoT environments.	Training and validation of federated deep learning models.
IoT-23	Realistic IoT malware and benign traffic dataset containing botnet and device communication scenarios.	Used to evaluate model generalization and robustness against unseen IoT attack behaviors.	External testing and robustness evaluation.
WESAD	Physiological and wearable sensor dataset containing ECG, respiration, EDA, and motion signals.	Used only for modeling normal behavioral patterns of healthcare wearable devices within the E-ZTA module. It is not used for intrusion classification.	Behavioral profiling and contextual risk verification at the edge layer.

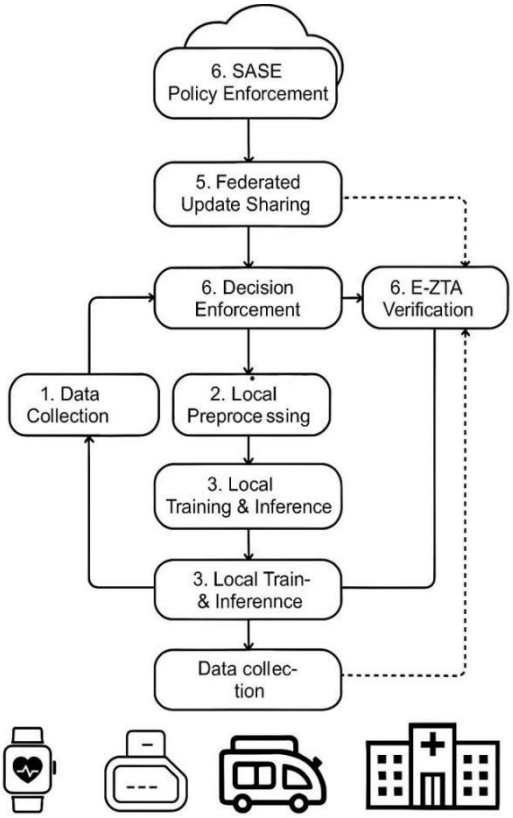


Fig. 2. Workflow of the proposed FL-EZTF framework showing sequential steps: data collection, preprocessing, local training and inference, federated update sharing, E-ZTA verification, decision enforcement, and SASE policy integration.

Table 5. Data Preprocessing Stages in the FL-EZTF Framework

Stage	Preprocessing Step	Techniques Used
1	Data Cleaning	Removal of duplicate records, null values, corrupted entries, and irrelevant traffic features from raw IoT datasets.
2	Feature Encoding	One-hot encoding and label encoding of categorical attributes such as protocol type, service category, and connection flags.
3	Feature Normalization	Min–max normalization applied to numerical traffic features to maintain consistent feature ranges across heterogeneous IoT devices.
4	Feature Selectionand Reduction	Correlation analysis and Principal Component Analysis (PCA) used to eliminate redundant features and reduce dimensionality.
5	Temporal Window Generation	Sliding window segmentation applied to capture sequential traffic behavior and temporal attack patterns.
6	Non-IID Data Partitioning	Dataset distributed across federated clients with uneven class and feature distributions to simulate realistic healthcare IoT environments.
7	Localized Edge Processing	All preprocessing operations executed locally at healthcare edge nodes to preserve privacy and reduce centralized data exposure.

4.2. Data Preprocessing

Table 5 summarizes the data preprocessing pipeline integrated into the proposed FL-EZTF framework. First, raw IoT traffic data and healthcare telemetry data are filtered to remove duplicate, incomplete, and irrelevant data. For heterogeneous devices, categorical network attributes are transformed using one-hot and label encoding, while numerical features are transformed using min-max normalization. Feature reduction and dimensionality optimization are performed using Principal Component Analysis (PCA) and correlation analysis to balance edge computing and efficiency.

To capture the temporal behavior of attacks and the dependent structure of traffic, the sliding window segmentation is used. The prepared data is then distributed to each federated client using a non-IID partitioning method aligned with realistic healthcare IoT deployments and traffic distribution. All preprocessing steps are done at the edge or client node, which preserves data privacy and aligns with the principles of federated learning.

4.3. Federated Simulation Details

Table 6 presents the federated simulation parameters of the proposed FL-EZTF model. Each healthcare institution represents a federated client with diverse IoT traffic and device profiles. To simulate realistic healthcare IoT scenarios, datasets are partitioned using a Non-IID strategy with imbalanced features and class distributions among clients. Federated learning is performed over 100 global communication rounds. Each client performs 5 local epochs using the Adam optimizer with a batch size of 64.

In addressing reviewers' concerns about the scalability, experiments are also performed with 10, 25, and 50 federated clients. Also, the FL-EZTF model adopts a trust-aware Federated Averaging method to enhance the framework's robustness against unreliable or malicious participants. Additionally, the combination of gradient compression and a sparse model update approach reduces the communication overhead, allowing the framework to be efficiently applied to distributed healthcare edge environments.

Table 6. Federated Simulation Configuration for the Proposed FL-EZTF Framework

Simulation Parameter	Configuration Details
Number of Federated Clients	10, 25, and 50 simulated clients representing hospitals or healthcare edge gateways.
Client Representation	Each client represents an independent healthcare institution with local IoT devices and heterogeneous traffic behavior.
Data Distribution Strategy	Non-IID partitioning to simulate realistic traffic diversity across distributed healthcare IoT environments.
Non-IID Partitioning Method	Uneven class distribution and feature skew applied across federated clients.
Global Communication Rounds	100 communication rounds performed for stable federated convergence.
Local Training Epochs	5 local epochs executed at each client during every communication round.
Batch Size	Mini-batch size of 64 samples used for local model optimization.
Optimizer	Adam optimizer with learning rate of 0.001.
Federated Aggregation Method	Trust-aware Federated Averaging (TA-FedAvg) with weighted client aggregation.
Client Participation Rate	Partial client participation enabled to simulate dynamic healthcare edge availability.
Communication Optimization	Gradient compression and sparse update transmission applied to reduce bandwidth overhead.

Table 7. Model Architectures and Hyperparameter Configuration

Parameter	Configuration
Model Types	LSTM Autoencoder (LSTM-AE), CNN–LSTM Hybrid, 1D-CNN
Input Features	Selected network and telemetry features after preprocessing and PCA reduction
LSTM-AE Structure	Two LSTM layers with 128 and 64 hidden units for sequential anomaly reconstruction
CNN–LSTM Structure	1D convolutional layers for spatial feature extraction followed by LSTM layers for temporal learning
1D-CNN Structure	Lightweight convolutional layers optimized for resource-constrained healthcare IoT devices
Activation Functions	ReLU for convolution layers and Tanh for LSTM layers
Dropout Rate	0.3 for overfitting reduction and training stability
Optimizer	Adam optimizer
Learning Rate	0.001
Loss Functions	Mean Squared Error (LSTM-AE), Categorical Cross-Entropy (CNN–LSTM and 1D-CNN)
Batch Size	64 samples
Training Strategy	Local federated training with trust-aware global aggregation (TA-FedAvg)

4.4. Model Architectures & Hyperparameters

Table 7 describes the architectures and hyperparameters used within the proposed FL-EZTF framework. To deploy in resource-limited healthcare IoT environments while effectively capturing the temporal and spatial patterns of attacks, lightweight deep learning models are used. The LSTM Autoencoder is used for the reconstruction of sequential anomalies and the detection of abnormal IoT activities, while the CNN–LSTM hybrid model is used for the detection of coordinated attacks due to its spatial and temporal feature learning abilities. The 1D-CNN model is designed for real-time, low latency inferences on wearable and edge healthcare devices with limited computing capabilities.

All models are trained using dimensionally reduced feature vectors generated after feature preprocessing and PCAbased feature reduction. In heterogeneous federated environments, dropout regularization is applied to mitigate the impact of overfitting, and the Adam optimizer with a learning rate of 0.001 is used to ensure convergence. The proposed trust-aware federated aggregation mechanism aggregates the local model updates generated at the federated healthcare clients.

4.5. Baselines

Evaluating the performed comparisons with the FL-EZTF framework, various established baseline frameworks used within the context of IoT security and intrusion detection have been considered. The first comparison is with a Centralized Deep Learning Intrusion Detection System (Centralized DL IDS) [27]. Centralized learning models, although they can achieve a high level of accuracy for detection, tend to be very risky for the privacy of users and for healthcare systems, impose a high level of communication overhead, and lack scalability in a distributed setting.

Lack of adaptive trust management and policy enforcement, within the context of a Federated Learning (FL)-based Intrusion Detection System (IDS), is referred to as the second baseline [28]. A comparison of this kind helps to determine the merits and demerits of the frameworks incorporating federated learning only in the context of IoT Healthcare Security. The evaluation scope is enlarged by comparing the framework with a Zero Trust Architecture (ZTA)-only framework (ZTAonly 2025). Zero Trust (ZT) systems improve security of access; however, support to detect and mitigate attacks in a real-time and automated manner is largely absent and remains unexplored. The evaluation framework also includes a Single Architecture for Security in the Enterprise (SASE)-only framework [29]. Absence of federated intelligence, within the context of access policy control and Cloud/Edge management security, is what this baseline considers. Distributed security includes, but is not limited to, integration of Secure Web Gateways (SWG), Cloud Access Security Brokers (CASB), Firewall-as-a-Service (FWaaS), and Zero Trust Network Access (ZTNA). The inability to address the evolving nature of cyber threats through collaborative learning and adaptive threat intelligence remains a disadvantage for the framework. Finally, the proposed FL-EZTF framework also compares FedProx and Byzantine-resilient aggregation methods to assess scalability, communication efficiency, and the ability to counter malicious federated participants. With these comparisons, FL-EZTF intends to offer advancements in privacy preservation, adaptive trust enforcement, detection accuracy, robustness, and threat mitigation in real-time across distributed healthcare IoT ecosystems.

4.6. Evaluation Metrics

Table 8 lists the evaluation metrics of the proposed FL-EZTF framework. The evaluation of the federated learning module is done using the standard classification metrics of accuracy, precision, recall, and F1-score. These assess the reliability of intrusion detection and classification. Moreover, training efficiency and containment are evaluated by the False Positive Rate (FPR) and the number of convergence rounds. The suitability of the proposed framework for resource-constrained healthcare IoT is evaluated by the communication overhead. To measure the trust-aware federated aggregation mechanism's resilience to unreliable or malicious clients' attacks, the Trust-aware Federated Aggregation Mechanism incorporates the Attack Success Rate (ASR), the Byzantine Detection Rate (BDR), and exposed Poisoned Client Impact (PCI). For the E-ZTA decision and containment layer, containment time, decision latency, and Mean Time to Detection (MTTD) are the evaluation metrics for real time threat response and adaptive security infringement. In addition, the False Rejection Rate (FRR) is evaluated to measure the influence of security measures on legitimate users and devices in healthcare. Overall, these metrics provide a comprehensive evaluation of detection accuracy, scalability, the balance of communication efficiency, and operational feasibility in distributed healthcare IoT environments.

5. Results and Discussion

5.1. Intrusion Detection Performance

The proposed FL-EZTF framework's intrusion detection performance is assessed using multiple baseline approaches, including Centralized DL IDS, FL-only IDS, ZTA-only, SASE-only, FedProx, and Byzantine-Robust FL models. Each experiment was conducted five times. The results show average performance with standard deviation. As presented in Table 9, FL-EZTF outperforms all the other methods in terms of detection accuracy and false positive rates. The integration of trust-aware federated aggregation, adaptive trust verification, and edge-level policy enforcement enhances detection reliability and trust within the federated learning architecture for distributed healthcare IoT systems.

5.2. Federated Learning Convergence Analysis

The convergence capacity of the proposed FL-EZTF framework is analyzed by numerous federated communication rounds. As presented in Table 10, the FL-EZTF framework offers rapid convergence and improved model stability, compared to standard federated learning frameworks. The trust-aware aggregation mechanism lessens the detrimental effects of both uncertain and unreliable client updates and enhances learning consistency across the health care IoT ecosystems.

5.3. Communication Overhead and Scalability Analysis

The flexibility and efficiency of communication for various numbers of federated healthcare clients were tested. The study analyzes communication latency, overhead, and the accuracy of detection versus the number of clients. Table 11 shows that the framework's detection accuracy remains optimal with increased clients. The framework balances communication overhead and latency despite a gradual increase with a large number of clients. The results of this study confirm positive scalable results for the distributed Integrated Federated Learning for Healthcare IoT with Thin Client (FL-EZTF) systems.

5.4. Robustness Against Poisoning and Byzantine Attacks

Poisoning attacks simulate adversarial robustness evaluations, permitting 20% of federated clients to send altered model updates during aggregation. FL-EZTF's performance is evaluated against other standard federated learning methods, defending against malicious participatory clients. Table 12 displays how the FL-EZTF framework is more robust in the presence of malicious federated clients than other baseline methods. The aggregation strategy is trust-aware, which decreases the impact of malicious updates, and further enhances the detection of Byzantine clients. Consequently, FL-EZTF has lower adversarial attack successes and overall stable performance for intrusion detection in adversarial environments.

Table 8. Critical Evaluation Parameters for the FL-EZTF Framework

Parameter	Description
Federated Learning (FL) Module	
Accuracy (%)	Overall correctness of intrusion classification.
Precision (%)	Percentage of predicted attacks that are true positives.
Recall (%)	Fraction of actual attacks successfully detected.
F1-score (%)	Harmonic balance between precision and recall.
False Positive Rate (FPR)	Legitimate traffic incorrectly classified as malicious.
Convergence Rounds	Number of federated rounds required for stable convergence.
Communication Overhead	Bandwidth consumption during federated model updates.
Attack Success Rate (ASR)	Percentage of successful adversarial or poisoning attacks.
Byzantine Detection Rate (BDR)	Ability to identify malicious or unreliable federated clients.
Poisoned Client Impact (PCI)	Influence of compromised client updates on global model performance.
E-ZTA Decision and Containment Layer	
Containment Time (s)	Delay between threat detection and device isolation.
Decision Latency (ms)	Time required for risk evaluation and policy enforcement.
Mean Time to Detection (MTTD)	Average time required to detect malicious activity.
False Rejection Rate (FRR)	Legitimate users or devices incorrectly restricted or quarantined.

Table 9. Intrusion Detection Performance Comparison of FL-EZTF and Baseline Methods

Method	Accuracy	Precision	Recall	F1-Score	FPR
Centralized DL IDS	95.4 ± 0.5	94.8 ± 0.6	95.9 ± 0.5	95.3 ± 0.4	4.7 ± 0.3
FL-only IDS	93.2 ± 0.6	92.4 ± 0.5	93.8 ± 0.6	93.1 ± 0.5	5.6 ± 0.4
ZTA-only	84.7 ± 0.8	83.5 ± 0.7	85.1 ± 0.9	84.2 ± 0.7	9.2 ± 0.5
SASE-only	86.5 ± 0.7	85.9 ± 0.8	86.7 ± 0.7	86.2 ± 0.6	8.4 ± 0.4
FedProx	94.1 ± 0.5	93.7 ± 0.6	94.4 ± 0.5	94.0 ± 0.5	5.1 ± 0.3
Byzantine-Robust FL	95.0 ± 0.4	94.5 ± 0.5	95.2 ± 0.4	94.8 ± 0.4	4.3 ± 0.3
Proposed FL-EZTF	97.1 ± 0.3	96.6 ± 0.4	97.5 ± 0.3	97.0 ± 0.3	3.1 ± 0.2

Table 10. Federated Learning Convergence Comparison

Method	Convergence Rounds	Final Accuracy
FedAvg	128	93.4
FedProx	112	94.3
Byzantine-Robust FL	104	95.1
Proposed FL-EZTF	89	97.1

Table 11. Scalability and Communication Overhead Analysis

Clients	Accuracy (%)	Latency (ms)	Communication Overhead (MB)
10	97.1	82	4.1
25	96.5	97	5.8
50	95.8	118	7.2

Table 12. Robustness Evaluation Under Poisoning and Byzantine Attacks

Method	Accuracy Under Attack (%)	ASR (%)	BDR (%)
FedAvg	81.4	27.5	61.2
FedProx	86.3	19.8	73.6
Byzantine-Robust FL	91.5	11.2	88.4
Proposed FL-EZTF	94.6	6.7	94.1

5.5. E-ZTA Decision and Threat Containment Analysis

The E-ZTA decision and containment layer seeks to understand the impact of adaptive trust enforcement coupled with real-time threat enforcement in a distributed healthcare IoT context. As depicted in Table 13, the FL-EZTF framework compared to baseline systems shows a dramatic improvement in containment and decision latency. The combination of E-ZTA and SASE-based adaptive policy enforcement leads to the quick isolation of breached devices and containment of incidents within the healthcare IoT ecosystem. The framework also demonstrates effective security and operational balance through further reductions in the False Rejection Rate.

5.6. Comparative Analysis with Baseline Methods

The comparative analysis indicates that the proposed FL-EZTF framework strikes a better balance among intrusion detection, scalability, communication efficiency, adversarial robustness, and adaptive threat containment. Centralized learning techniques enable strong detection, but privacy, scalability, and other challenges emerge with centralized data collection. FL-only techniques, while strengthening privacy, do not offer adaptive trust management or real-time enforcement. ZTA-only and SASE-only approaches provide access control and distributed policy enforcement but, in tandem, exhibit limited intrusion detection and threat intelligence.

Under the integration of trust-aware federated learning and SASE-based security orchestration, the FL-EZTF framework incorporates intelligent intrusion detection with adaptive trust and cloud-edge policy enforcement and management. Hence, the proposed framework provides a scalable and privacy-preserving security solution that meets the requirements of healthcare IoT.

5.7. Discussion and Practical Implications

The experimental evaluation verifies that the framework FL-EZTF markedly enhances the reliability of intrusion detection and the efficiency of communication, as well as robustness to adversarial attacks. Moreover, it enhances the containment of adaptive threats within healthcare IoT systems. The integration of trust-aware federated aggregation mitigates the harmful effects of malicious participants within federated learning and enhances the overall stability of the global model. The integration of E-ZTA and SASE also promotes the enforcement of security control across both the cloud and the edge, within acceptable latency for decisions and faster responses to threats. While the advantages highlighted previously are important, some notable shortcomings exist. The operational testing was performed not on actual hospital deployments but on simulated healthcare IoT environments. Additionally, significant communication overhead could be experienced in very large federated networks with extremely high client mobility. The next steps will concern the

Table 13. E-ZTA Decision and Threat Containment Performance

Framework	Containment Time (s)	Decision Latency (ms)	FRR (%)
Centralized DL IDS	6.8	176	6.1
FL-only IDS	7.3	162	5.5
ZTA-only	8.7	214	7.9
SASE-only	7.8	191	6.8
Proposed FL-EZTF	3.2	81	3.4

integration of lightweight explainable AI, and advanced federated Byzantine-resilient optimization for large federated IoT environments within the healthcare domain. In the provided figure 3, we visualize the performance of the proposed

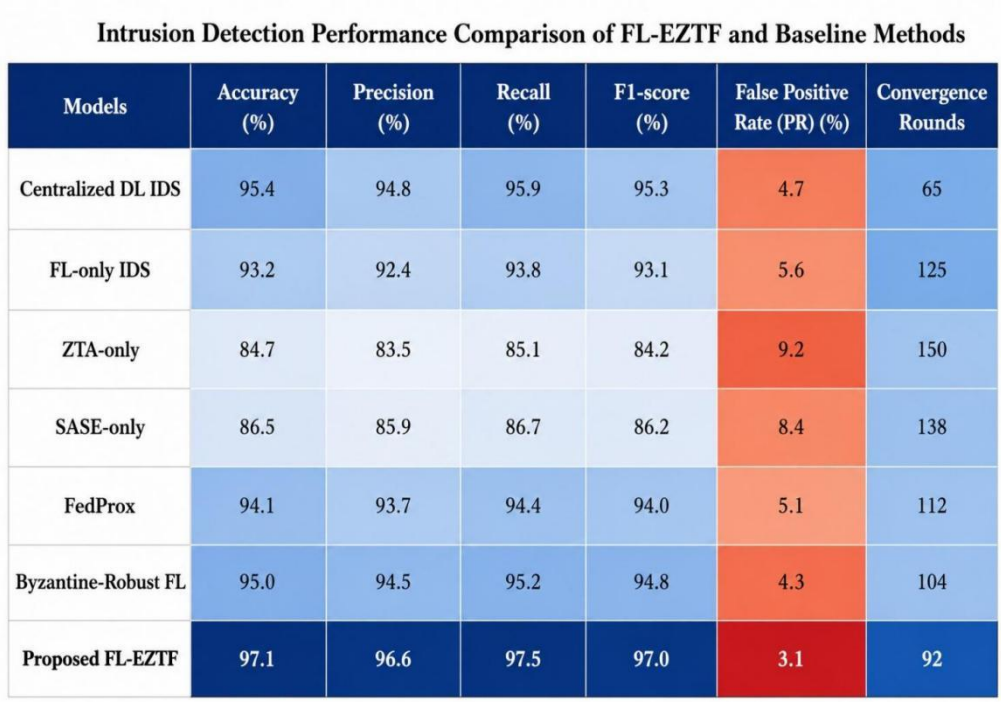


Fig. 3. Heatmap comparison of baseline models and the proposed FL-EZTF framework across key detection and efficiency metrics.

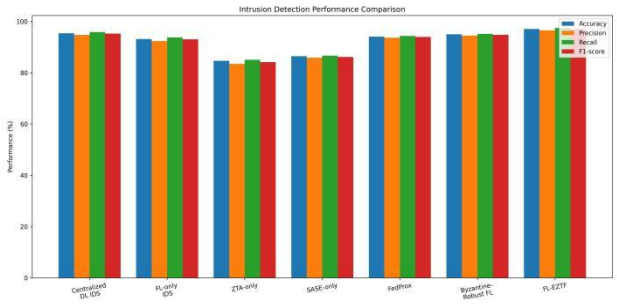
FL-EZTF framework with various baseline methods using heatmaps. From the visualization we can see that FL-EZTF is consistently better in detection accuracy, fewer false positives, and better convergence.

Figure 4 depicts the in-depth assessment of the FL-EZTF framework, addressing multiple dimensions of performance. Evidence in Figure 4a indicates that FL-EZTF outperforms all baseline methods in detection with respect to accuracy, precision, recall, F1-score, and the false positive rate. The results in Figure 4b suggest that compared to other typical federated learning methods, the integration of trust-aware federated aggregation improves the stability of the global model and decreases the convergence time. Figure 4c depicts that as the number of federated healthcare clients increases, the detection performance of FL-EZTF remains stable, and the communication overhead remains low. In Figure 4d, the framework outperforms existing solutions against poisoning and Byzantine attacks in terms of both attack success rate and malicious client detection. Finally, the results in Figure 4e indicate that the use of the E-ZTA decision and containment layer improves the adaptive healthcare IoT security enforcement by reducing decision and containment latency and the false rejection rate.

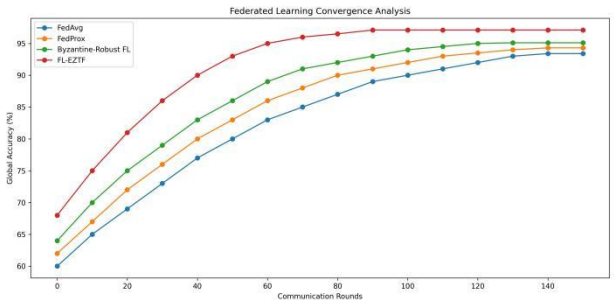
6. Conclusion and Future Work

In this study, an innovative framework called FL-EZTF was developed, based on trust-aware federated learning, Enhanced Zero Trust Architecture (E-ZTA), and SASE-enabled policy enforcement, to deliver adaptive privacy and security mechanisms for IoT-based healthcare systems. The principles of this framework differ from traditional methods of centralized or standalone federated intrusion detection. Instead, it combines distributed anomaly detection with ongoing trust verification and adaptive threat containment within the cloud-edge continuum. FL-EZTF enhances privacy preservation and intrusion detection capability and enables federated collaboration by retaining sensitive healthcare data within the local boundaries of the participating healthcare organizations.

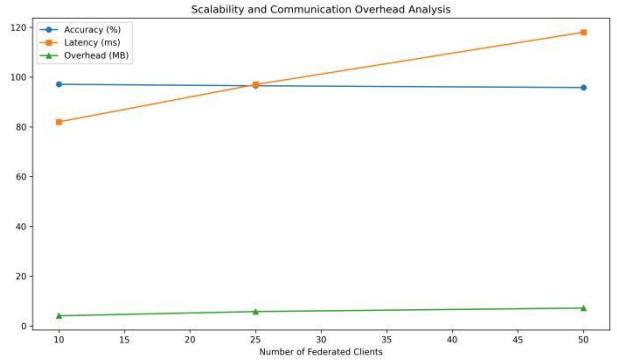
FL-EZTF's experimental evaluation in various healthcare IoT settings demonstrated improvements in detection accuracy, reduction in false positives, convergence, adversarial attacks, and containment response times in comparison to centralized, federated-only, and policy-only baseline approaches. Due to the incorporation of the trust-aware aggregation and adaptive policy enforcement, FL-EZTF demonstrates resilience to malicious federated participants with low decision



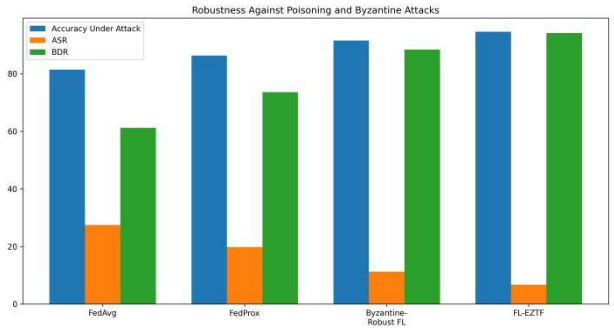
(a) Intrusion Detection Performance Comparison



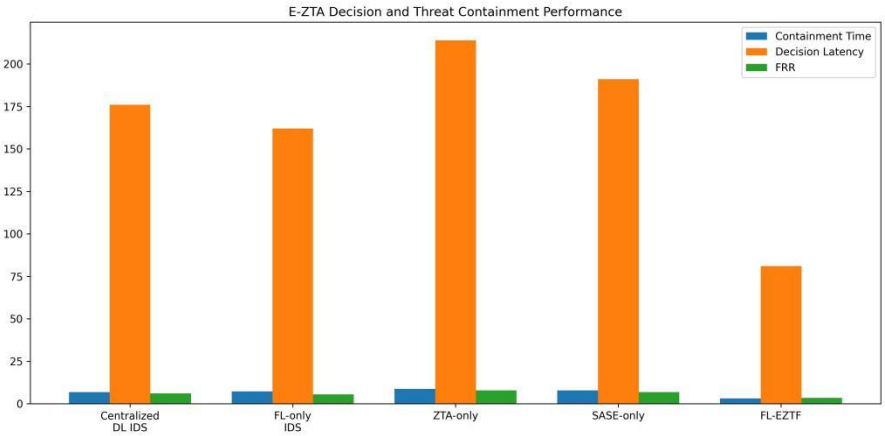
(b) Federated Learning Convergence Analysis



(c) Scalability and Communication Overhead Analysis



(d) Robustness Against Poisoning and Byzantine Attacks



(e) E-ZTA Decision and Threat Containment Performance

Fig. 4. Comprehensive performance evaluation of the proposed FL-EZTF framework across intrusion detection, federated convergence, scalability, adversarial robustness, and adaptive threat containment metrics.

latency. The framework also supports containment in time-critical healthcare scenarios. The framework's resilience to performance degradation under increasing participation of federated clients also supports its feasibility for large-scale, highly distributed IoT systems.

Promising as these initial results may be, some shortcomings remain. The framework was only validated in healthcare IoT simulation setups, and some evaluations in real hospital infrastructures should be completed to improve this framework. The focus of the upcoming studies will be to develop the framework into larger and more dynamic federated systems and to integrate Byzantine-resilient aggregation, lightweight explainable AI, and real-time adaptive learning in order to address evolving threats and provide resilience to the frame. Energy-efficient federated optimization for real-time deployment of FL-EZTF in functional smart healthcare systems will also be prioritized.

All the Declarations and Statements

Author Contributions Statement
Urvashi – Conceptualization, Methodology, Investigation, Writing–Original Draft, and Supervision. Proposed the research idea, designed the overall framework, coordinated the research activities, and drafted the initial manuscript.
Parul Agarwal– Data Curation, Software Implementation, Validation, and Formal Analysis. Performed dataset preparation, preprocessing, implementation of the proposed framework, and contributed to experimental validation.
Kamlesh Kumar Raghuvashi – Model Training, Performance Evaluation, Visualization, and Statistical Analysis. Conducted model training, evaluated system performance using benchmark datasets, prepared visualizations, and analyzed experimental results.
Jawed Ahmed – Writing–Review and Editing, Project Administration, and Technical Review. Reviewed and edited the manuscript, ensured technical consistency, and contributed to interpretation of findings and manuscript refinement.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement
The authors declare no conflicts of interest.

Funding Declaration
This research received no external funding.

Data Availability Statement
CIC-IoT-2023, IoT-23, and WESAD were the benchmark datasets made publicly available and utilized in this study. The datasets, made publicly available in the official repositories for the datasets, were selected to ensure a wide coverage for experimental validation of IoT network attacks, malicious traffic, and health-related wearable sensor collected data.

Ethical Declarations
This study does not involve human participants, human data, or animals. Therefore, ethical approval and informed consent were not required.

Acknowledgments
The authors sincerely thank the reviewers and editors for their professional evaluation and valuable recommendations, which contributed significantly to improving the quality and reliability of this research.

Declaration of Generative AI in Scholarly Writing
Generative Artificial Intelligence (AI) tools were used exclusively to strengthen the language and readability of the manuscript.

Abbreviations
The following abbreviations are used in this manuscript:

AI – Artificial Intelligence
ANN – Artificial Neural Network
ASR – Attack Success Rate
BDR – Byzantine Detection Rate
CASB – Cloud Access Security Broker
CNN – Convolutional Neural Network
DDoS – Distributed Denial-of-Service
DL – Deep Learning
DoS – Denial-of-Service
ECG – Electrocardiography
EDA – Electrodermal Activity
EHR – Electronic Health Record
ZTA – Enhanced Zero Trust Architecture
FedAvg – Federated Averaging
FedProx – Federated Proximal Optimization
FL – Federated Learning
FL-EZTF – Federated Learning-Enhanced Zero Trust Framework
FPR – False Positive Rate

FRR – False Rejection Rate
FWaaS – Firewall as a Service
GAN – Generative Adversarial Network
GRU – Gated Recurrent Unit
IDS – Intrusion Detection System
IoT – Internet of Things
LSTM – Long Short-Term Memory
LSTM-AE – Long Short-Term Memory Autoencoder
MiTM – Man-in-the-Middle
MQTT – Message Queuing Telemetry Transport
MTTD – Mean Time to Detection
PCA – Principal Component Analysis
ReLU – Rectified Linear Unit
R2L – Remote-to-Local Attack
SASE – Secure Access Service Edge
SOC – Security Operations Center
SWG – Secure Web Gateway
U2R – User-to-Root Attack
ZTA – Zero Trust Architecture
ZTNA – Zero Trust Network Access

Appendix A/B/C…, with appendix title

None

References

[1] A. Thakkar and R. Lohiya. Attack classification of imbalanced intrusion data for iot network using ensemble learning-based deep neural network. IEEE Internet of Things Journal, 10(13):11888–11895, 2023.doi: 10.1109/JIOT.2023.3274675.

[2] M. Malik, M. Dutta, et al. Feature engineering and machine learning framework for ddos attack detection in the standardized internet of things. IEEE Internet of Things Journal, 10(10):8658–8669, 2023. doi: 10.1109/JIOT.2023.3241033.

[3] P. Kumar, R. Kumar, A. Aljuhani, D. Javeed, A. Jolfaei, and A. N. Islam. Digital twin-driven sdn for smart grid: A deep learning integrated blockchain for cybersecurity. Solar Energy, 263:111921, 2023.doi: 10.1016/j.solener.2023.111921.

[4] D. Javeed, T. Gao, M. S. Saeed, and M. T. Khan. Fog-empowered augmented intelligence-based proactive defensive mechanism for iot-enabled smart industries. IEEE Internet of Things Journal, 10(16):14298–14309, 2023.doi: 10.1109/JIOT.2023.3282604.

[5] N. Cheng, S. Wu, X. Wang, Z. Yin, C. Li, W. Chen, and F. Chen. Ai for uav-assisted iot applications: A comprehensive review. IEEE Internet of Things Journal, 10(14):12608–12630, 2023.doi: 10.1109/JIOT.2023.3269488.

[6] M. Zawish, N. Ashraf, R. I. Ansari, and S. Davy. Energy-aware ai-driven framework for edge-computing-based iot applications. IEEE Internet of Things Journal, 10(6):5013–5023, 2022.doi: 10.1109/JIOT.2021.3129862.

[7] G. W. de Oliveira, M. Nogueira, A. L. dos Santos, and D. M. Batista. Intelligent vnf placement to mitigate ddos attacks on industrial iot. IEEE Transactions on Network and Service Management, 20(3):2621–2634, 2023.doi: 10.1109/TNSM.2023.3278472.

[8] Y. R. Siwakoti, M. Bhurtel, D. B. Rawat, A. Oest, and R. Johnson. Advances in iot security: Vulnerabilities, enabled criminal services, attacks and countermeasures. IEEE Internet of Things Journal, 10(14):11964–11986, 2023.doi: 10.1109/JIOT.2023.3264268.

[9] J. Cui, H. Sun, H. Zhong, J. Zhang, L. Wei, I. Bolodurina, and D. He. Collaborative intrusion detection system for sdvn: A fairness federated deep learning approach. IEEE Transactions on Parallel and Distributed Systems, 34(6):1713–1727, 2023.doi: 10.1109/TPDS.2023.3244537.

[10] A. Muhammad, K. Lin, J. Gao, and B. Chen. Robust multi-model personalized federated learning via model distillation. In International Conference on Algorithms and Architectures for Parallel Processing, pages 432–446. Springer, 2021.doi: 10.1007/978-3-030-86909-0_32.

[11] P. Singh, G. S. Gaba, A. Kaur, M. Hedabou, and A. Gurtov. Dew-cloud-based hierarchical federated learning for intrusion detection in iomt. IEEE Journal of Biomedical and Health Informatics, 27(2):722–731, 2022.doi: 10.1109/JBHI.2021.3127041.

[12] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann. Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. Journal of Network and Systems Management, 31(1):3, 2023.doi: 10.1007/s10922-022-0969-8.

[13] F. Naeem, M. Ali, and G. Kaddoum. Federated-learning-empowered semi-supervised active learning framework for intrusion detection in zsm. IEEE Communications Magazine, 61(2):88–94, 2023.doi: 10.1109/MCOM.001.22315.

[14] V. T. Truong and L. B. Le. Metacids: Privacy-preserving collaborative intrusion detection for metaverse based on blockchain and online federated learning. IEEE Open Journal of the Computer Society, 4:141–155, 2023.doi: 10.1109/OJCOMS.2023.3241629.

[15] J. Li, X. Tong, J. Liu, and L. Cheng. An efficient federated learning system for network intrusion detection. IEEE Systems Journal, 17(3):4064–4075, 2023.doi: 10.1109/JSYST.2023.3248037.

[16] A. Omotosho, Y. Qendah, and C. Hammer. Ids-ma: Intrusion detection system for iot mqtt attacks using centralized and federated learning. In Proceedings of the IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), pages 678–

688. IEEE, 2023.doi: 10.1109/COMPSAC57554.2023.00098.
[17] M. Amiri-Zarandi, R. A. Dara, and X. Lin. Sids: A federated learning approach for intrusion detection in iot using social internet of things. Computer Networks, 236:110005, 2023.doi: 10.1016/j.comnet.2023.110005.
[18] N. Hamdi. Federated learning-based intrusion detection system for internet of things. International Journal of Information Security, 22(6):1937–1948, 2023.doi: 10.1007/s10207-023-00526-7.
[19] R. Zhao, Y. Wang, Z. Xue, T. Ohtsuki, B. Adebisi, and G. Gui. Semi-supervised federated learning based intrusion detection method for internet of things. IEEE Internet of Things Journal, 10(10):8594–8606, 2022.doi: 10.1109/JIOT.2022.3147306.
[20] Z. Lian and C. Su. Decentralized federated learning for internet of things anomaly detection. In Proceedings of the ACM Asia Conference on Computer and Communications Security (AsiaCCS), pages 1249–1251. ACM, 2022.doi: 10.1145/3548692.3560657.
[21] T. A. Ahanger, A. Aldaej, M. Atiquzzaman, I. Ullah, and M. Yousufudin. Federated learning-inspired technique for attack classification in iot networks. Mathematics, 10(12):2141, 2022.doi: 10.3390/math10122141.
[22] A. Tabassum, A. Erbad, W. Lebda, A. Mohamed, and M. Guizani. Fedgan-ids: Privacy-preserving ids using gan and federated learning. Computer Communications, 192:299–310, 2022.doi: 10.1016/j.comcom.2022.07.018.
[23] D. Man, F. Zeng, W. Yang, M. Yu, J. Lv, and Y. Wang. Intelligent intrusion detection based on federated learning for edge-assisted internet of things. Security and Communication Networks, 2021:1–11, 2021.doi: 10.1155/2021/5871207.
[24] D. C. Attota, V. Mothukuri, R. M. Parizi, and S. Pouriyeh. An ensemble multiview federated learning intrusion detection for iot. IEEE Access, 9:117734–117745, 2021.doi: 10.1109/ACCESS.2021.3128914.
[25] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava. Federated learning-based anomaly detection for iot security attacks. IEEE Internet of Things Journal, 9(4):2545–2554, 2021.doi: 10.1109/JIOT.2020.3043126.
[26] K. Yadav, B. B. Gupta, C.-H. Hsu, and K. T. Chui. Unsupervised federated learning based iot intrusion detection. In Proceedings of the IEEE 10th Global Conference on Consumer Electronics (GCCE), pages 298–301. IEEE, 2021.doi: 10.1109/GCCE53087.2021.9662332.
[27] M. S. Amine, F. A. Nada, and K. M. Hosny. Improved deep learning model for intrusion detection in the internet of things. Scientific Reports, 15:21547, 2025.doi: 10.1038/s41598-025-01246-9.
[28] R. W. Anwer, M. Abrar, M. Ullah, and M. A. Shah. Advanced intrusion detection in industrial internet of things using federated learning and lstm models. Ad Hoc Networks, 156:103421, 2025.doi: 10.1016/j.adhoc.2025.103421.
[29] Z. S. M. A. Bashi. Unified secure access service edge (sase): Architecture and security enforcement. International Journal of Pervasive Computing and Communications, 21(1):45–58, 2025.doi: 10.1108/IJPCC-01-2025-0007.

Authors' Profiles

Urvashi, Urvashi is a Research Scholar in the Department of Computer Science and Engineering at Jamia Hamdard University, New Delhi, India. Her research interests include contemporary developments and emerging challenges in computer science and related interdisciplinary domains. She actively contributes to scholarly research and academic publications. Urvashi completed her undergraduate studies at PGDAV College, University of Delhi, and earned her Master of Computer Applications (MCA) from the University of Delhi. She has 8 years of teaching experience at the University of Delhi, where she has been involved in academic instruction and student mentoring in the field of computer science and related disciplines. Her research interests are focused on the Internet of Things (IoT), with an emphasis on exploring emerging technologies, connected systems, and their applications in solving real-world challenges. She is interested in contributing to research and innovation in IoT-driven solutions and advancing knowledge in the area of intelligent and interconnected computing systems.

Dr Parul Agarwal She is associated with Jamia Hamdard since 2002. She is currently a Professor, Dean, school of engineering sciences and technology, and also heading the Department of Computer Science and Engineering at Jamia Hamdard. Her area of specialization include Fuzzy Data Mining, Cloud Computing, Sustainable computing, and Soft Computing. She has published several papers in reputed and SCI, Scopus and Elsevier indexed journals and many book chapters published by CRC press, Springer, IGI-Global are to her credit. She has edited one book with CRC , one book edited with IGI GLOBAL, and three others with Springer (all SCOPUS indexed). She is the guest editor of several Special issues of reputed Scopus and SCI indexed journals. She has chaired several sessions of International/ National Conferences of repute. Currently, several PhD. Scholars are working under her supervision in the field of Brain Signalling, Energy minimization in Cloud, Time series forecasting, and Smart Building management for smart cities. She has organized a workshop as Principal Investigator in 2017, on "Use of ICT in sustainable Computing" approved by Department of Science and Technology, Govt. of India, worth 5.75 Lakhs. She has guided more than 80 Masters thesis (MCA and M.Tech.). Member of several committees at university level and membership of several professional bodies like ISTE, and senior member IEEE are to her credit.

Dr. Kamlesh Kumar Raghuvanshi He is an Assistant Professor in the Department of Computer Science at Ramanujan College, University of Delhi. He possesses more than 23 years of professional experience, including 14 years in teaching and research and 9 years in the information technology industry. He earned his Ph.D. in Computer Science and has established himself as an academician, researcher, and technology professional with expertise in software engineering, enterprise applications, ERP solutions, educational technology, and digital transformation. Throughout his academic career, he has been actively involved in teaching undergraduate and postgraduate courses, mentoring students, and contributing to curriculum development and institutional growth. Dr. Raghuvanshi has published more than 15 research papers in reputed national and international journals and conference proceedings. He is the author of four books and has successfully guided two research scholars. His research interests include software engineering, enterprise resource planning systems, e-governance, artificial intelligence applications, and technology-enabled education. Prior to joining academia, he worked with leading multinational organizations, including IBM, Tata Consultancy Services (TCS), Wipro Technologies, and Tech Mahindra, gaining extensive experience in software development, project management, and enterprise solutions. His rich industry background enables him to effectively bridge the gap between academic learning and industry requirements.

Dr Jawed Ahmed He is a Professor in the School of Engineering Science and Technology, where he teaches postgraduate students in Computer Science and Bioinformatics. With over 20 years of teaching experience, his primary areas of interest include Bioinformatics, Machine Learning, and Data Science. He has successfully guided 5 PhD candidates to completion and is currently supervising 10 PhD scholars. Beyond academics and research, Prof. Jawed Ahmed serves as: Director, Centre for Innovation, Incubation and Entrepreneurship,Jamia Hamdard University, Deputy Advisor, Foreign Students Affairs, Jamia Hamdard University, Coordinator, National Service Scheme (NSS), Ministry of Youth Affairs and Sports, Government of India and Chairman, Delhi Chapter, Indian Society for Technical Education (ISTE). He remains actively engaged in promoting innovation, technical education, and community service.

How to cite this paper

Urvashi, Parul Agarwal, Kamlesh Kumar Raghuvanshi, Jawed Ahmed, "FL-EZTF: A Privacy-Preserving Federated Deep Learning Framework with Enhanced Zero Trust for Healthcare IoT Security", International Journal of Engineering and Manufacturing (IJEM), Vol.16, No.4, pp.324-343, 2026. DOI:10.5815/ijem.2026.04.22