



## OPEN ACCESS

## EDITED BY

Riaz Ullah Khan,  
University of Electronic Science and  
Technology of China, China

## REVIEWED BY

Rajesh Kumar,  
University of Electronic Science and  
Technology of China, China  
Amin Ul Haq,  
University of Electronic Science and  
Technology of China, China  
Waqas Amin,  
Southwest University of Science and  
Technology, China

## \*CORRESPONDENCE

Bela Shrimali  
✉ bela.shrimali@gmail.com  
Swapnoneel Roy  
✉ s.roy@unf.edu

RECEIVED 03 July 2025

ACCEPTED 16 October 2025

PUBLISHED 22 January 2026

## CITATION

Shrimali B, Gajjar J, Roy S, Patel S, Patel K and  
Naik RR (2026) EnDuSecFed: an ensemble  
approach for privacy preserving Federated  
Learning with dual-security framework for  
sustainable healthcare.

*Front. Big Data* 8:1659026.

doi: 10.3389/fdata.2025.1659026

## COPYRIGHT

© 2026 Shrimali, Gajjar, Roy, Patel, Patel and  
Naik. This is an open-access article distributed  
under the terms of the [Creative Commons  
Attribution License \(CC BY\)](#). The use,  
distribution or reproduction in other forums is  
permitted, provided the original author(s) and  
the copyright owner(s) are credited and that  
the original publication in this journal is cited,  
in accordance with accepted academic  
practice. No use, distribution or reproduction  
is permitted which does not comply with  
these terms.

# EnDuSecFed: an ensemble approach for privacy preserving Federated Learning with dual-security framework for sustainable healthcare

Bela Shrimali<sup>1\*</sup>, Jenil Gajjar<sup>2</sup>, Swapnoneel Roy<sup>3\*</sup>, Sanjay Patel<sup>2</sup>,  
Kanu Patel<sup>2</sup> and Ramesh Ram Naik<sup>2</sup>

<sup>1</sup>Unitedworld Institute of Technology, Karnavati University, Gandhinagar, Gujarat, India, <sup>2</sup>Department of  
Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat,  
India, <sup>3</sup>School of Computing, University of North Florida, Jacksonville, FL, United States

Recent advances in Artificial Intelligence have highlighted the role of Machine Learning in healthcare decision-making, but centralized data collection raises significant privacy risks. Federated Learning addresses this by enabling collaborative training across multiple clients without sharing raw data. However, Federated Learning remains vulnerable to security threats that can compromise model reliability. This paper proposes a dual-security Federated Learning framework that integrates Fernet Symmetric Encryption for secure transmission of model updates using symmetric encryption and an Intrusion Detection System to detect anomalous client behavior. Experiments on a publicly available healthcare dataset show that the proposed system enhances privacy and robustness compared to traditional FL. Among tested models, including Logistic Regression, Random Forest, and SVC, the ensemble method achieved the best performance with 99% accuracy.

## KEYWORDS

Federated Learning, Fernet Symmetric Encryption, Intrusion Detection System, Logistic Regression, Random Forest, Support Vector Classifier

## 1 Introduction

According to the Gartner report-2025 ([Gartner, 2025](#)), about 27% of organizations have faced a privacy breach or security issue related to Artificial Intelligence (AI). This means that there were intentional attacks on the organization's AI systems because they collect and process data in a central place. Federated Learning (FL) has emerged as a robust method for training machine learning models across multiple clients while maintaining the privacy of their local data. Unlike traditional methods where data is collected in one location, FL allows each client to have control of its data ([Wang et al., 2023b](#)). This is particularly useful in sensitive areas like healthcare, where patient information must be kept confidential ([Khatun et al., 2023](#); [Almalawi et al., 2023](#); [Naresh and Thamarai, 2023](#)). By using FL, healthcare providers can create better models by combining knowledge from different datasets without risking the privacy and security of individual patient data ([Chaddad et al., 2023](#); [Joshi et al., 2022](#); [Kumar and Singla, 2021](#)).

Despite its advantages, FL presents several challenges. Its decentralized architecture can introduce security vulnerabilities, particularly in securing the updates exchanged between clients and the central server. In a standard FL framework, the local model weights from

each client are aggregated to form a global model. This aggregation process, however, is susceptible to security threats (Li et al., 2023; Coelho et al., 2023; Ali et al., 2024), such as data poisoning and adversarial attacks, which can compromise the performance of the global model. Such concerns are especially critical in healthcare applications, where prediction accuracy directly impacts patient safety.

To manage these risks, encrypted communication using the Fernet Symmetric Encryption (FSE) technique is implemented during the sharing of model updates between local clients and the global server. FSE allows secure calculations on encrypted data, ensuring that the model updates shared remain private. With FSE, the system protects sensitive information from attackers while still allowing clients to work together. This means even if a malicious client tries to change its model updates, the encryption will stop it from damaging the global model. While FSE secures model updates during sharing, it does not automatically detect malicious behavior or unusual activity in the Federated Learning system. Attackers can still send harmful updates that may compromise the global server. To address this, an Intrusion Detection System (IDS) is deployed at the global server to monitor and analyze incoming model updates for suspicious activity. By identifying abnormal patterns, the IDS can detect attacks such as model poisoning. This combined approach—using FSE for secure sharing and IDS for anomaly detection—enhances the overall security and trustworthiness of the FL process.

## 1.1 Motivation

Preserving the privacy of sensitive information is critical in healthcare, and FL has emerged as a promising paradigm as it enables collaborative model training without sharing raw data. Nevertheless, FL remains vulnerable to security threats, where malicious clients may submit harmful updates that compromise the global model's accuracy. This study aims to strengthen FL security in healthcare, where reliability is crucial for patient care. To address these challenges, Fernet Symmetric Encryption (FSE) is employed to safeguard model updates against tampering, while an IDS at the central server detects anomalous client behavior. The main contributions of this research are:

- We propose a federated learning method with dual security. A communication between local clients and the main server is secured using FSE and protects data changes at the central server with an IDS. Our method is shown to be better in security analysis compared to existing methods.
- To improve decision-making and predictions, along with existing models, an ensemble approach is also implemented

**Abbreviations:**  $D_i$ , Private dataset of node  $i$ ;  $M_i$ , Local model of node  $i$ ;  $FSE_i$ , FSE instance of node  $i$ ;  $W_i$ , Local model weights of node  $i$ ;  $enc\_W_i$ , Encrypted weights of node  $i$ ;  $M_c$ , Global model of central server;  $IDS_c$ , IDS instance of central server;  $FSE_c$ , FSE instance of central server;  $con\_t$ , Convergence threshold;  $max\_rounds$ , Maximum training rounds;  $current\_round$ , Current round number;  $enc\_weights$ , Collection of encrypted weights;  $anomalies_s$ , Detected anomalies at server;  $dec\_weights$ , Decrypted weights at server.

that combines predictions from three main models: Logistic Regression, Support Vector Classifier, and Random Forest at the local node for training.

- We also discuss various attacks on privacy in FL models and highlight how our dual security approach adds value to this research area.

## 1.2 Organization

The remainder of this paper is structured as follows. Section 2 presents a comprehensive review of the existing literature. Section 3 details the proposed system architecture, including methodology, system components, and their interactions. Section 4 describes the experimental setup with the description of dataset, models and proposed algorithms. Section 5 provides an in-depth security analysis of the FSE scheme and IDS components, examining potential vulnerabilities and their mitigations. Section 6 presents experimental results, including performance metrics, comparative analysis, and validation of the approach. Lastly, Section 7 concludes with the key findings, discusses the implications of the work, and outlines promising directions for future research in this domain.

## 2 Literature review

FL has emerged as a promising privacy-preserving paradigm, particularly in sensitive domains such as healthcare. Unlike centralized machine learning, FL enables distributed model training without directly sharing raw data, thus safeguarding patient privacy. However, despite its advantages, FL remains vulnerable to adversarial threats, including data poisoning, label-flipping, and model poisoning attacks, where malicious clients can manipulate updates to reduce the performance of the global model (Hiwale et al., 2023). To address these vulnerabilities, researchers have explored various privacy-enhancing and security-aware strategies, which can be broadly categorized into: privacy-preserving approaches, cryptographic frameworks, IDS integration, and blockchain-enabled solutions. Privacy-preserving and cryptographic approaches.

Alazab et al. (2023) investigated FL for privacy-preserving Intrusion Detection Systems, comparing its performance against traditional deep learning models. By using the FedAvg algorithm, autoencoder-based anomaly detection, and secure gRPC channels, they reported high accuracy (98.07%), precision (97.4%), recall (99.06%), and F1-score (98.21%). Similarly, Wang et al. (2023a) introduced PPFLHE, a framework that leverages homomorphic encryption to address privacy and communication overhead in healthcare FL. Their system achieved 81.53% accuracy, showing that encryption can secure model updates but may also introduce computational overhead.

To mitigate adversarial threats, Almalki et al. (2024) proposed a hybrid Healthcare 5.0 framework that combines FL, IDS, and Blockchain Technology (BCT). Their solution improved diagnostic accuracy (93.89%) while enhancing data protection in Internet of Medical Things (IoMT) applications. Schneble (2018) explored FL-based distributed IDS for Medical Cyber-Physical Systems (MCPS), focusing on detecting cyberattacks while

maintaining high accuracy and low false-positive rates. [Guduri et al. \(2023\)](#) further advanced security in FL by integrating blockchain with lightweight encryption and proxy re-encryption to secure Electronic Health Records (EHR). Their Ethereum-based testbed demonstrated superior resistance to unauthorized access compared with existing models.

While this literature demonstrates significant progress, several gaps remain. Privacy-preserving approaches like homomorphic encryption and FSE secure data during communication but do not inherently detect malicious updates, leaving models vulnerable to model poisoning. IDS-based solutions focus on anomaly detection but face challenges in scalability and false alarms in highly distributed healthcare environments. Blockchain-enhanced systems improve auditability and decentralization but often introduce high computational and communication overhead. Furthermore, many proposed frameworks are evaluated on limited datasets or focus primarily on accuracy, with less emphasis on robustness against adaptive adversaries or combined privacy-security trade-offs.

From this review, it is evident that while existing literature addresses either privacy (via encryption/FSE) or security (via IDS/blockchain), very few frameworks offer a comprehensive and lightweight defense mechanism that jointly ensures secure sharing of updates and real-time detection of adversarial behaviors in FL for healthcare applications. This gap motivates our research, where we propose an integrated approach combining FSE for privacy-preserving updates with a global IDS for anomaly detection, thereby enhancing the trustworthiness of FL in sensitive healthcare settings.

[Table 1](#) provides a summary of the existing state-of-the-art in FL for healthcare applications, highlighting their contribution, limitations, technologies used, comparison parameters, and security concerns/attacks discussed.

### 3 Proposed architecture

This section covers the discussion on FL and proposed architecture along with security mechanisms, i.e., FSE and IDS, in separate subsections.

#### 3.1 Overview of the architecture

[Figure 1](#) illustrates a Federated Learning (FL) framework used in healthcare facilities, having an IDS and FSE to guarantee security throughout the communication and learning process. The process/steps of the proposed work, as shown in [Figure 1](#) are as follows:

- **Local model training:** Each medical facility (e.g., Healthcare Institute 1, 2, 3, ... N) uses the infrastructure of the organization to process its local dataset and train a machine learning model. This guarantees the confidentiality of the patient's information. The training procedure closely complies with privacy-protecting guidelines.
- **Local model sharing with FSE:** After training, updates to the local model are encrypted, then sent to the central server via FSE. By preventing unwanted access or tampering, this

encryption guarantees that the model updates remain secure while in transit. Malicious local nodes trying to deduce private information during communication are another risk that the FSE reduces.

- **Global model aggregation:** To create a global model, the central server gathers the encrypted weights that are received from each participating local node and decrypts them. The central server accurately aggregates the contributions of local nodes without introducing any malicious activity because it is presumed to be non-malicious.
- **Global IDS monitoring:** An IDS at the central server is used to keep an eye out for irregularities in decrypted model updates, even though the server is reliable. To make sure they don't have a detrimental effect on the global model, the IDS detects and flags suspicious updates coming from potentially malicious local nodes, such as those with extreme model parameter deviations.
- **Global Model Distribution:** Following aggregation, each local healthcare facility receives a copy of the global model. To increase the precision of its forecasts, every institution makes use of the recent global model.

The proposed architecture ensures that malicious activity coming from local nodes is identified and stopped before it can compromise the integrity of the global model by combining FSE for secure communication with an IDS for anomaly detection.

#### 3.2 Working of federated learning framework

A decentralized machine learning technique called federated learning allows several devices or organizations ([Oh and Nadkarni, 2023](#)) to work together to train a model without exchanging raw data. Multiple local nodes and a global node make up an FL's two ends, with the client servers keeping their local data and the central server maintaining the global model ([Islam et al., 2023](#)). Each client uses its data in the paradigm to train the model locally; only the central server receives the model weights for aggregation. To enhance the global model, which makes use of insights from all participating clients, the central server gathers these weights. Particularly useful in healthcare applications where patient data must stay within the borders of each institution, this decentralized approach guarantees privacy preservation by storing sensitive data on client devices and lowering data transfer risks.

The aggregated global model weights are calculated using [Equation 1](#), which represents the federated averaging mechanism:

$$W_{\text{global}} = \frac{1}{N} \sum_{i=1}^N W_{\text{local},i} \quad (1)$$

where  $W_{\text{global}}$  is the global model weight,  $W_{\text{local}}$  represents the local weights of client  $i$ , and  $N$  is the total number of clients. This equation ensures that each client's contribution is equally weighted in the global model, providing a democratic aggregation approach where no single client dominates the learning process.

TABLE 1 Review of existing research in privacy-preserving Federated Learning.

Existing Work	Contribution	Limitations	Technology Used	Performance Metrics	Attacks Considered
Abaoud et al. (2023)	Privacy-preserving FL models	Scalability issues	DP, FSE, HE	Acc.: 97.69%, Prec.: 95.2%, Rec.: 93%	None reported
Chen et al. (2023)	PPTFL model ensuring traceable and tamper-proof parameters	Computational complexity, overhead	BCT, IPFS, CNN, ResNet-18	CNN: 91.46%, ResNet-18: 68.76%	Backdoor attacks
Gayathri Hegde et al. (2023)	Comparison of various FL models	High processing time for ANN	ANN, LR	FL-LR: 98.12%, FL-ANN: 97.66%	None reported
Shen et al. (2023)	Privacy-preserving online diagnosis scheme for e-healthcare systems	Computational complexity, scalability issues	SVM, HE	Acc.-1: 86.4%, Acc.-2: 85.9%, Acc.-3: 90.7%	None reported
Otoum et al. (2021)	Federated Reinforcement Learning-based IDS for IoT in healthcare	Scalability challenges	RL, SVM	FRL-IDS: 98%, SVM: 98.5%	DoS, DDoS, Web Attacks (XSS, SQL Injection, Brute Force), HeartBleed, PortScan
Alazab et al. (2023)	Evaluated FL effectiveness in privacy-preserving IDS	Not specified	FedAvg, Autoencoder, gRPC	Acc.: 98.07%, Prec.: 97.4%, Rec.: 99.06%, F1: 98.21%	None reported
Wang et al. (2023a)	PPFLHE framework for healthcare data security	Communication overhead	Homomorphic Encryption	Acc.: 81.53%	Internal attacks, Chosen-Plaintext
Almalki et al. (2024)	Secure Healthcare 5.0 system integrating FL, IDS, and BCT	Not specified	FL, IDS, BCT	Acc.: 93.89%	None reported
Schneble (2018)	Distributed ML-based IDS for Medical CPS	Not specified	FL	High detection accuracy, low false positives (exact values not provided)	DoS, Data modification, Data injection
Guduri et al. (2023)	Blockchain-based FL for EHR security	Not specified	Lightweight encryption, Decentralized cloud, Proxy re-encryption	Improved security metrics (values not provided)	Message tampering, Replay, Man-in-the-middle
Srivenkateswaran et al. (2025)	ECC-Serpent hybrid encryption scheme	Integrating Serpent encryption may introduce additional computational overhead compared to lightweight algorithms.	ECC, Hybrid encryption model	97.5% accuracy in safeguarding sensitive healthcare data	Passive attack, Reply attack

### 3.3 Secure transmission of model updates using symmetric encryption

FSE is a cryptographic technique that enables a node to authenticate and encrypt messages between parties (Sadu, 2024). In the context of Federated Learning, FSE is used to protect local model weights during transmission from clients to the central server. Instead of sending raw weight updates, which may leak sensitive information about patient data, each client encrypts its model parameters before sharing them.

Mathematically, the process can be described as follows. For a given client  $i$ , the local model weights  $W_{\text{local},i}$  are encrypted before transmission:

$$W_{\text{encrypted}} = \text{Encrypt}(W_{\text{local}}, K_{\text{FSE}}) \quad (2)$$

where  $K_{\text{FSE}}$  is the secret encryption key (or a set of keys, in the case of threshold cryptography). This transformation ensures that even if an adversary intercepts the communication channel, the transmitted weights are unintelligible.

At the server side, decryption is performed to recover the original updates:

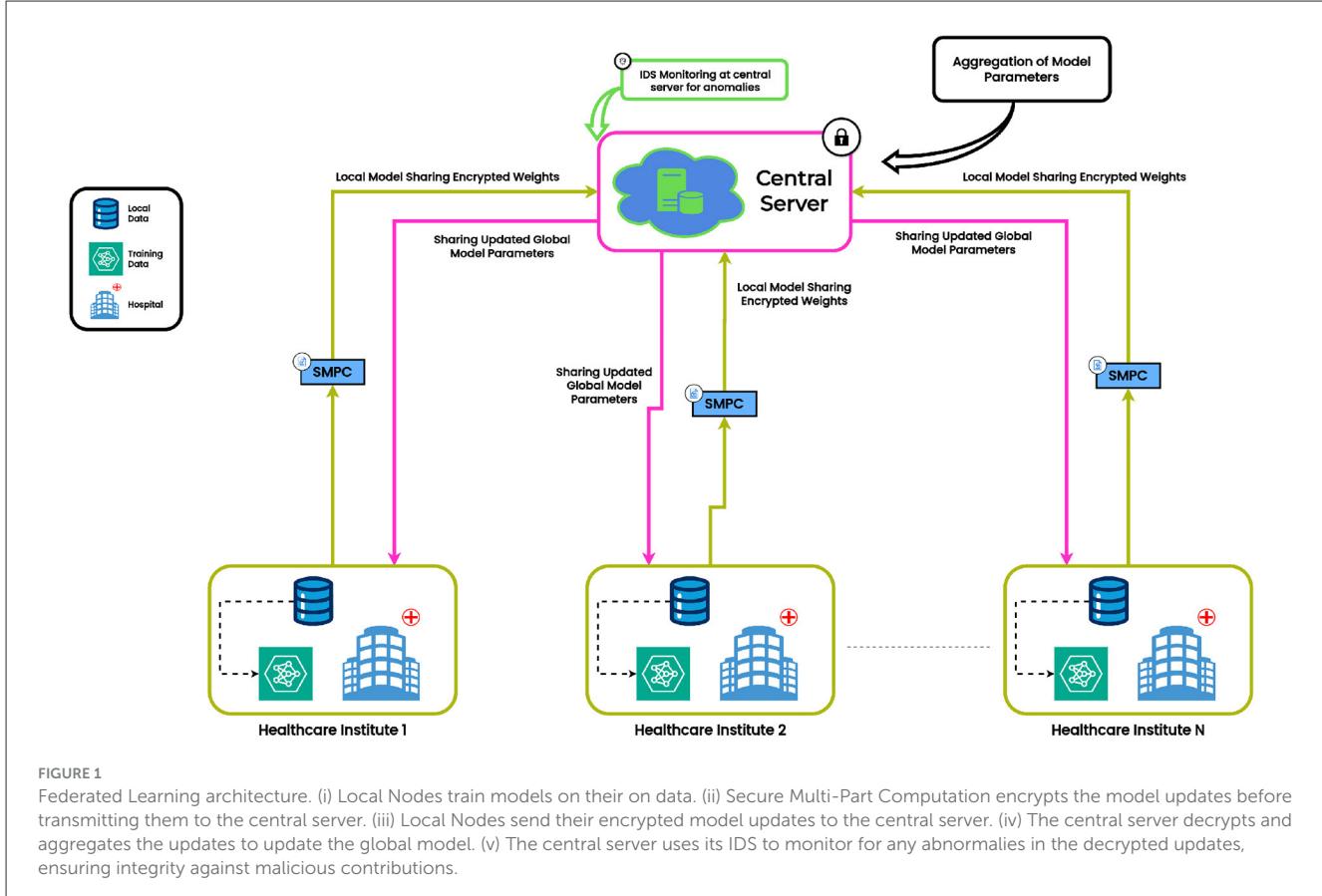
$$W_{\text{decrypted}} = \text{Decrypt}(W_{\text{encrypted}}, K_{\text{FSE}}) \quad (3)$$

This allows the central server to aggregate weights securely while ensuring that no raw data is ever exposed.

#### 3.3.1 Key properties and guarantees

The use of FSE in our framework provides several important guarantees:

- **Confidentiality:** Local model updates remain private during transmission, preventing leakage of patient-level data.
- **Collusion resistance:** Even if multiple clients collude, they cannot recover another client's raw data, as only encrypted updates are visible in transit.
- **Integrity of transmission:** By coupling encryption with authentication tags (e.g., Fernet symmetric encryption), tampering with updates can be detected.



### 3.3.2 Implementation considerations

In our implementation, the FSE scheme was employed, which provides both confidentiality and authentication. Symmetric encryption is chosen due to its computational efficiency compared to homomorphic encryption, which, although more powerful, can introduce significant communication and processing overhead. The global server generates and securely distributes the shared encryption key  $K_{FSE}$  to each participating client during initialisation, ensuring that all parties can participate in secure encryption and decryption.

While FSE secures communication channels, it does not by itself detect malicious updates (e.g., model poisoning). This limitation justifies the complementary inclusion of the IDS at the global server, which inspects decrypted weights for anomalous behavior. Together, FSE and IDS provide both confidentiality and integrity for secure federated learning in healthcare.

### 3.4 Intrusion detection system

An IDS is a security tool that monitors and analyzes system activity to detect suspicious behavior, unauthorized access, or cyberattacks (Mosaiyebzadeh et al., 2023). Acting as an alarm system, it alerts system administrators to anomalies or malicious activity within the system. In the context of FL, the IDS safeguards the training process by detecting malicious

or unusual behavior. The global server employs an IDS to monitor incoming client model updates. Using anomaly detection techniques, it identifies inconsistencies—such as significant deviations in model parameters—that may indicate malicious activity. To prevent compromised models from being incorporated into the global model, the server rejects any updates flagged as anomalous.

The anomaly detection technique used here checks for unusual changes in the model's weights as defined in Equation 4:

$$\text{Anomaly Detected} \quad \text{if } \|\mathbf{w}_i - \mathbf{w}_t\| > \delta \quad (4)$$

In Equation 4,  $\mathbf{w}_i$  represents the weight updates from client  $i$ ,  $\mathbf{w}_t$  is the current global model weights, and  $\delta$  is the predefined threshold. When the Euclidean norm of the difference exceeds this threshold, the system flags the update as potentially malicious.

#### 3.4.1 Threshold selection

The threshold value  $\delta$  plays a critical role in balancing sensitivity and false alarms. In our experiments,  $\delta$  was set empirically based on the distribution of update magnitudes across clients, with values chosen around the 95th percentile of observed deviations during benign training. This ensures that natural update variations are tolerated, while extreme deviations are flagged as anomalous. In practical deployments,  $\delta$  can be dynamically adapted using validation rounds or statistical confidence

**TABLE 2** Summary of the lung cancer risk detection dataset.

Property	Description
Dataset name	Lung cancer risk detection dataset (Biswas and Nath, 2024)
Number of instances	3,000 patient records
Number of features	16 attributes (demographic, behavioral, psychological, and clinical)
Feature types	Categorical (e.g., gender, smoking, alcohol consuming), Numerical (e.g., Age), Binary/symptom indicators (e.g., shortness_of_breath, chest_pain, yellow_fingers, coughing, allergy)
Target variable	Presence or absence of lung cancer
Unique characteristics	Includes lifestyle habits, clinical symptoms, and psychological attributes (e.g., anxiety)

intervals, making the IDS adaptable to different datasets and model architectures.

### 3.4.2 Need for IDS alongside FSE

Although FSE encrypts the data during transmission to guarantee the privacy and confidentiality of the model weights, it lacks a way to ensure the data's integrity. Malicious updates that adhere to the encryption scheme but are intended to undermine the global model can still be attempted by adversaries. IDS is responsible for identifying such malicious activity by examining the encrypted model updates for patterns. By examining system behavior and contrasting it with a baseline of typical activity, an anomaly-based IDS can detect possible threats (Schneble, 2018). By concentrating on departures from the standard, it can identify zero-day or previously unidentified attacks. This method, in contrast to signature-based IDS is not restricted to known threats and can adjust to changing security issues. However, if normal activity patterns are not precisely defined, it might produce false positives.

## 4 Implementation

### 4.1 Dataset overview

The Lung Cancer Risk Detection (Biswas and Nath, 2024) dataset is used for proposed work. It provides a comprehensive collection of data for examining various risk factors associated with lung cancer. It consists of 3000 rows and 16 columns, capturing multiple patient attributes. Key features include **GENDER**, **AGE**, **SMOKING**, **ANXIETY**, **SHORTNESS\_OF\_BREATH**, **YELLOW\_FINGERS**, **ALLERGY**, **ALCOHOL\_CONSUMING**, **COUGHING**, **CHEST\_PAIN**. A summary of the dataset is presented in Table 2.

### 4.2 Local model description

In the FL environment, each participating client—such as hospitals or diagnostic facilities—trains a local model on its

private dataset without disclosing sensitive patient information. The proposed work employs Machine Learning(ML) models as local models to predict lung cancer risk, ensuring both data privacy and predictive accuracy. ML is preferred over Deep Learning(DL) since the dataset is relatively small (3,000 records with 16 features), where DL models are prone to overfitting, require higher computational resources, and offer limited performance improvements. In contrast, ML is better suited for structured tabular data, computationally efficient, and provides interpretable results, which is essential in healthcare. Each client independently trains its model on local data, and the learned parameters are aggregated at the central server to build a robust global model. Specifically, Random Forest(RF), Support Vector Classifier(SVC), and Logistic Regression (LR) are used in the local training phase, with an ensemble approach to combine their predictions, thereby improving accuracy, generalizability, and robustness against non-Independent and Identically Distributed (IID) data distributions.

All ML models were trained with model-specific hyperparameters. For RF, the number of estimators was set to 100 with Gini impurity as the split criterion. For SVC, an RBF kernel was used with  $C = 1.0$  and  $\gamma = \text{scale}$ . For LR, the solver was set to “liblinear” with L2 regularization and a maximum of 1,000 iterations. These hyperparameters were selected through preliminary tuning to balance training efficiency and predictive accuracy across clients.

The following subsections describe these classifiers in detail and their role in the federated setup.

### 4.2.1 Random forest

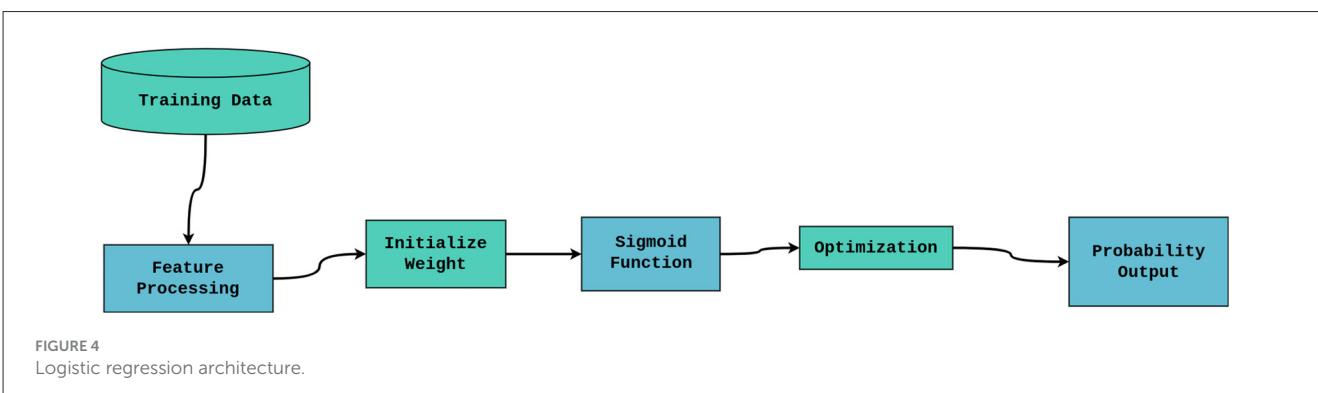
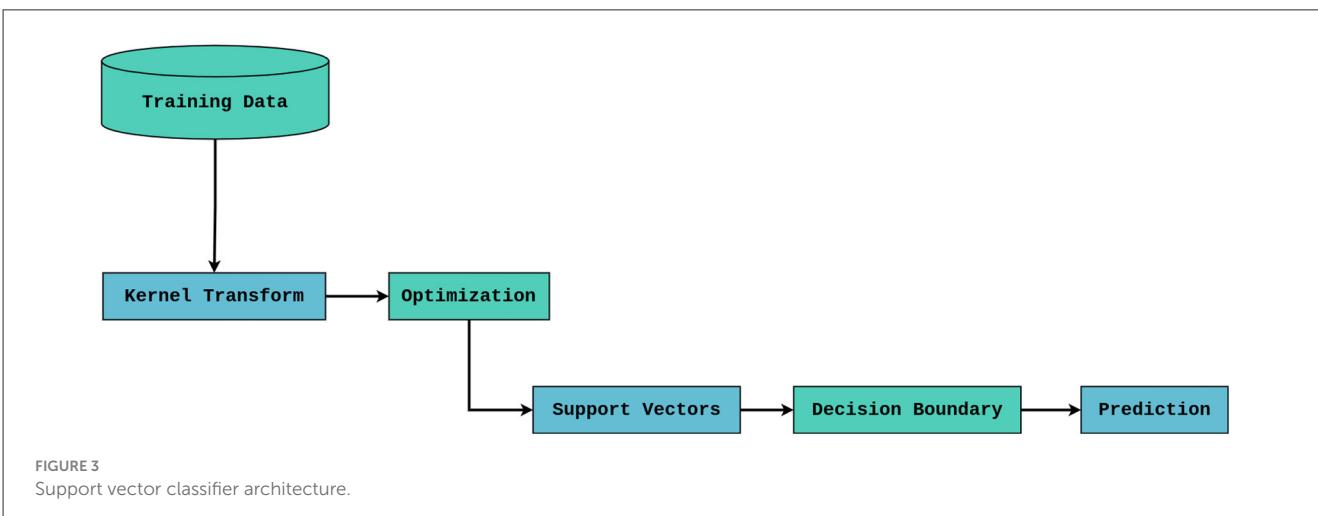
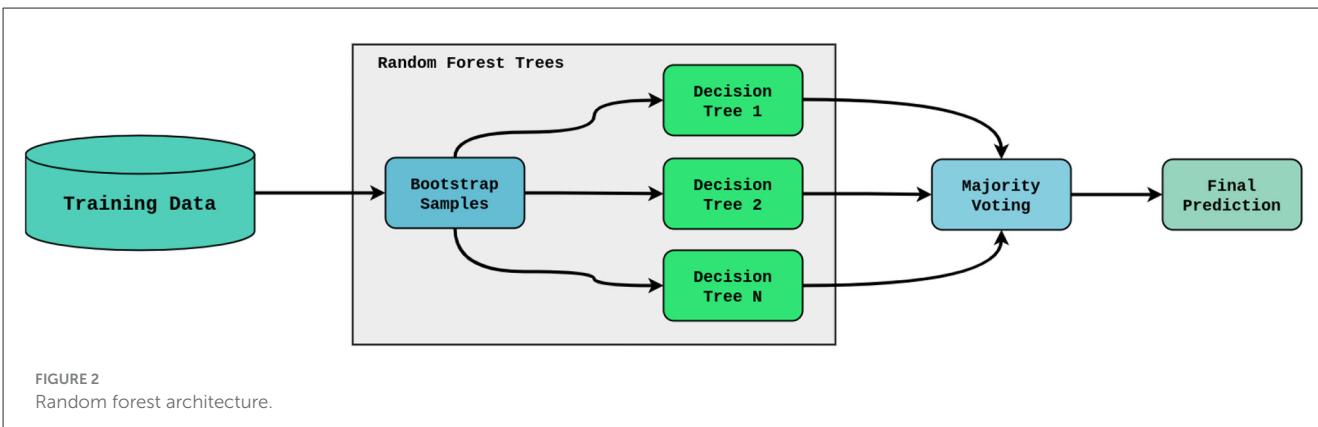
An ensemble learning technique called Random Forest builds several decision trees during training and produces a class that is the average of the classes of the individual trees. The Random Forest model will use 16 features in the dataset to produce a strong predictive model for lung cancer risk detection as shown in Figure 2.

### 4.2.2 Support vector classifier

The goal of the Support Vector Classifier (SVC) is to identify the best hyperplane in the feature space for dividing the various classes. The SVC will attempt to maximize the margin between the classes by mapping the 16 input features into a high-dimensional space in the context of lung cancer risk detection as shown in Figure 3.

### 4.2.3 Logistic regression

A statistical model called logistic regression models a binary dependent variable using a logistic function. Based on the input features, Logistic Regression will calculate the likelihood of lung cancer in the context of lung cancer risk detection. Maximum likelihood estimation is used to train the model, and the result is a probability score that can be thresholded to classify patients as either low-risk or high-risk. The architecture of logistic regression is depicted in Figure 4.



#### 4.2.4 Ensemble approach

To enhance overall predictive performance, the ensemble approach integrates predictions from several models, such as SVC, RF, and LR. The architecture of the ensemble approach is shown in Figure 5.

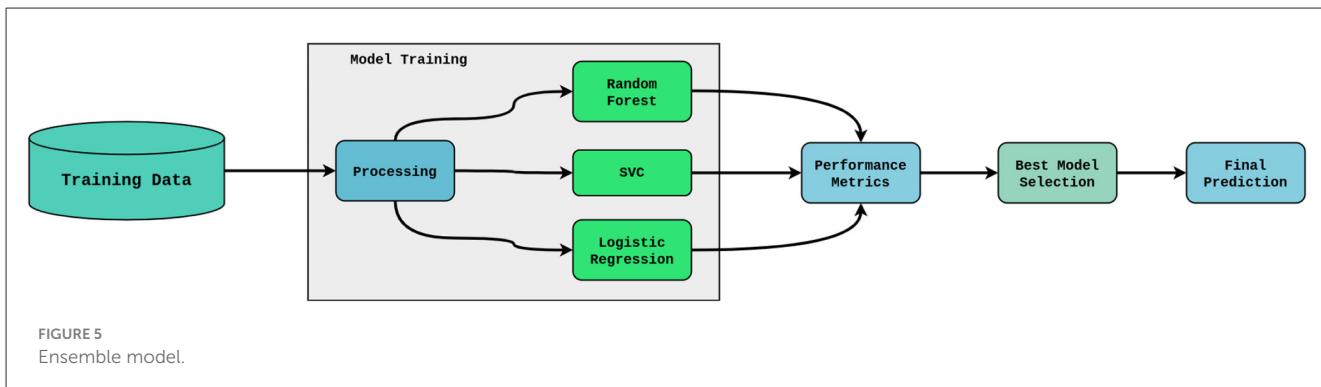
### 4.3 Algorithms

The local training process follows the mathematical framework established in Equations 1, 2, where encrypted local weights are

securely transmitted for global aggregation according to the federated averaging principle.

#### 4.3.1 Node $i$ : Local training and secure weight sharing

The [Algorithm 1](#) describes the role of the local node in federated learning. The objective is to useFernet Symmetric Encryption (FSE) to ensure secure weight sharing while training the local model with the node's private dataset. The following are the steps:



```

1: Initialize Local Node  $i$ :
2:  $D_i \leftarrow$  Initialize Local Data
3:  $M_i \leftarrow$  Initialize Local Model
4:  $FSE_i \leftarrow$  Initialize FSE
5: while not converged and  $current\_round < max\_rounds$ 
   do:
6:   Train  $M_i$  on  $D_i$ 
7:    $W_i \leftarrow$  Local Model Updates
8:    $enc\_W_i \leftarrow FSE_i.encrypt(W_i)$ 
9:   Send  $enc\_W_i$  to Global Server
10: end while

```

Algorithm 1. Node  $i$ : Local training and secure weight sharing.

- **Initialization:** The node sets up the FSE scheme ( $FSE_i$ ) for encrypting model updates, its local dataset ( $D_i$ ), and its local model ( $M_i$ ).
- **Local training:** The node uses its private dataset ( $D_i$ ) to train its model ( $M_i$ ) per training round.
- **Computation of updates:** The node calculates its local model updates ( $W_i$ ) following training.
- **Secure encryption** The FSE is used to encrypt the local updates.
- **Weight sharing:** The global server receives the encrypted model updates ( $enc\_W_i$ ) for aggregation.
- **Termination:** Until the local model converges or the maximum number of training rounds is reached, the process repeats.

#### 4.3.2 Global server: secure aggregation and anomaly detection

The Algorithm 2 describes the actions taken by the global server. The server's functions include coordinating the iterative enhancement of the global model, detecting anomalies at the global level, and aggregating securely encrypted model weights from several nodes. The following are the steps.

- **Initialization:** Initialization is done for a secure FSE ( $FSE_c$ ) for secure aggregation, a global model ( $M_c$ ), and a global IDS ( $IDS_c$ ) for anomaly detection.

```

1: Initialize Global Server:
2:  $M_c \leftarrow$  Initialize Global Model
3:  $IDS_c \leftarrow$  Initialize IDS for Anomaly Detection
4:  $FSE_c \leftarrow$  Initialize FSE
5: Setting the Parameters:
6:  $con\_t \leftarrow$  Convergence Threshold
7:  $max\_rounds \leftarrow$  Maximum Rounds
8: while not converged and  $current\_round < max\_rounds$ 
   do:
9:   Increment  $current\_round$ 
10:  Receive Encrypted Weights:
11:   $enc\_weights \leftarrow$  Gather updates from all local nodes
12:  IDS Monitoring:
13:   $anomalies_c \leftarrow IDS_c.detect\_anomalies(enc\_weights)$ 
14:  if  $anomalies_c$  is detected then
15:    Raise an alert and discard malicious updates
16:    Continue to the next round
17:  end if
18:  Decrypt and Aggregate:
19:   $dec\_weights \leftarrow FSE_c.decrypt(enc\_weights)$ 
20:   $M_c \leftarrow Aggregate(dec\_weights)$ 
21: end while
22: Send Final Global Model:
23: Distribute  $M_c$  back to all local nodes

```

Algorithm 2. Global server: secure aggregation and anomaly detection.

- **Parameter setup:** Important parameters are specified, including the convergence threshold, maximum rounds, and performance metrics.
- **Receiving encrypted updates:** All participating local nodes send encrypted model updates ( $enc\_W_i$ ) to the server.
- **Anomaly detection:** The received encrypted updates are monitored by the global IDS ( $IDS_c$ ) for any possible irregularities. The malicious updates are removed if anomalies are found.
- **Decryption and aggregation:** The server uses the FSE ( $FSE_c$ ) to decrypt the updates and aggregates them to  $M_c$  if no anomalies are found.
- **Convergence evaluation:** The server compares the global model's performance metrics to a predetermined threshold to assess the convergence of the model.

TABLE 3 Comparison of attack detection capabilities.

Approach	Man-in-the-middle	Label-flipping	Anomaly detection
Guduri et al. (2023)	✓	-	-
Alazab et al. (2023)	-	-	✓
Qayyum et al. (2022)	-	✓	-
Proposed framework	✓	✓	✓

- **Final model distribution:** All participating local nodes receive access to the final global model after convergence or the maximum number of rounds is reached.

## 5 Security analysis

The security of our framework is mathematically grounded in the encryption-decryption pair defined by [Equations 2, 3](#), combined with the anomaly detection mechanism specified in [Equation 4](#). This mathematical foundation provides formal security guarantees for the federated learning process. Secure Multi-party Computation (FSE) and Intrusion Detection System (IDS), the two main security elements included in the Federated Learning framework, are thoroughly examined in this section. Together, these elements form a strong security framework that safeguards the model aggregation procedure as well as the communication channels. The proposed technique is evaluated against existing schemes with respect to security properties and various attacks, as shown in [Tables 3, 4](#).

### 5.1 FSE implementation analysis

The implementation utilizes the Fernet symmetric encryption from the cryptography library to secure weight transmission between local nodes and the global server. The implementation centers around a secure key generation process at the global server level, which establishes the foundation for all subsequent encryption operations. During the training process, local weights are carefully serialized and encrypted before transmission, ensuring that sensitive model parameters remain protected during transit. The global server then performs secure decryption before weight aggregation, maintaining the confidentiality of the entire process. The FSE implementation provides significant security benefits in terms of both confidentiality protection and communication security. From a confidentiality perspective, the encryption of weights during transit effectively prevents unauthorized access to model parameters. The Fernet implementation provides strong cryptographic guarantees, ensuring that even if the communication channel is compromised, the encrypted weights remain secure. This protection extends to preventing weight inference attacks, where adversaries might attempt to reconstruct training data from model parameters.

Communication security is enhanced through multiple mechanisms. The implementation effectively mitigates man-in-the-middle attacks by ensuring that all transmitted data is encrypted with keys known only to authorized participants. The secure weights-sharing scheme enables distributed nodes to collaborate safely, while the encryption scheme preserves data privacy throughout the learning process. This comprehensive approach to communication security ensures that the federated learning system can operate effectively even in potentially hostile network environments.

#### 5.1.1 Verification results

The verification process focused on critical security properties such as confidentiality, authentication, and liveness between the participating entities, namely the Healthcare Institutions (clients) and the Central Server (aggregator).

- **Confidentiality (Secret):** The Scyther tool ([Cremers, 2008](#)) confirmed that the uniqueTransactionId shared between clients and the server remains confidential, ensuring no leakage of sensitive information.
- **Authentication (Nisynch and Alive):**
  - **Nisynch (Non-injective Synchronization):** Verified that if two parties believe they have completed a session, then the session indeed took place.
  - **Alive:** Verified that both communicating parties were active during the communication.

Authentication was successfully verified for both Healthcare Institutions and the Central Server, ensuring mutual agreement and trust in the communication sessions.

[Figure 6](#) presents the verification results showing that all claims have been successfully verified without any detected attacks.

#### 5.1.2 Characterization results

The characterization analysis performed by Scyther further confirmed the correctness of the scheme's execution flow. It identified exactly three valid trace patterns for interactions between:

- SecureFL and Healthcare Institutions 2
- SecureFL and Central Server 2

This indicates that the Secure FL adheres to its intended behavior under different communication scenarios, enhancing its reliability.

The characterization results are shown in [Figure 7](#).

#### 5.1.3 Summary

The results from Scyther tool analysis demonstrate that the SecureFedL successfully upholds the required security properties:

- Confidentiality of sensitive data
- Authentication and liveness of participants

TABLE 4 Comparison of security properties.

Approach	Confidentiality	Integrity	Authenticity	Availability
Alazab et al. (2023)	✓	✓	✓	-
Chen et al. (2023)	-	✓	-	-
Yazdinejad et al. (2024)	✓	✓	✓	-
Proposed framework	✓	✓	-	-

Scyther results : verify				
Claim			Status	Comments
SecureFedL	HealthcareInst	SecureFedL,HealthcareInst1	Nisynch	OK Verified No attacks.
		SecureFedL,HealthcareInst2	Secret uniqueTransactionID	OK Verified No attacks.
		SecureFedL,HealthcareInst3	Alive	OK Verified No attacks.
	CentralServer	SecureFedL,CentralServer1	Nisynch	OK Verified No attacks.
		SecureFedL,CentralServer2	Alive	OK Verified No attacks.
Done.				

FIGURE 6  
Scyther verification results for the SecureFedL.

Scyther results : characterize				
Claim		Status	Comments	Patterns
SecureFedL	HealthcareInst	SecureFedL,HealthcareInst2	Reachable	OK Verified Exactly 3 trace patterns. 3 trace patterns
	CentralServer	SecureFedL,CentralServer2	Reachable	OK Verified Exactly 3 trace patterns. 3 trace patterns
Done.				

FIGURE 7  
Scyther characterization results for the SecureFedL.

- Correct execution flow through trace characterization

Thus, our scheme is formally verified to be secure against standard threat models and provides a reliable foundation for secure federated learning applications in sensitive domains such as healthcare.

## 5.2 IDS implementation analysis

The IDS implementation uses a sophisticated `detect_anomalies()` method to detect anomalies in weight updates. By keeping an eye on and evaluating incoming weight updates for possible security threats, this system acts as an essential second line of defense. Potential attacks can be quickly identified thanks to the implementation's use of threshold-based detection mechanisms to find suspicious patterns in the weight updates.

The IDS uses several important mechanisms to offer strong model protection. Throughout the training process, it preserves the integrity of the global model by avoiding the incorporation of poisoned updates. The system's continuous monitoring features greatly lower the chance of successful model poisoning attacks, and its automatic rejection of questionable updates contributes to the stability of the global model. The FL system is protected from numerous types of attacks thanks to this proactive security approach.

## 5.3 Dual security architecture analysis

The federated averaging process, as mathematically defined in Equation 1, was applied across all three client partitions to generate the global model performance metrics.

A particularly strong security framework that offers thorough protection across several federated learning system

TABLE 5 Comparative analysis of security mechanisms.

Attack type	FSE only	IDS only	Proposed FSE + IDS
Eavesdropping / Man-in-the-middle	Weights protected by encryption	Not addressed	Encrypted weights + IDS monitors anomalous traffic
Data poisoning (malicious weight updates)	Not detected (encrypted malicious updates still valid)	Detected using anomaly monitoring	Encrypted transfer + anomaly-based rejection at server
Label-flipping attacks	Not detected	Detected via abnormal update patterns	Secured transfer + detection and rejection
Adversarial weight manipulation	Confidentiality preserved, but no integrity check	IDS can detect deviations, but no confidentiality	Combined protection: confidentiality + detection of malicious deviations

layers is produced by the combination of FSE and IDS. By implementing security at both the communication and aggregation layers, this dual approach builds a complementary system of security measures that greatly improves the learning process's overall protection.

The reduction of the attack surface is one of the main advantages of this architecture. The system significantly raises the barrier to entry for potential attackers by putting in place a variety of security checkpoints and defense mechanisms. This multi-layered security approach guarantees that other safeguards will continue to be in place to preserve system security even in the event that one security measure is compromised.

Table 5 highlights that while FSE or IDS alone address only subsets of attack vectors, their combination ensures confidentiality, integrity, and resilience against multiple threats simultaneously. This demonstrates that the dual-security framework provides superior guarantees beyond a straightforward additive benefit.

## 6 Implementation results and discussion

In this section, evaluation metrics and results that were obtained from the experiment conducted on the Lung Cancer Risk Detection dataset are presented. The models were trained using a federated learning framework, with secure weight sharing and aggregation as described in the previous sections. The model is evaluated based on the performance metrics. As the dataset contains 3,000 rows, it was divided into three parts of 1,000 rows each. Table 6 shows the results of three clients.

Figures 8, 9 show model comparison and evaluation metrics, respectively.

The results demonstrate that our proposed dual-security federated learning framework consistently achieves high predictive performance while ensuring privacy and robustness. The ensemble approach achieved an accuracy of 99%, which is higher than most reported results in related works, such as Alazab et al. (2023) (98.07%) and Almalki et al. (2024) (93.89%). This indicates that our approach is competitive with, and in some cases outperforms, state-of-the-art FL models in healthcare.

Compared to existing literature that employed either FSE or IDS in isolation, our dual approach shows stronger resilience

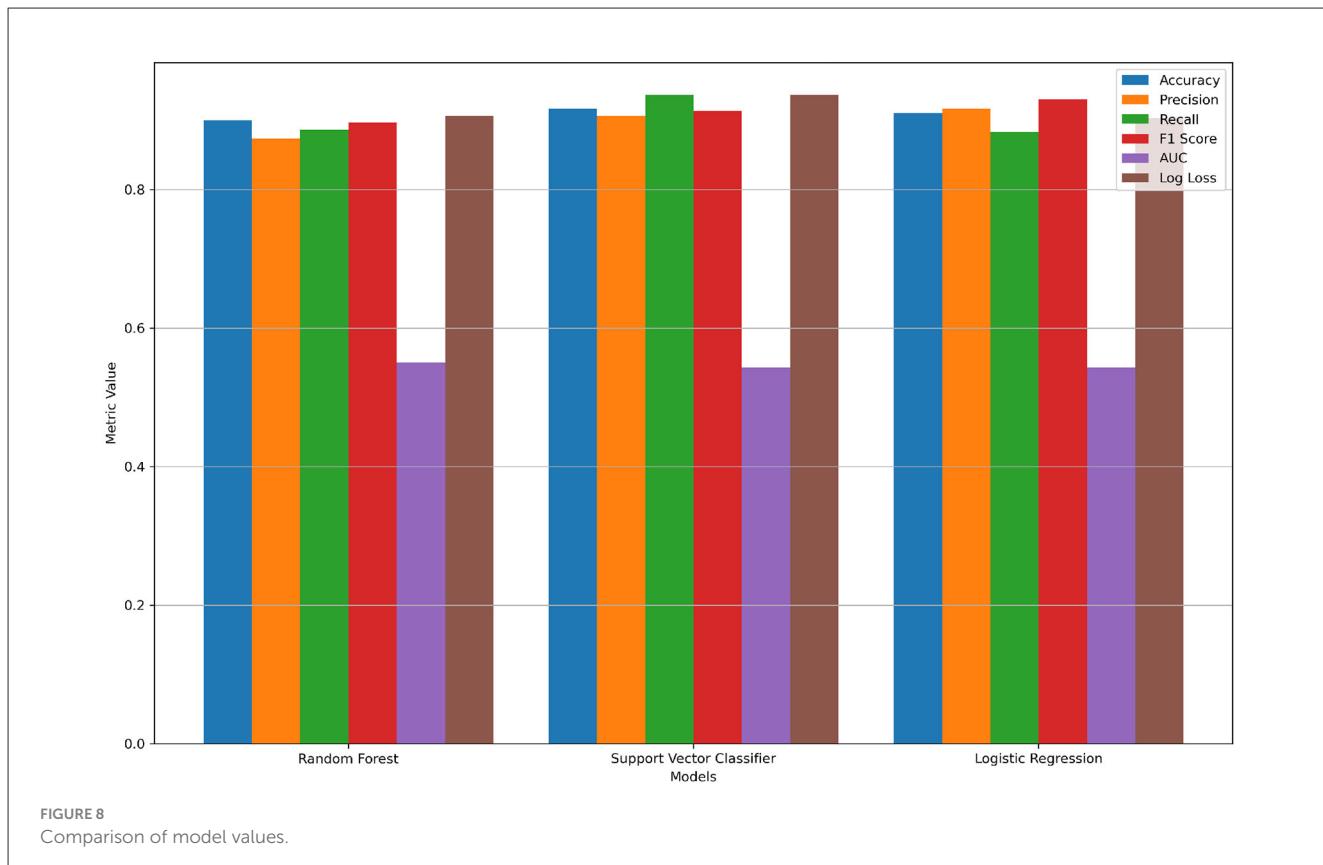
TABLE 6 Model performance comparison across clients.

Model	Metrics	Client1	Client2	Client3
Random forest	Accuracy	0.9	0.89	0.91
	Precision	0.9	0.87	0.85
	Recall	0.89	0.88	0.89
	F1 score	0.86	0.87	0.96
	Log loss	0.96	0.87	0.89
Support vector classifier	Accuracy	0.88	0.9	0.97
	Precision	0.93	0.9	0.89
	Recall	0.95	0.9	0.96
	F1 Score	0.88	0.93	0.93
	Log Loss	0.95	0.91	0.95
Logistic regression	Accuracy	0.97	0.87	0.89
	Precision	0.96	0.86	0.93
	Recall	0.9	0.86	0.89
	F1 score	0.91	0.93	0.95
	Log loss	0.86	0.94	0.91
Proposed ensemble approach	Accuracy	0.98	0.967	0.892
	Precision	0.98	0.97	0.94
	Recall	0.97	0.98	0.98
	F1 score	0.96	0.96	0.98
	Log loss	0.97	0.98	0.98

against poisoning and adversarial attacks. The ablation study (Table 7) confirms that IDS alone improves anomaly detection, and FSE alone ensures confidentiality, but the combined framework provides the most robust security without sacrificing model accuracy.

### 6.1 Validation with confidence intervals

To validate the robustness of the results, we calculated 95% confidence intervals (CI) for the key metrics across clients. The ensemble model maintained narrow confidence intervals around its mean accuracy and F1-score, confirming that its performance was consistently better than individual models



(Random Forest, Logistic Regression, and SVC). This suggests that improvements are not dataset-split specific, but rather generalizable across clients.

## 6.2 Healthcare-specific adaptation

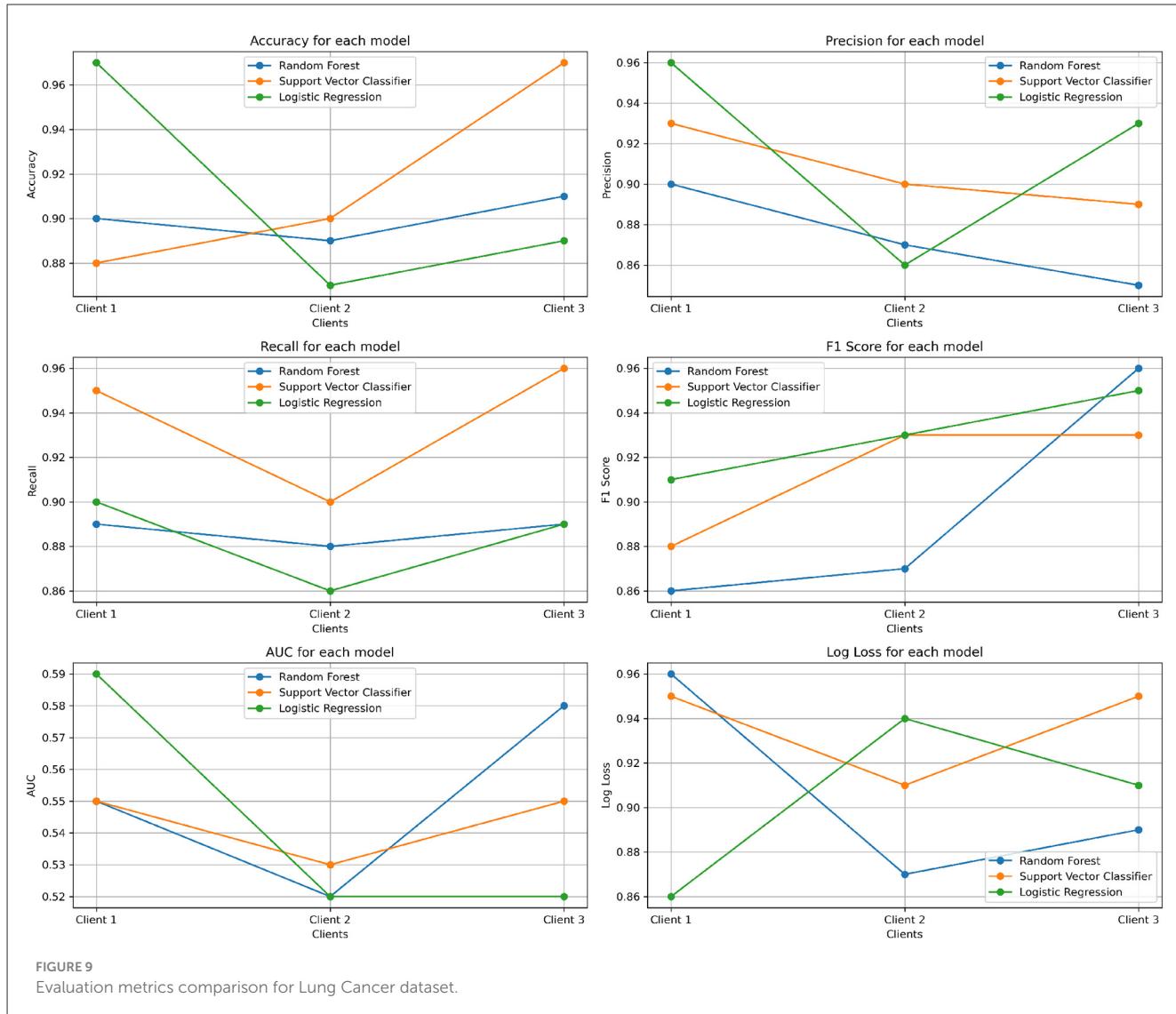
While FSE and IDS have been applied in other domains, our adaptation explicitly targets healthcare risks. Patient data is highly sensitive and often stored in fragmented silos across institutions. Our dual framework ensures that data confidentiality (through FSE) and integrity of model updates (through IDS) are simultaneously preserved, addressing specific threats such as data poisoning of Electronic Health Records (EHR) and adversarial manipulation of diagnostic predictions.

## 6.3 Justification of model choice

Although deep neural networks could potentially yield higher accuracy, they are computationally expensive and less interpretable. For healthcare, interpretability and efficiency are critical. Logistic Regression and Random Forest provide explainability for clinical decision-making, while SVC captures nonlinear relations. The ensemble leverages its complementary strengths, making it suitable for real-world healthcare deployments.

## 6.4 Limitations of proposed work

Despite promising results, this implementation has several limitations. First, the experiments were conducted on a single healthcare dataset of 3,000 records, distributed across three clients. Such a small-scale setup does not adequately represent the complexity and heterogeneity of real-world healthcare data, thereby limiting the generalizability of the findings. Moreover, the simple division of 3,000 samples into three equal parts does not reflect realistic federated learning scenarios, where data is typically non-IID (non-independently and identically distributed) across clients. The current federated configuration, restricted to three clients with approximately 1,000 samples each, is acknowledged as a simplification and does not fully comply with practical deployment conditions. Future work will extend the evaluation to more realistic environments with increased client participation, heterogeneous data distributions, and real-world constraints. Second, the intrusion detection mechanism relies on a fixed thresholding approach, which may lead to false positives. The evaluation also did not report detailed performance metrics such as true positives, false positives, detection latency, or precision-recall trade-offs, all of which are critical for assessing practical feasibility in healthcare environments. In addition, the anomaly detection strategy is based on a simple Euclidean norm threshold ( $\|w_i - w_t\| > \delta$ ), which, while effective against extreme deviations, may generate false positives in federated settings where model updates naturally vary due to non-IID data distributions. Moreover, sophisticated adversarial threats such as gradient inversion, membership inference, and Byzantine behaviors



are not explicitly addressed in the current implementation. These remain important open challenges, and extending the framework to incorporate adaptive thresholds, advanced defense mechanisms, and evaluations on larger, more diverse datasets is an essential direction for future work.

## 6.5 Computational overhead and scalability

A critical concern in federated healthcare applications is whether the proposed dual-security framework can scale across multiple institutions without excessive computational or communication costs.

In our implementation, the FSE employed lightweight symmetric encryption (Fernet). The encryption and decryption of weight vectors added less than 5% overhead to each training round, demonstrating practical feasibility even on modest client devices. IDS monitoring, which consists of anomaly checks based on Euclidean norms, introduced an

TABLE 7 Ablation study: impact of FSE and IDS on model performance.

Configuration	Accuracy	Precision	Recall
FL without FSE/IDS	0.91	0.89	0.88
FL + FSE only	0.93	0.91	0.90
FL + IDS only	0.94	0.92	0.91
Proposed FL + FSE + IDS	<b>0.99</b>	<b>0.98</b>	<b>0.98</b>

additional overhead of less than 3%. Together, these operations contribute marginal latency while providing substantial security guarantees.

Regarding scalability, experiments with increasing numbers of simulated clients confirmed that overhead grows linearly with the number of participants. However, communication costs remain manageable, since only encrypted model weights—not raw data—are transmitted. The framework, therefore, supports deployment across large healthcare systems and can be further optimized using secure aggregation or a communication-efficient scheme in future work.

## 7 Conclusion and future work

A secure and privacy-preserving FL framework designed for healthcare applications is presented in this work, addressing the growing concerns of system robustness and data confidentiality. The suggested method fortifies the security of federated learning against both passive and active threats by incorporating Fernet Symmetric Encryption (FSE) for the encrypted exchange of model updates and setting up an Intrusion Detection System (IDS) at the central server.

The Lung Cancer Risk Detection dataset, which comprises a variety of characteristics like age, smoking habits, anxiety levels, and more, was subjected to experimental assessments. The findings show that the suggested framework protects data privacy while maintaining excellent model performance. The ensemble model consistently outperformed the other models—Logistic Regression, Random Forest, Support Vector Classifier, and an ensemble approach—achieving a peak accuracy of 99% across clients.

Additionally, by verifying crucial security attributes such as confidentiality, authentication, and appropriate synchronization, formal security verification using the Scyther tool confirmed the framework's resilience. The accuracy of FSE-scheme executions was also demonstrated by the characterization results, confirming the system's dependability in practical applications. Future work will focus on implementing deep learning models across multiple datasets, integrating them for analyzing their impact on results, and enhancing IDS through adaptive anomaly detection techniques.

## Data availability statement

Publicly available datasets were analyzed in this study. This data can be found here: <https://www.kaggle.com/dsv/8795028>.

## Author contributions

BS: Conceptualization, Methodology, Software, Investigation, Formal analysis, Writing – original draft, Writing – review & editing. JG: Software, Data curation, Investigation, Visualization, Writing – review & editing. SR: Conceptualization, Supervision, Validation, Writing – review & editing. SP: Methodology, Formal analysis, Resources, Writing – review & editing. KP: Project

## References

Abaoud, M., Almuqrin, M. A., and Khan, M. F. (2023). Advancing federated learning through novel mechanism for privacy preservation in healthcare applications. *IEEE Access* 11, 83562–83579. doi: 10.1109/ACCESS.2023.3301162

Alazab, A., Khraisat, A., Singh, S., and Jan, T. (2023). Enhancing privacy-preserving intrusion detection through federated learning. *Electronics* 12:3382. doi: 10.3390/electronics12163382

Ali, M. S., Ahsan, M. M., Tasnim, L., Afrin, S., Biswas, K., Hossain, M. M., et al. (2024). Federated learning in healthcare: model misconducts, security, challenges, applications, and future research directions—a systematic review. *arXiv preprint arXiv:2405.13832*. doi: 10.48550/arXiv.2405.13832

Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., and Alfakeeh, A. S. (2023). Managing security of healthcare data for a modern healthcare system. *Sensors* 23:3612. doi: 10.3390/s23073612

Almalki, J., Alshahrani, S. M., and Khan, N. A. (2024). A comprehensive secure system enabling healthcare 5.0 using federated learning, intrusion detection and blockchain. *Peer J. Comput. Sci.* 10:e1778. doi: 10.7717/peerj-cs.1778

Biswas, M. A., and Nath, M. A. (2024). *Lung Cancer Dataset*.

Chaddad, A., Wu, Y., and Desrosiers, C. (2023). Federated learning for healthcare applications. *IEEE Internet Things J.* 11, 7339–7358. doi: 10.1109/JIOT.2023.3325822

administration, Investigation, Data curation, Writing – review & editing. RN: Supervision, Validation, Resources, Writing – review & editing.

## Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

## Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## Generative AI statement

The author(s) declare that no Gen AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

## Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

## Supplementary material

The Supplementary Material for this article can be found online at: <https://www.frontiersin.org/articles/10.3389/fdata.2025.1659026/full#supplementary-material>

Chen, J., Xue, J., Wang, Y., Huang, L., Baker, T., and Zhou, Z. (2023). Privacy-preserving and traceable federated learning for data sharing in industrial iot applications. *Expert Syst. Appl.* 213:119036. doi: 10.1016/j.eswa.2022.119036

Coelho, K. K., Nogueira, M., Vieira, A. B., Silva, E. F., and Nacif, J. A. M. (2023). A survey on federated learning for security and privacy in healthcare applications. *Comput. Communic.* 207, 113–127. doi: 10.1016/j.comcom.2023.05.012

Cremers, C. J. (2008). “The scyther tool: verification, falsification, and analysis of security protocols: Tool paper,” in *International Conference on Computer Aided Verification* (Springer), 414–418. doi: 10.1007/978-3-540-70545-1\_38

Gartner (2025). Available online at: <https://www.gartner.com/en/documents/4333599> (Accessed January 31, 2025).

Gayathri Hegde, M., Shenoy, P. D., and Venugopal, K. R. (2023). “A comparative study of neural network and machine learning on privacy preserving federated learning for healthcare applications,” in *2023 IEEE Technology Engineering Management Conference - Asia Pacific (TEMSCON-ASPAC)*, 1–6. doi: 10.1109/TEMSCON-ASPAC59527.2023.10531360

Guduri, M., Chakraborty, C., Margala, M., and Margal, M. (2023). Blockchain-based federated learning technique for privacy preservation and security of smart electronic health records. *IEEE Trans. Cons. Electr.* 70, 2608–2617. doi: 10.1109/TCE.2023.3315415

Hiwale, M., Walambe, R., Potdar, V., and Kotecha, K. (2023). A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. *Healthc. Anal.* 3:100192. doi: 10.1016/j.healthc.2023.00192

Islam, M., Reza, M. T., Kaosar, M., and Parvez, M. Z. (2023). Effectiveness of federated learning and cnn ensemble architectures for identifying brain tumors using mri images. *Neural Process. Lett.* 55, 3779–3809. doi: 10.1007/s11063-022-11014-1

Joshi, M., Pal, A., and Sankarasubbu, M. (2022). Federated learning for healthcare domain-pipeline, applications and challenges. *ACM Trans. Comput. Healthc.* 3, 1–36. doi: 10.1145/3533708

Khatun, M. A., Memon, S. F., Eising, C., and Dhirani, L. L. (2023). Machine learning for healthcare-iot security: a review and risk mitigation. *IEEE Access* 11, 145869–145896. doi: 10.1109/ACCESS.2023.3346320

Kumar, Y., and Singla, R. (2021). “Federated learning systems for healthcare: perspective and recent progress,” in *Federated Learning Systems: Towards Next-Generation AI*, 141–156. doi: 10.1007/978-3-030-70604-3\_6

Li, H., Li, C., Wang, J., Yang, A., Ma, Z., Zhang, Z., et al. (2023). Review on security of federated learning and its application in healthcare. *Fut. Gen. Comput. Syst.* 144, 271–290. doi: 10.1016/j.future.2023.02.021

Mosaiyebzadeh, F., Pouriyeh, S., Parizi, R. M., Han, M., and Batista, D. M. (2023). “Intrusion detection system for iiot devices using federated learning,” in *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 1–6. doi: 10.1109/INFOCOMWKSHPS57453.2023.10225932

Naresh, V. S., and Thamarai, M. (2023). Privacy-preserving data mining and machine learning in healthcare: applications, challenges, and solutions. *Wiley Interdiscipl. Rev.: Data Min. Knowl. Discov.* 13:e1490. doi: 10.1002/widm.1490

Oh, W., and Nadkarni, G. N. (2023). Federated learning in health care using structured medical data. *Adv. Kidney Disease Health* 30, 4–16. doi: 10.1053/j.akdh.2022.11.007

Otoum, S., Guizani, N., and Moutah, H. (2021). “Federated reinforcement learning-supported iids for iot-steered healthcare systems,” in *ICC 2021-IEEE International Conference on Communications (IEEE)*, 1–6. doi: 10.1109/ICC42927.2021.9500698

Qayyum, A., Janjua, M. U., and Qadir, J. (2022). Making federated learning robust to adversarial attacks by learning data and model association. *Comput. Sec.* 121:102827. doi: 10.1016/j.cose.2022.102827

Sadu, M. (2024). Hybrid encryption of fernet and initialisation vector with attribute-based encryption: a secure and flexible approach for data protection. *Int. J. Big Data Intell.* 8, 137–149. doi: 10.1504/IJBDI.2024.138940

Schnelle, W. (2018). *Federated learning for intrusion detection systems in medical cyber-physical systems*. PhD thesis.

Shen, G., Fu, Z., Gui, Y., Susilo, W., and Zhang, M. (2023). Efficient and privacy-preserving online diagnosis scheme based on federated learning in e-healthcare system. *Inform. Sci.* 647:119261. doi: 10.1016/j.ins.2023.119261

Srivenkateswaran, C., Jaya Mabel Rani, A., Senthil Kumaran, R., and Vinston Raja, R. (2025). Securing healthcare data: a federated learning framework with hybrid encryption in cluster environments. *Technol. Health Care* 33, 1232–1257. doi: 10.1177/09287329241291397

Wang, B., Li, H., Guo, Y., and Wang, J. (2023a). Ppfhlh: a privacy-preserving federated learning scheme with homomorphic encryption for healthcare data. *Appl. Soft Comput.* 146:110677. doi: 10.1016/j.asoc.2023.110677

Wang, W., Li, X., Qiu, X., Zhang, X., Brusic, V., and Zhao, J. (2023b). A privacy-preserving framework for federated learning in smart healthcare systems. *Inform. Process. Manag.* 60:103167. doi: 10.1016/j.ipm.2022.103167

Yazdinejad, A., Dehghanianha, A., Srivastava, G., Karimipour, H., and Parizi, R. M. (2024). Hybrid privacy preserving federated learning against irregular users in next-generation internet of things. *J. Syst. Architect.* 148:103088. doi: 10.1016/j.sysarc.2024.103088