

A Federated Siamese-Autoencoder Framework For Robust ECG-Based Biometric Authentication With Spoof Attack Detection

S. Kasinathan¹, C. Ananth^{*2} and N. Mohananthini³

¹Research Scholar, Department of Computer and Information Science, Annamalai University, Annamalai Nagar, Tamilnadu, India.

²Assistant Professor/Programmer, Department of Computer and Information Science, Annamalai University, Annamalai Nagar, Tamilnadu, India.

³Associate Professor, Department of Electrical and Electronics Engineering, Muthayammal Engineering College (Autonomous), Rasipuram, Tamilnadu, India.

*Corresponding Author: C. Ananth

Abstract

User authentication based on electrocardiogram (ECG) data has emerged as a convincing modality for continuous and unobtrusive biometric-based user authentication leveraging the liveness property and physiologically unique characteristics of ECG. Unfortunately, spoofing attacks make it a non-trivial problem in practice and thus will be a main target for research given their implications on data privacy. This study presents a unique two-stage deep learning framework that combines federated metric learning with reconstruction-based anomaly detection to provide secure ECG authentication. The first one is using a federated Siamese neural network to learn discriminative embedding on scattered clients without transmitting raw data, which protects the user but improves the generalization. The model employ triplet-based optimization to ensure high inter-subject separability and intra-subject compactness in the embedding space. The second stage involves training an autoencoder on only clean original ECG features for the purpose of creating a model of healthy physiological activity; spoofed or manipulated signals can then be identified by analysis of a reconstruction error. The proposed framework analyzes multi-domain ECG features derived from time, frequency, heart rate variability and wavelet domains to fully characterize cardiac signals. Experimental results show that the model is capable of achieving high authentication accuracy with low equal error rate and effectively discriminate between spoofed inputs under diverse attack situations. The combination of federated learning and reconstruction-based spoof detection leads to a scalable, privacy-presumably secure, and resilient approach for future biometric authentication systems.

Keywords: ECG Biometrics, Federated Learning, Siamese Neural Network, Metric Learning, Spoof Detection, Autoencoder, Biometric Authentication, Deep Learning.

1. Introduction

Biometric authentication is seen as one of the essential parts in modern security systems, specifically in healthcare and IoT or wearables where constant identity authentication is vital while not interrupting a user. While the well-known biometric modalities like fingerprints, face and iris recognition are widely used, they become increasingly prone to several weaknesses regarding spoof attacks, replay threats and privacy issues. In contrast, physiological signals (in particular electrocardiogram (ECG)) have garnered considerable focus as they exhibit intrinsic liveness, individuality, and resistance to forgery. The electrical activity of the human heart which ECG signals represent is unique and hard to reproduce, thus providing a promising solution for secure authentication systems [1], [2]. Proposed enhancements: Deep learning based biometric systems for ECG. Specifically, Siamese neural networks (SNNs) have been extensively studied for learning discriminative representations and assessing similarity between the ECG signals. These models allow the verification even using scarce training samples and prove to generalize well across users [1], [3]. In addition, deep learning-based methods have achieved high authentication accuracy by automatically deriving reliable features from ECG signals,

thereby eliminating the limitations of manual feature engineering [4]. Emerging paradigms like self-supervised and contrastive learning build on this notion of scalability by mitigating a need for labeled training data while increasing performance in previously unseen domains [2].

These advances notwithstanding, multiple challenges remain unaddressed. A major challenge is the susceptibility of biometric systems to spoofing and signal manipulation attacks. In recent studies, it has been found that ECG signals can be compromised or generated artificially to mimic genuine users [5], thus posing a serious risk to the reliability of the system. In addition, most of the current authentication frameworks mainly put emphasis on classification accuracy rather than security audit including spoofing detection and anomaly comparison. This disparity illustrates the importance of unified frameworks that both verify users and ensure resilience to adversarial and spoofing attacks. ECG-based authentication also faces a huge challenge with respect to data privacy. Such centralized training approaches require aggregation of sensitive physiological data, presenting ethical and regulatory challenges [6]. Federated Learning has been proposed as a potential solution to this challenge, by allowing the training of models across multiple devices without sharing raw data. Recent research shows that federated learning can achieve privacy protection and excellent authentication performance in distributed settings [6]. Moreover, autoencoder-based models have remained that are having been employed for anomaly detection on ECG signals, making use of reconstruction error to differ between proper and faulty inputs [7]. These approaches offer a built-in detection mechanism for spoofed or manipulated signals. Moreover, adding multi-domain feature representation, including time-domain (TD), frequency domain (FD), heart rate variability (HRV), and wavelet features in the generalized approach led to a more robust characterization of complex ECG signals. This exhaustive feature extraction improves inter-person discrimination while facilitating noise resilience and signal dynamics to the system [4], [8]. Nonetheless, despite being widely used in some specific scenarios, the joint application of federated metric learning and reconstruction-based spoof detection within a single framework remains unexplored in the entirety of literature.

To overcome these limitations, this paper presents a novel dual-stage deep learning framework, “A Federated Siamese–Autoencoder Framework for Robust ECG-Based Biometric Authentication with Spoof Attack Detection (FedSiam-AE)”, that combines federated Siamese learning for privacy-preserving authentication with autoencoder-based reconstruction analysis for spoof attack detection. Specifically, the suggested FedSiam-AE employs distributed training to support scalability and privacy of data, as well as the use of anomaly detection mechanisms to create better resistance against spoofing attacks. The proposed framework integrates deep metric learning with the use of reconstruction-based validation to achieve a secure, scalable and practical solution for next-generation ECG biometric systems.

2. Literature Review

Zhang et al. Utilizing temporal and morphological features of ECG signals for strong identity verification, [9] proposed a deep convolutional neural net (CNN) based ECG biometric authorization system. The authors propose the method of adaptive feature learning for intra-subject variability for multiple datasets which shows improvement in authentication accuracy for ECG based biometric systems. Prakash et al. [10] presented a CNN–LSTM lightweight ECG authentication system (BAED) which conducts feature extraction and classification in one architecture. The model also simplifies computational

complexity and mobile deployment, without sacrificing recognition performance. Wang et al. [11] proposed an ECG biometric recognition framework based on adaptive feature pooling allowing the system to adapt to different lengths of heartbeat signals without re-training. The method exhibited significant generalizability across data sets and further increased robustness to changing physiological conditions. Lonbar et al. [12] proposed an ECG authentication system based on deep learning that encodes the original ECG signals into time–frequency domain representations via Wigner–Ville distribution. It uses convolutional neural networks to classify the extracted features, which leads significantly improved accuracy and noise resistance. Choi et al. In [13], multi-stream convolutional neural networks were used to authenticate users based on ECG and EMG signals. This leads to improved recognition accuracy as well as robustness in practical situations e.g., driving scenarios by fusing various physiological signals.

López et al. [14] proposed a deep learning based ECG identification framework with demographic-aware modeling— the model is assisted by some auxiliary attributes such as gender during classification process. Such a simplified feature space is also very efficient with regard to large populations. Al Alfi et al. [15]: the proposed ECG authentication system using GCN method, where mutual information features based on multi-lead ECG are used. This enables the model to reflect spatial and statistical dependencies, results in policy higher recognition performance and robustness. Li et al. A study conducted by [16] focuses on the overall security of biometric systems that use physiological signals and addresses vulnerability to replay attacks and spoofing. The study highlighted the need for incorporating anti-spoofing strategies along with standardized evaluation metrics like FAR and FRR. In the work of Pan and Kim [17], a fake ECG signal generation method based on GAN was proposed for ECG biometrics spoofing detection. This research Leverage frequency-domain artefact and utilising Siamese networks can successfully classify genuine signal or spoofed signal. Garg et al. [18] attack on adversarial ECG biometric systems with GAN-based signal generation. This shows that attackers could reconstruct ECG template to fake users, thus is in urgent need of other defense achieve.

Abdullahi et al. [19] studied template-level attacks and protection mechanisms in biometric systems (including ECG biometrics). The study outlines various types of attack scenarios and stresses the importance for secure template storage as well as transformation techniques to alleviate those vulnerabilities. Wang et al. [20] introduced a continuous authentication framework based on physiological signals, highlighting the intrinsic liveness detection capability of ECG signals. The field study showed better robustness against spoof attacks than behavioral biometrics. Gimba et al. [21] proposed a system for multimodal biometric authentication, which combined ECG signals with other modalities to make it more resilient against spoofing attacks. Fusion-based methods are more robust in the presence of noise and adversaries. Aguilar et al. [22] then described physiological signal-based authentication systems and discussed the issues in spoofing, replay attacks, as well as dataset limitations. The study underlined the lack of specific evaluation protocols and strong security mechanisms. Singh et al. #38, and Zang et al. [23] focusing on anti-spoofing methods in any biometric systems, highlight the limitations of existing deep learning models for unseen attacks application in their experimental studies. Generalizable and explainable spoof detection mechanisms are needed, the study said.

Though there have been substantial advances made in ECG-based biometric authentication, the current literature suffers from a number of key concerns that limit

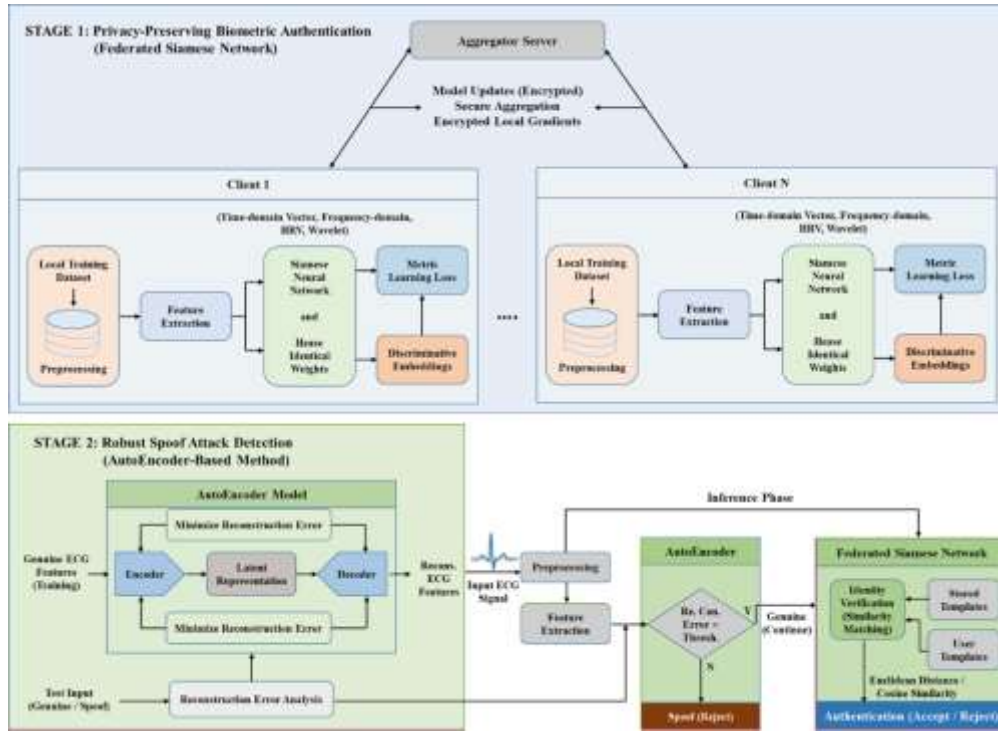
practical implementation of this technique in realistic settings. Most studies concentrate only on deep learning architectures to enhance classification accuracy, receiving less attention with respect to security attack countermeasures such as spoofing and adversarial signal manipulation. While some papers have presented methods for spoof detection, they are typically treated as an auxiliary module rather than tightly integrated with the authentication pipeline. Moreover, current solutions are based on centralized training methods, leading to privacy and scalability issues in distributed healthcare scenarios involving internet of things (IoT) networks. This leaves a significant research opportunity in this space as there are no common framework ensuring privacy preservation, strong authenticated user and spoof detection at the same time.

These issues motivated the need for a more comprehensive ECG-based biometric system which can be deployed under real-world constraints while protecting sensitive physiological information. At the same time, this study can also improve the reliability and democracy of the system by integrating privacy protection learning paradigms with robust anti-spoofing mechanisms. To that all end, this paper presents a novel dual-stage framework that integrates federated metric learning and reconstruction-based anomaly detection to facilitate secure authentication against repeated voice attacks in the same network; thus providing spoof identification capability into an integrated setup. Section 3 presents the detailed design and implementation of the proposed framework, including feature extraction, federated Siamese learning, and autoencoder-based spoof detection.

3. Proposed Methodology

This study, “A Federated Siamese-Autoencoder Framework for Robust ECG-Based Biometric Authentication with Spoof Attack Detection (FedSiam-AE)” proposes a novel dual-stage deep learning framework to securely and privacy-preserving ECG-based biometric authentication. The proposed method starts with a thoroughly preprocessing and feature extraction stage, in which multi-domain features are extracted from time domain, frequency domain, heart rate variability (HRV) and wavelet-based descriptors to characterize the intrinsic patterns by ECG signals. If so, in the first step, the model learns discriminative embeddings of each user on distributed clients with a federated Siamese neural network without sharing any raw data, achieving inter-user separability and intra-user consistency through the metric learning process while privacy is preserved. The second stage is to train an autoencoder based reconstruction model using the real ECG features to learn normal physiological patterns, which can be effectively detected spoof via analyzing the errors in reconstruction. In inference, the framework first checks the genuineness of input signal using autoencoder and protects identity verification by similarity matching in learned embedding space. Such an integrated architecture guarantees strong authentication, resilience from the spoofing attack, and maintains data privacy. Figure 1 presents the overall architecture of our proposed FedSiam-AE framework.

Figure 1. Architecture of the proposed FedSiam-AE framework



3.1 ECG Signal Preprocessing Pipeline

In the proposed FedSiam-AE framework, preprocessing is a crucial step that adapts the raw ECG signals into clean, structured and standardized data for reliable feature extraction and learning. Electrocardiograms(ECGs) signals obtained from real-world scenarios are generally corrupted by different artifacts such as baseline drift, power frequency noise and muscle noise. This distorts the inputs that can negatively impact authentication and spoof detection models performance. Hence, a systematic preprocessing pipeline aims to improve signal quality with minimal alterations to the underlying physiological features.

3.1.1 Bandpass Filtering

A bandpass filter is used to suppress noise while keeping diagnostically relevant components from the raw ECG signal. Let $x[n]$ denote the discrete ECG signal. The filtered signal $\tilde{x}[n]$ is obtained through convolution with the filter impulse response $h[n]$:

$$\tilde{x}[n] = \sum_{k=-\infty}^{\infty} x[k]h[n-k] \quad (1)$$

Usually, a 0.5–40 Hz bandpass is applied as baseline drift and high-frequency noise removal, while the morphological content like P-wave, QRS complex and T-wave is retained. A smooth frequency response leads to use of a Butterworth filter and zero-phase filtering is achieved by forward-backward processing which removes phase distorting.

3.1.2 Signal Segmentation

After filtering, the ECG signal is split into overlapping windows of fixed length to account for temporal patterns. Let $\tilde{x}[n]$ represent the filtered signal. Each segment $s_k[n]$ of length L is defined as:

$$s_k[n] = \tilde{x}[n + kS], \quad 0 \leq n < L \quad (2)$$

Where S denotes the step size, typically set to $\frac{L}{2}$ to achieve 50% overlap, and k is the segment index. The overlapping segmentation strategy promotes robustness through redundant temporal information and reduces boundary effects.

3.1.3 R-Peak Detection

Correct detection of R-peaks is crucial for the extraction of heart rate variability (HRV) features. The proposed model then used a simplified Pan-Tompkins-inspired method consisting of differentiation, squaring and moving window integration. First, the signal is differentiated to emphasize rapid transitions:

$$y_1[n] = x[n] - x[n - 1] \quad (3)$$

The result is then squared to enhance prominent peaks:

$$y_2[n] = (y_1[n])^2 \quad (4)$$

Subsequently, a moving average filter is applied:

$$y_3[n] = \frac{1}{W} \sum_{i=0}^{W-1} y_2[n - i] \quad (5)$$

Where W represents the window length. R-peaks are identified as local maxima in $y_3[n]$ that exceed an adaptive threshold while satisfying a refractory constraint to avoid multiple detections within a short interval.

3.1.4 RR Interval Computation

After detecting the positions of R-peaks, then calculate the distance between two adjacent peaks to derive HRV-related features. RR interval is defined as follows:

$$RR_i = \frac{R_{i+1} - R_i}{f_s} \quad (6)$$

Where R_i and R_{i+1} denote successive R-peak indices and f_s is the sampling frequency. These intervals encode temporal differences in the heart rate and define individual heart shape signatures.

3.1.5 Signal Normalization

Each ECG segment is normalized using z-score normalization to reduce inter-subject and inter-session variation:

$$s_k^{norm}[n] = \frac{s_k[n] - \mu_k}{\sigma_k + \epsilon} \quad (7)$$

Where μ_k and σ_k represent the mean and standard deviation of the segment, respectively, and ϵ is a small constant to prevent division by zero. By normalizing amplitudes this way, the amplitude of the segments will scale them all equally. This allows for more robust and converging learning models.

3.1.6 Numerical Stability and Data Validation

In order to be robust, the preprocessing step includes some safeguards for invalid values. All NaN or Inf value are replaced with 0 and recurring segments with low variance will be dropped to ensure that do not create rutted features. This would ensure that only segments with stable and informative feature values would be passed to the next step of feature extraction.

3.2 Feature Extraction

After preprocessing, ECG segments are converted into a feature representation that is both discriminative and preserves the underlying physiological and morphological information of cardiac activity. FedSiam-AE framework consists of multi-domain feature extraction via time-domain, frequency-domain, HRV and wavelet features. This rich representation improves discriminability between subjects and is also robust to noise and intra-subject variation.

Let $s[n]$ denote a preprocessed ECG segment of length L . The extracted feature vector is defined as:

$$f = [f_{time}, f_{freq}, f_{HRV}, f_{wavelet}] \quad (8)$$

where each component corresponds to a specific feature domain.

3.2.1 Time-Domain Features

Time-domain characteristics of the ECG signal describe its statistical and morphologic properties. Thus, these features are computationally inexpensive and provide essential information about amplitude and the distribution of signal values. The mean and standard deviation of the signal are given by:

$$\mu = \frac{1}{L} \sum_{n=0}^{L-1} s[n], \quad \sigma = \sqrt{\frac{1}{L} \sum_{n=0}^{L-1} (s[n] - \mu)^2} \quad (9)$$

Additional statistical descriptors include:

- Minimum and maximum values:

$$s_{min} = \min(s[n]), \quad s_{max} = \max(s[n]) \quad (10)$$

- Root mean square (RMS):

$$RMS = \sqrt{\frac{1}{L} \sum_{n=0}^{L-1} s[n]^2} \quad (11)$$

- Signal energy:

$$E = \sum_{n=0}^{L-1} s[n]^2 \quad (12)$$

- Skewness and kurtosis:

$$Skewness = \frac{1}{L} \sum \left(\frac{s[n] - \mu}{\sigma} \right)^3, \quad Kurtosis = \frac{1}{L} \sum \left(\frac{s[n] - \mu}{\sigma} \right)^4 \quad (13)$$

- Zero-crossing rate:

$$ZCR = \frac{1}{L-1} \sum_{n=1}^{L-1} \mathbb{1}(s[n] \cdot s[n-1] < 0) \quad (14)$$

Such properties can well describe amplitude changes, waveform symmetric property and oscillatory characteristic.

3.2.2 Frequency-Domain Features

Model-free frequency domain analysis of the ECG signal demonstrates corresponding spectral characteristics important for differentiating individuals based on well-established physiological rhythms. The power spectral density (PSD) is estimated using Welch's method:

$$P_{xx}(f) = \frac{1}{U} \sum_{m=1}^M |\mathcal{F}\{w[n]s_m[n]\}|^2 \quad (15)$$

Where $w[n]$ is a window function and U is a normalization factor.

From the PSD, the following features are derived:

- Mean and variance of spectral power
- Maximum spectral magnitude
- Total spectral energy:

$$E_{freq} = \sum_f P_{xx}(f) \quad (16)$$

- Band power within specific frequency ranges:

$$BP_{[f_1, f_2]} = \int_{f_1}^{f_2} P_{xx}(f) df \quad (17)$$

Common bands are low-frequency (0.5–4Hz), mid-frequency (4–15 Hz) and high-frequency (15–40 Hz) bands.

3.2.3 Heart Rate Variability (HRV) Features

HRV descriptors are calculated based on RR intervals and represent the temporal characteristics of heart activity. Given RR intervals $\{RR_i\}$, the following features are computed:

- Mean RR interval:

$$\mu_{RR} = \frac{1}{N} \sum_{i=1}^N RR_i \quad (18)$$

- Standard deviation:

$$\sigma_{RR} = \sqrt{\frac{1}{N} \sum (RR_i - \mu_{RR})^2} \quad (19)$$

- Root mean square of successive differences (RMSSD):

$$RMSSD = \sqrt{\frac{1}{N-1} \sum (RR_{i+1} - RR_i)^2} \quad (20)$$

- NN50 and pNN50:

$$NN50 = \sum \parallel (|RR_{i+1} - RR_i| > 0.05), \quad pNN50 = \frac{NN50}{N} \quad (21)$$

Features derived from these capture both short-term variability and the behavior of the autonomic nervous system, making them primary candidates for how biometric distinctiveness contributes to personal security.

3.2.4 Wavelet-Based Features

The ECG segment is then subjected to discrete wavelet transform (DWT) in order to achieve localization with respect to both time and frequency. Signal is decomposed to several levels:

$$s[n] = A_j[n] + \sum_{j=1}^J D_j[n] \quad (22)$$

Where $A_j[n]$ represents the approximation coefficients and $D_j[n]$ are detail coefficients at level j . For each coefficient set, statistical features are extracted: μ_c , σ_c , $Skewness_c$, $Kurtosis_c$

Such features capture short-time patterns and localized variation of the signal, which are important for individual differences in ECG signals.

3.2.5 Feature Vector Construction

All extracted features are concatenated to form a unified feature vector:

$$f = [f_1, f_2, \dots, f_d] \quad (23)$$

Where d denotes the total number of features. The output is then globally normalized and fed into the learning part of proposed FedSiam-AE architecture. Specifically, a federated Siamese neural network is trained for discriminative embedding learning and then an autoencoder-based model for reconstruction-driven spoof detection. The design of these models and the training procedure are discussed in the following section.

3.3 Federated Siamese Metric Learning for ECG Authentication

The proposed FedSiam-AE framework is a two-level structure, where the upper level learns a discriminative embedding space using ECG-based biometric authentication modeled with federated Siamese neural network. This step is to project feature vectors extracted from ECG signals into a compact latent space that has same-sample points clustered together and different-source samples well removed. Moreover, it utilizes federated learning to preserve the privacy of data by performing distributed training without exchanging raw physiological information.

3.3.1 Siamese Network Architecture

A Siamese neural network is made of two identical subnetworks sharing the same parameterization. Each subnetwork acts as an encoder function $f_{\theta}(\cdot)$, which maps an input feature vector $f \in \mathbb{R}^d$ into an embedding space:

$$z = f_{\theta}(f) \quad (24)$$

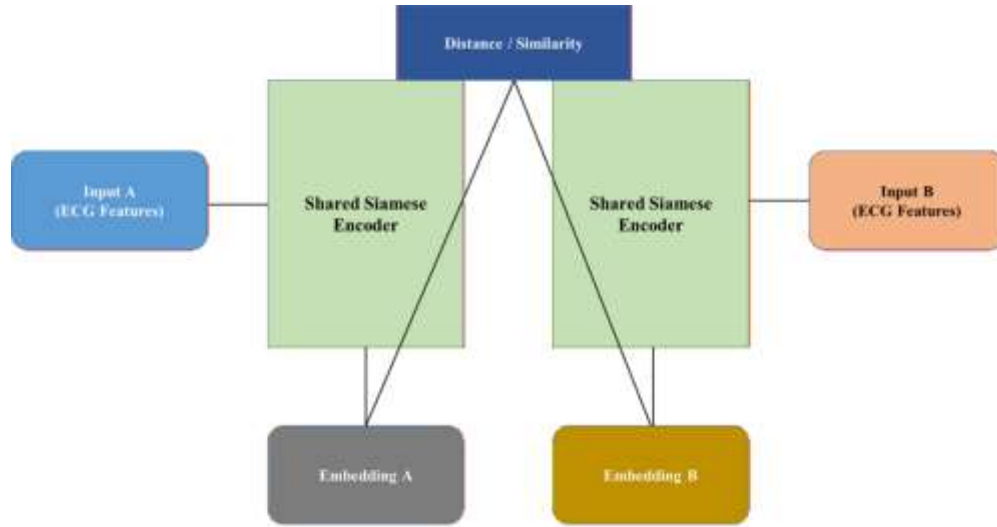
Where $z \in \mathbb{R}^m$ represents the learned embedding and θ denotes the model parameters. To ensure scale invariance, the embeddings are normalized using ℓ_2 -normalization:

$$z_{norm} = \frac{z}{\|z\|_2} \quad (25)$$

As such, this normalization allows these similarities to be computed using cosine similarity or the dot product.

Figure 2 depicts the architecture of the Siamese network used in this study. Its architecture comprises two subnetworks that share parameters and generate discriminative embeddings from input ECG feature vectors. These embeddings are then compared with a similarity function to perform identity verification.

Figure 2. Architecture of the Siamese network used for ECG-based authentication



In fact, features are transformed consistently in the same feature space across inputs thus allowing metric learning.

3.3.2 Triplet-Based Metric Learning

The model is trained on triplet loss, which operates on three samples, to learn a discriminative embedding space:

- Anchor f_a
- Positive f_p
- Negative f_n

Let,

$$z_a = f_{\theta}(f_a), \quad z_p = f_{\theta}(f_p), \quad z_n = f_{\theta}(f_n) \quad (26)$$

The Euclidean distances are computed as:

$$d_{ap} = \|z_a - z_p\|_2, \quad d_{an} = \|z_a - z_n\|_2 \quad (27)$$

The triplet loss is defined as:

$$\mathcal{L}_{triplet} = \max(0, d_{ap} - d_{an} + \alpha) \quad (28)$$

Where α is a margin parameter that enforces separation between positive and negative pairs. This loss function ensures that $d_{ap} + \alpha < d_{an}$ thereby improving intra-class compactness and inter-class separability.

3.3.3 Hard Negative Mining

The model utilizes hard negative mining to increase convergence as well as to improve the discriminative learning. Instead of randomly sampling negative examples the model sample the hardest negative example closest to anchor:

$$f_n^* = \arg \min_{f_n} \|z_a - z_n\|_2 \quad (29)$$

This strategy forces the model to learn more robust decision boundaries.

3.3.4 Federated Learning Framework

The Siamese model is trained on a federated learning paradigm to protect data privacy which multiple clients collaboratively train a common model without disclosing the original ECG records. Let K denote the number of clients. Each client k trains a local model θ_k using its private dataset. The global model is updated using Federated Averaging (FedAvg):

$$\theta^{(t+1)} = \sum_{k=1}^K \frac{n_k}{n} \theta_k^{(t)} \quad (30)$$

Where n_k is the number of samples at client k , $n = \sum_{k=1}^K n_k$, t denotes the communication round. This technique keeps the sensitive ECG data local, retaining benefits of collaborative learning.

3.3.5 Embedding-Based Authentication

Once trained, each ECG sample is mapped to a corresponding embedding vector. To authenticate, a template vector for each user should be created by averaging embeddings:

$$z_{template}^{(u)} = \frac{1}{N_u} \sum_{i=1}^{N_u} z_i \quad (31)$$

Where N_u is the number of samples for user u . During inference, a query embedding z_q is compared with stored templates using cosine similarity:

$$sim(z_q, z_u) = z_q \cdot z_u \quad (32)$$

The identity corresponding to the highest similarity score is selected.

3.3.6 Decision Thresholding

The similarity score between the query embedding and stored user templates is used as a measure of authenticity which can then be contextually applied to a decision threshold. Let z_q be the embedding of the query sample and z_u be the template embedding for user u . The similarity score is calculated by cosine similarity:

$$sim(z_q, z_u) = \frac{z_q \cdot z_u}{\|z_q\|_2 \|z_u\|_2} \quad (33)$$

The authentication decision is then formulated as:

$$\text{Accept if } \max_u sim(z_q, z_u) \geq T, \text{ Reject otherwise} \quad (34)$$

Where T represents the decision threshold.

The Siamese network is helpful for identity confirmation, but does not directly cover applications for spoofing or attacking the signals from an adversary. Consequently, additional verification stage is needed to guarantee the genuineness of input ECG signals. The following section proposes an autoencoder-based reconstruction model capable of identifying spoofed inputs by examining the errors produced during reconstruction.

3.4 Autoencoder-Based Reconstruction Learning for Spoof Detection

Although the federated Siamese network is capable of carrying out identity verification, it has no explicit measure to be sure an ECG signal input to the network is indeed what it claims to be. To tackle this limitation, the proposed FedSiam-AE framework first defines a second stage of spoofing detection based on reconstruction learning driven by autoencoders. This stage focuses on classifying authentic ECG input as real data and

spoofed or manipulated input with malicious intent as fake, by modelling the underlying distribution of physiological patterns.

3.4.1 Autoencoder Architecture

An autoencoder is a type of neural network that learns to represent input data in a compressed form by minimizing reconstruction error. The architecture of the encoder consists of two components: an encoder $g_\theta(\cdot)$ and a decoder $h_\phi(\cdot)$.

Given an input feature vector $f \in \mathbb{R}^d$, the encoding process is defined as:

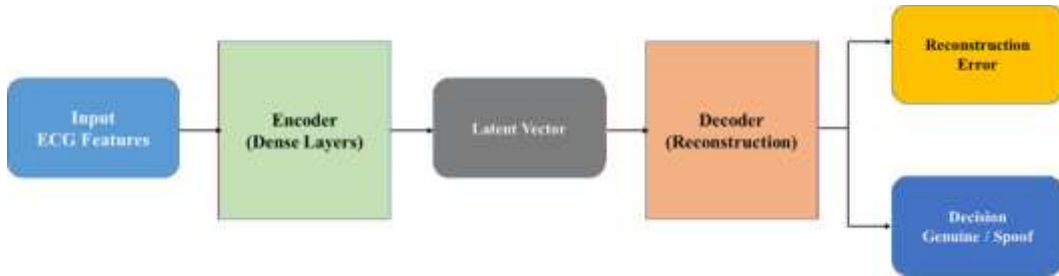
$$z = g_\theta(f) \quad (35)$$

Where $z \in \mathbb{R}^k$ is the latent representation ($k < d$). The decoder reconstructs the input as:

$$\hat{f} = h_\phi(z) = h_\phi(g_\theta(f)) \quad (36)$$

The model parameters θ and ϕ are optimized to minimize the reconstruction error. The architecture of the autoencoder used for reconstruction-based spoof detection is illustrated in Figure 3.

Figure 3. Architecture of the autoencoder-based spoof detection module



3.4.2 Training on Genuine ECG Features

To learn the distribution of authentic physiological signals, the autoencoder is trained only with clean genuine ECG feature vectors. Let $D_g = \{f_1, f_2, \dots, f_N\}$ denote the set of genuine samples. The training objective is to minimize the mean squared reconstruction error:

$$\mathcal{L}_{rec} = \frac{1}{N} \sum_{i=1}^N \|f_i - \hat{f}_i\|_2^2 \quad (37)$$

This approach trains the autoencoder to encode a compact manifold of typical heartbeats, as well as ensuring ignorance of anomalous or replayed data.

3.4.3 Reconstruction Error Computation

For a given input feature vector f , the reconstruction error is calculated during inference as $e = \|f - \hat{f}\|_2^2$. A logarithmic transformation is then performed to stabilize the dynamic range and improve numerical behaviour $e_{log} = \log(e + \epsilon)$, where ϵ is a small constant to avoid numerical instability. For multiple segments, the final error is obtained by averaging:

$$e_{final} = \frac{1}{M} \sum_{i=1}^M e_{log}^{(i)} \quad (38)$$

Where M is the number of segments.

3.4.4 Spoof Detection Decision Rule

Authenticity is determined based on the reconstruction error with respect to threshold T_s , which acts as an indicator.

$$\text{Genuine if } e_{final} \leq T_s, \text{ Spoof if } e_{final} > T_s \quad (39)$$

The underlying assumption behind this decision rule is that the authentic ECG signals reside in close proximity to the learned manifold resulting in a low reconstruction error while the spoofed signals are far apart producing higher error.

3.4.5 Threshold Optimization

It is worth noting that the best spoof detection threshold T_s , can be calculated using statistical analysis of reconstruction errors from genuine and spoof samples. Let, ε_g denote reconstruction errors for genuine samples and ε_s denote reconstruction errors for spoof samples. The threshold is chosen to maximize the distance between these distributions, typically via the Youden Index:

$$T_s^* = \arg \max_T (TPR(T) - FPR(T)) \quad (40)$$

Where, TPR is the true positive rate and FPR is the false positive rate. Another way of choosing the threshold is to take it as the point where Equal Error Rate (EER) lies.

3.4.6 Integration with Authentication Stage

In the FedSiam-AE framework, spoof detection component is treated as a pre-verification step. During inference:

- The autoencoder first performs a test on the input ECG features.
- When classified to be genuine, the features are fed through the siamese network for identifying identities.
- When classified spoof, it terminates the authentication.

The gradual fusing seamlessly integrates various forms of information in such a way that only genuine signals are used for matching identity, thus bolstering the overall authentication process's security.

3.5 GUI-based Testing

The GUI of FedSiam-AE framework is designed to provide an intuitive, interactive platform for real-time ECG-based authentication and spoof detection. The interface is structured as 2×3 grid layout that allows a clear sequential workflow. The top row consists of the application's fundamental operational modules, with control buttons such as Load ECG, Extract Features, Authenticate and Exit in sequence placed in left panel. The loaded ECG signal is visualized in the top-middle panel, and extracted feature details are displayed in the top-right panel. Row 2 interprets these results, where the identified user and similarity score from the authentication result is shown in the bottom-left panel; genuine/spoof detection result through reconstruction error is displayed on the bottom-middle panel; and finally access granted/denied status of the system is shown in the bottom-rightmost panel. In the GUI, dynamic controls are used to prevent invalid operations from being performed by enabling/disabling buttons depending on what part of execution is being executed. It enables visualization of every branch of the FedSiam-AE pipeline including signal capture, feature extraction, spoof detection, and identity verification in an intuitive interface without needing programming ability that can improve usability and transparency of the new technology while making it practically usable for biometric security systems.

The complete algorithm of the proposed FedSiam-AE framework is given below.

Algorithm: FedSiam-AE (Federated Siamese–Autoencoder Framework for ECG Authentication with Spoof Detection)

Input: Raw ECG signals (.dat); trained Siamese model; trained Autoencoder; scaler; user templates.
Output: Authentication decision (Genuine/Spoof); identified user; similarity score.
1. Initialization • Set random seeds • Load trained Siamese model • Load trained Autoencoder model • Load feature scaler • Load user templates • Define thresholds: authentication threshold τ, spoof threshold τ_s 2. ECG Signal Acquisition a. Load ECG signal from .dat file b. Extract signal channel 3. Preprocessing a. Apply bandpass filter (0.5–40 Hz) b. Segment signal into fixed windows with overlap c. Detect R-peaks d. Compute RR intervals e. Normalize each segment 4. Feature Extraction a. Extract time-domain features (mean, std, RMS, energy, skewness, kurtosis) b. Extract frequency-domain features (PSD, band power) c. Extract HRV features (RR intervals, RMSSD, pNN50) d. Extract wavelet features e. Form feature vector f 5. Feature Scaling a. Apply trained StandardScaler to feature vectors 6. Spoof Detection (Autoencoder) a. Input feature vector f into autoencoder b. Compute reconstructed vector f_{hat} c. Compute reconstruction error: $e = f - f_h ^2$ d. Apply log transform: $e_{\text{log}} = \log(e + \epsilon)$ e. If $e_{\text{log}} > \tau_s$: classify as SPOOF terminate authentication else: proceed to authentication 7. Siamese Embedding Generation a. Pass scaled features into Siamese encoder b. Obtain embeddings z c. Normalize embeddings 8. Template Matching a. Compute similarity with user templates: $\text{sim} = z \cdot z_{\text{user}}$ b. Select user with maximum similarity 9. Decision Thresholding a. If similarity $\geq \tau$: classify as GENUINE else:

reject authentication
10. Output
• Authentication result (User ID / Rejected)
• Spoof detection result
• Similarity score

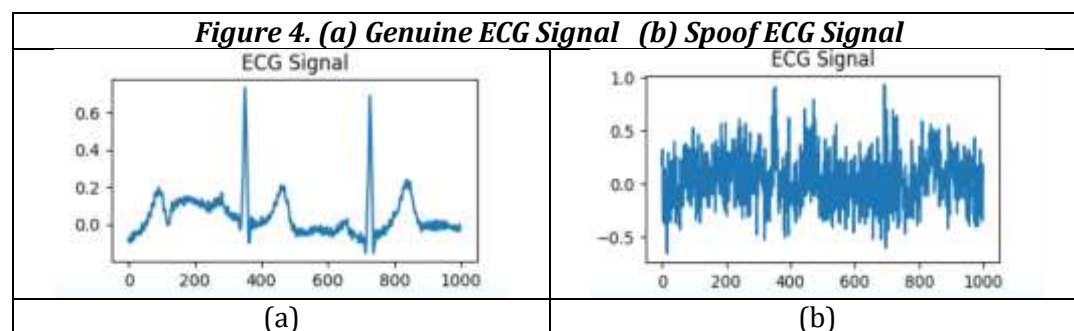
4. Results and Discussion

This study proposes a secure and robust ECG-based biometric authentication system to implement spoof detection based on federated Siamese metric learning and autoencoder-derived reconstruction analysis, which are assembled together to form the FedSiam-AE framework. The constructed framework is evaluated on a publicly available ECG dataset [24] that is chosen to encapsulate heterogeneity in cardiac patterns for biometric authentication. The model preprocess the raw ECG signals to transform them into multi-domain feature representations, including time-domain, frequency-domain, heart rate variability and wavelet-based features. For this experiment, the dataset is divided into training and testing sets by an 80:20 stratified split with respect to subjects. In the training phase, the model was trained on data distributed over multiple clients to generate a federated Siamese network while the autoencoder model is intensely trained using real ECG features to identify normal physiology. This experimental structure allows a fair assessment of the performance of authentication and spoof detection components under similar experimental conditions. Brief information about the dataset including total subjects, records and signal details are listed in Table 1.

Table 1. Description of ECG Dataset

Characteristics	Values
Source	PhysioNet
No. of Subjects	90
No. of Records	310 recordings
Sampling Frequency	500 Hz
Duration per Record	~20 seconds
Duration per Record	Single-lead ECG

The sample signal images of genuine and spoof classes are shown in Figure 4.



4.1 Authentication Performance Analysis

Specifically, the embedding representations that are extracted from the federated Siamese network to evaluate the authentication performance of the proposed FedSiam-AE framework. The performance of the model is evaluated using various metrics and

visualization tools, such as confusion matrix, Receiver Operating Characteristic (ROC) curve, Detection Error Tradeoff (DET) curve, False Acceptance Rate–False Rejection Rate (FAR–FRR) curve and score distributions. Figure 5 encompasses a confusion matrix depicting the classification performance of true and false samples, showing that the proposed model has correctly classified authorized from unauthorized users.

Figure 5. Confusion Matrix for ECG Authentication

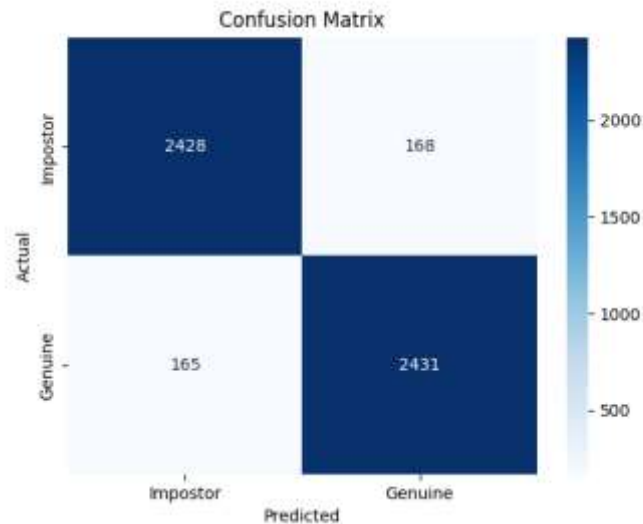
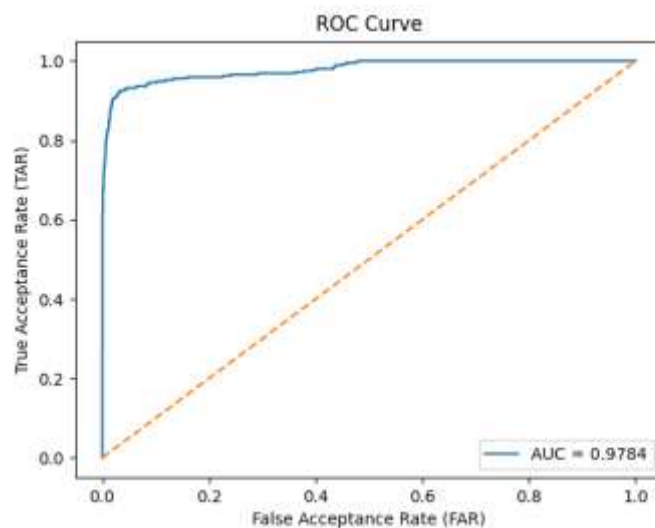


Figure 6 illustrates the receiver operating characteristic (ROC) curve showing the trade-off between true positive rate and false positive rate: The feature representation effectively distinguishes genuine vs. spoof samples, indicating that strong discriminative power of the learned embeddings is present.

Figure 6. ROC Curve for Authentication Performance



Additionally, the DET curve shown in Figure 7 gives an extended perspective on how different systems perform at varied thresholds relative to each other while the FAR–FRR curve (Figure 8) highlights a central focus point where Equal Error Rate will occur.

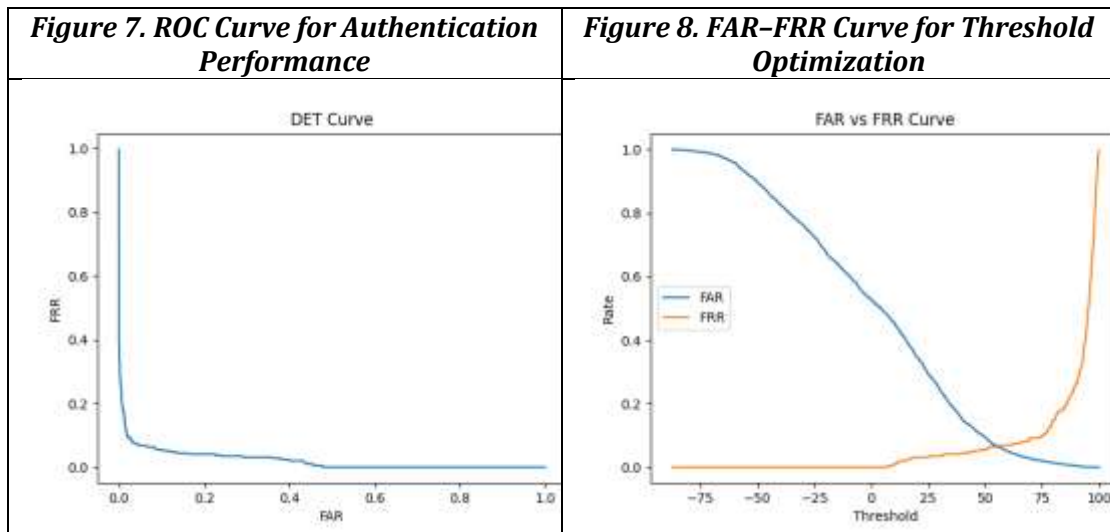
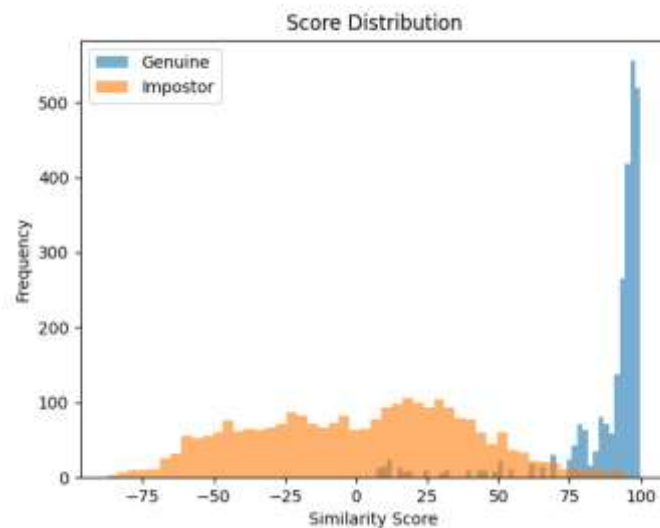


Figure 9 shows the similarity scores distribution for genuine and impostor samples, confirming that an effective metric learning was achieved.

Figure 9. FAR–FRR Curve for Threshold Optimization



In quantitative terms, the proposed framework yields an authentication accuracy of 93.59%, with a equal error rate (EER) of 6.41%, as depicted in Table 2. Using the filters calculated, the model finds the optimal decision threshold at 55.0625 which maintains an adequate balance between security and usability. Furthermore, embedding statistics demonstrate a normalized and strong embedding space via mean of -0.0029 and std dev 0.6250 . The findings indicate that the federated Siamese network learns discriminative features for reliable ECG-based authentication.

Table 2. Authentication Performance Metrics of the Proposed FedSiam-AE Framework

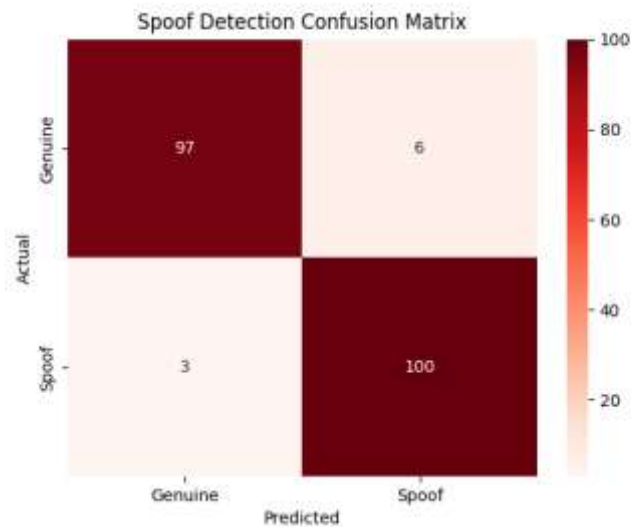
Metrics	Results
Accuracy	93.59 %
EER	6.41 %

Threshold	55.0625
Embedding Mean	-0.0029
Embedding Std	0.6250

4.2 Spoof Detection Performance Analysis

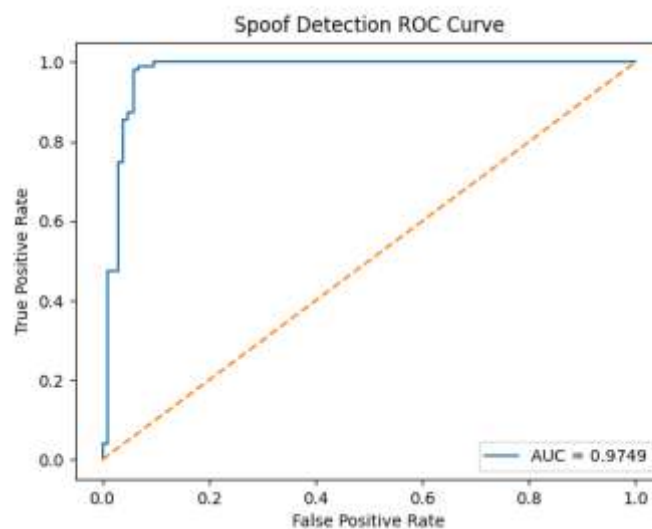
The effectiveness of the proposed framework is evaluated through the autoencoder-based reconstruction model on spoof detection. To analyze the performance, it is explored using confusion matrix, ROC curve and reconstruction error distribution. Figure 10 illustrates the confusion matrix for spoof detection, which reveals how effectively the model is able to differentiate between genuine and spoof ECG signals.

Figure 10. Confusion Matrix for Spoof Detection



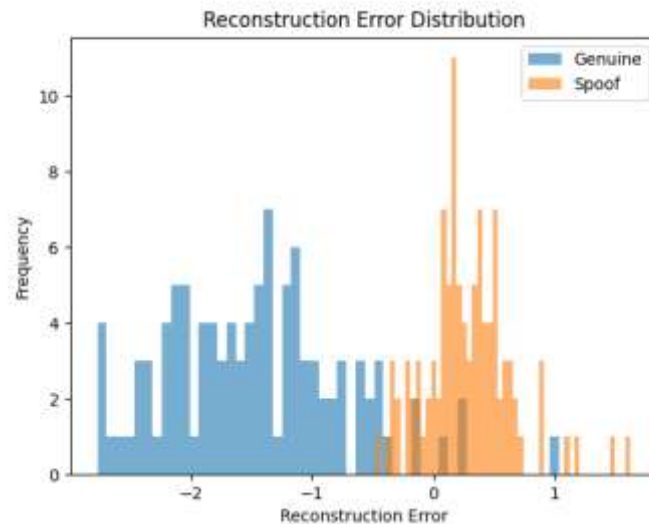
The ROC curve in Figure 11 exhibits the balance between positive detection sensitivity and false alarm rate, supporting robust discriminative performance.

Figure 11. ROC Curve for Spoof Detection Performance



Moreover, the implementation of reproach error distribution (as displayed in Figure 12) illustrates an evident distinction between the reproach errors and genuine samples, confirming the efficiency of reconstruction-based outlier observation.

Figure 12. Reconstruction Error Distribution for Genuine and Spoof Signals



The quantitative performance results are summarized in Table 3. Proposed model achieves 97.49% spoof detection accuracy, precision of 95.67%, recall of 95.63%, and F1-score of 95.63%. These results show that the proposed autoencoder successfully learns the actual distribution of genuine ECG signals and detects variations due to spoofing attacks.

Table 3. Spoof Detection Performance Metrics of the Proposed Framework

Metrics	Results
Accuracy	97.49 %
Precision	95.67 %
Recall	95.63 %
F1-score	95.63 %

A comparison of the current study FedSiam-AE framework with recent deep learning-based ECG authentication methods is shown in Table 4.

Table 4. Comparison of the Proposed FedSiam-AE Framework with Deep Learning-Based ECG Authentication Methods

Method	Model Type	Accuracy (%)	Spoof Detection	Key Characteristics
Jayaprakash et al. (2024) [14]	CNN	88.34	X	Deep feature learning with demographic-aware modeling
Lonbar et al. (2023) [25]	CNN-LSTM Hybrid	90.50	X	Multimodal biometric fusion with temporal learning

López et al. (2024) [14]	LSTM + Attention	91.79	X	Attention-based sequence modeling for improved feature focus
Proposed FedSiam-AE	Federated Siamese + Autoencoder	93.59	✓✓	Privacy-preserving + integrated spoof detection

Existing methods like the CNN based approach by Jayaprakash et al. Lonbar et al. (2023)), hybrid CNN-LSTM model (2024), and the LSTM with attention mechanism (López et al. (2024) gets decent authentication performances of 88.34%, 90.50% and 91.79%. Nevertheless, these approaches mainly address classification-performance only without mechanisms to detect spoofing or adversarial signal manipulation. On the other hand, with an additional autoencoder-based spoof detection module integrated into FedSiam-AE framework, it reaches 93.59% of accuracy. Notably, this dual-stage architecture not only leads to better performance of ECG-based authentication but also helps filter out spoofed ECG signals for enhanced security of the system. In addition, existing methods do not address the ability to perform privacy-preserving model training through federated learning. Experimental analysis confirms that the framework proposed can proactively enhance ECG-based biometric authentication system performance over simply deep learning ones.

The process of the proposed GUI for ECG-based authentication is shown in Figures 13–19. The graphical user interface facility offers a logical and well-structured way for the users to move straight through the entire process. The interface shown in Figure 13 is organized in a bordered panel 2×3 grid layout, with the first column containing the main control buttons Load ECG, Extract Features, Authenticate and Exit. Figure 14 shows the file selection dialog for selecting ECG signal data from a local machine, and Figure 15 presents the loaded ECG waveform present in GUI. Once the feature extraction is performed, successful processing is shown to the user with an output of extracted features, as can be seen in Figure 16. The results of the authenticated areas are displayed in its corresponding panels when performing on a true ECG signal (Figure 17). By the way, figure 18 shows a loading of the spoof ecg signal, and the decision about this is in figure 19.

Figure 13. GUI Layout of the Proposed ECG Authentication System

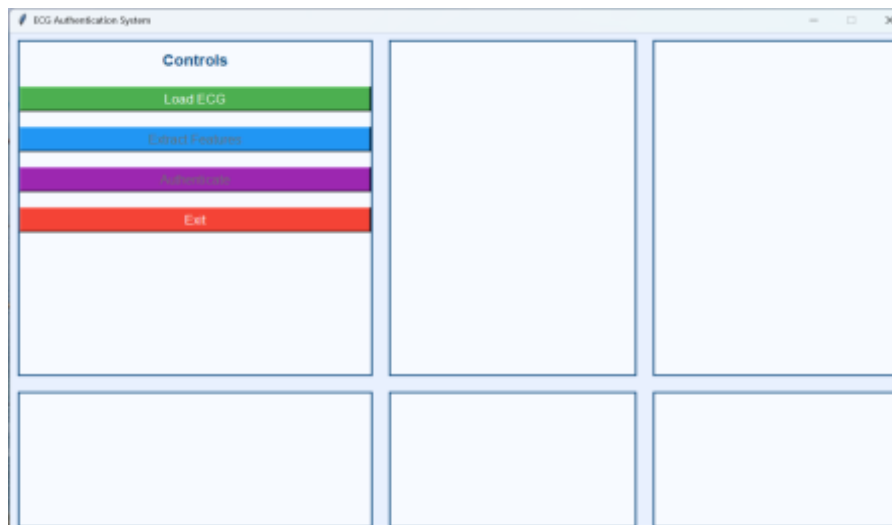


Figure 14. ECG File Selection Dialog Interface

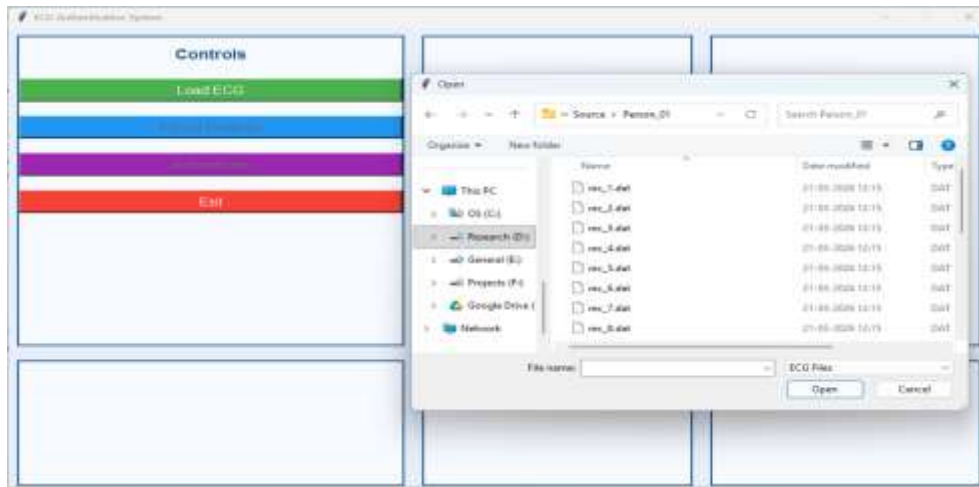


Figure 15. Visualization of Loaded ECG Signal in GUI



Figure 16. Display of Extracted ECG Features

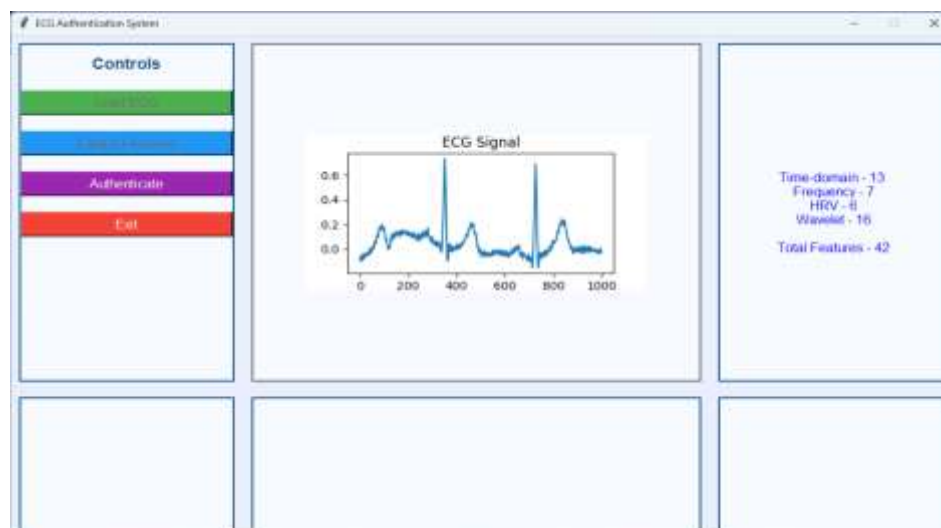


Figure 17. Authentication Result for Genuine ECG Signal



Figure 18. Loading of Spoof ECG Signal in GUI

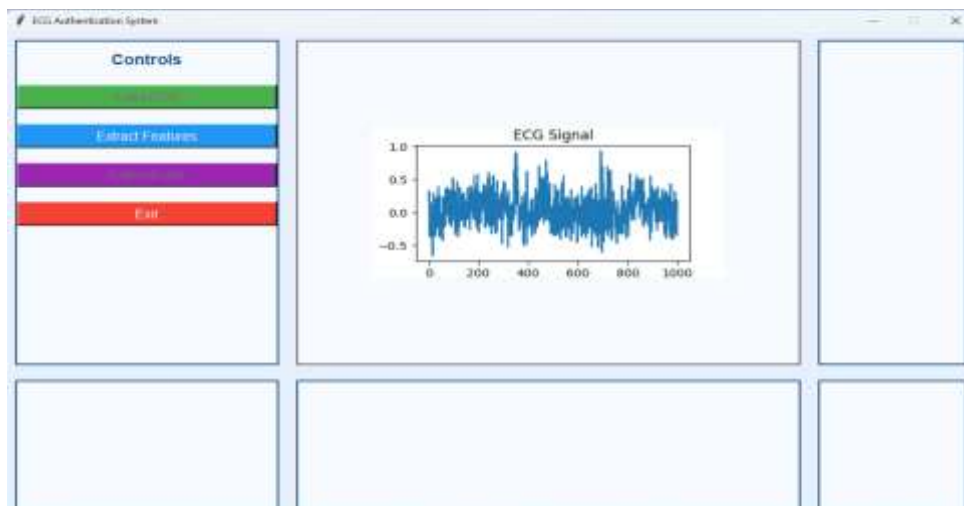
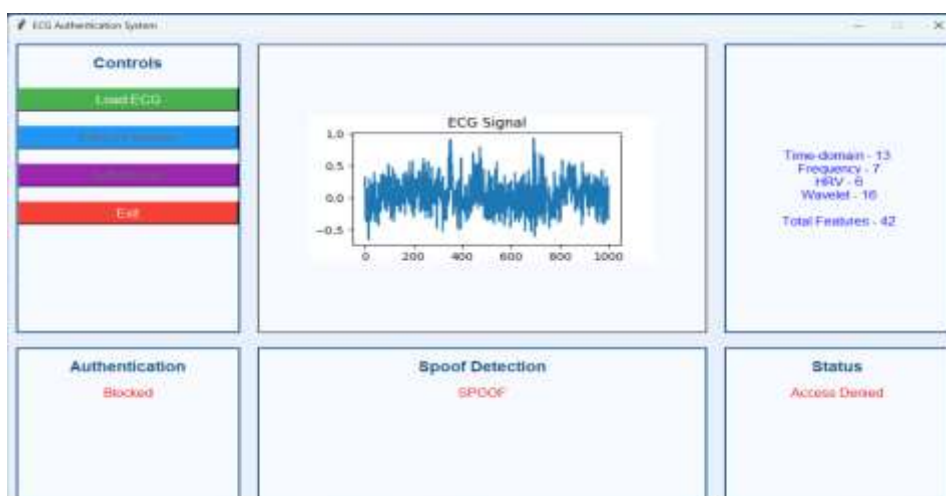


Figure 19. Authentication Result for Spoof ECG Signal



5. Conclusion

This work proposes a new approach (FedSiam-AE) that combines secure and privacy-preserving ECG-based biometric authentication with spoof detection. The proposed method, which integrates federated Siamese metric learning with autoencoder-based reconstruction analysis, resolves three fundamental challenges in biometric systems: data privacy, authentication reliability, and immunity to spoofing attacks. In this framework, federated learning is applied to train models collaboratively across distributed clients without sharing raw physiological data, maintaining user privacy and enhancing scalability for real-world applications. The experimental analysis indicates that the proposed approach yields robust authentication performance, achieving an accuracy of 93.59% and an Equal Error Rate of 6.41%, meanwhile keeping a strong discriminative power in the embedding space. Moreover, the autoencoder-based spoof detect module correctly labels whether or not ECG signals are fake and real with an accuracy of 97.49%, which is further supported by the clear separation seen in both similarity score distributions and reconstruction error patterns. While these centralized approaches offer improvements in authentication accuracy over previous deep learning algorithms, they tend to ignore important aspects such as spoof detection and data privacy. On the other hand, the FedSiam-AE framework is intended to be an end-to-end framework for all tasks because it integrates authentication and security in one form of architecture. The proposed system is thus a practical and scalable solution to next-generation biometric authentication, which is relevant in healthcare and IoT environments where the amount of sensitive data coupled with system dependence and reliability poses unforgiving challenges. Federated learning in conjunction with metric-based embedding and reconstruction-driven anomaly detection provides a solid basis for the design of secure, robust and privacy-aware biometric systems.

References

1. Hazratifard M, Agrawal V, Gebali F, Elmiligi H, Mamun M. Ensemble Siamese Network (ESN) Using ECG Signals for Human Authentication in Smart Healthcare System. *Sensors*. 2023; 23(10): 4727. <https://doi.org/10.3390/s23104727>
2. Wang G, Shanker S, Nag A, Lian Y, John D. ECG Biometric Authentication Using Self-Supervised Learning for IoT Edge Sensors. *arXiv preprint*. 2024. <https://arxiv.org/abs/2409.05627>
3. Behrozi P, Shirkani B, Hazratifard M. Using ECG Signals in Siamese Networks for Authentication in Digital Healthcare Systems. *Journal of Biomedical Research & Environmental Sciences*. 2022; 3(11): 1367-1373. <https://www.jelsciences.com/articles/jbres1605.php>
4. Jayaprakash A, Patro KK, Samantray S, Plawiak P, Hammad M. A Deep Learning Technique for Biometric Authentication Using ECG Beat Template Matching. *Information*. 2023; 14(2): 2-16. <https://www.researchgate.net/publication/367350712>
5. Deshpande S, Getnet Y, Dargie W. Detection of Intelligent Tampering in Wireless Electrocardiogram Signals Using Hybrid Machine Learning. *arXiv preprint*. 2025. <https://arxiv.org/abs/2507.06402>
6. Rai DH, Kafley S. Lightweight MobileNetV1+GRU for ECG Biometric Authentication: Federated and Adversarial Evaluation. *arXiv preprint*. 2025. <https://arxiv.org/abs/2509.20382>
7. Kapsecker M, Jonas SM. Cross-device federated unsupervised learning for ECG anomaly detection using autoencoders. *PLOS Digit Health*. 2025; 4(4): e0000793. <https://pmc.ncbi.nlm.nih.gov/articles/PMC11975069/>

8. Ibtehaz N, Chowdhury MEH, Khandakar A, Kiranyaz S, Rahman MS, Tahir A, Qiblawey Y, Rahman T. EDITH: ECG Biometrics Aided by Deep Learning for Reliable Individual Authentication. arXiv preprint. 2021. <https://arxiv.org/abs/2102.08026>
9. Zhang Q, Zhou D, Zeng X. HeartID: A Multiresolution Convolutional Neural Network for ECG-Based Biometric Human Identification in Smart Health Applications. IEEE Access. 2017; 5: 11805-11816.
<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7933065>
10. Prakash AJ, Kiran KP, Hammad M, Tadeusiewicz R, Pławiak P. BAED: A secured biometric authentication system using ECG and deep learning. Biocybernetics and Biomedical Engineering. 2022; 42(4): 1081-1093.
<https://www.sciencedirect.com/science/article/abs/pii/S0208521622000778>
11. Wang X, Cai W, Wang M. A novel approach for biometric recognition based on ECG feature vectors. Biomedical Signal Processing and Control. 2023; 86(A): 104922.
<https://www.sciencedirect.com/science/article/abs/pii/S1746809423003555>
12. Lonbar SM, Beigi A, Bagheri N, Peris-Lopez P, Camara C. Deep learning based biometric authentication system using a high temporal/frequency resolution transform. Frontiers in Digital Health. 2024; 17(6): 1463713.
<https://pmc.ncbi.nlm.nih.gov/articles/PMC11685233/>
13. Choi G, Ziyang G, Wu J, Esposito C, Choi C. Multi-modal biometrics based implicit driver identification System Using Multi-TF Images of ECG and EMG. Computers in Biology and Medicine. 2023; 159: 106851.
<https://www.sciencedirect.com/science/article/abs/pii/S0010482523003165>
14. López JLC, Parra C, Forero G. An ECG Deep Learning user identification architecture using ECG sex recognition as a selective parameter. Informatics in Medicine Unlocked. 2024; 50: 101563.
<https://www.sciencedirect.com/science/article/pii/S2352914824001199>
15. Alfi MA, Lopez PP, Camara C. Enhancing biometric identification using 12-lead ECG signals and graph convolutional networks. Frontiers in Digital Health. 2025; 7: 1547208. <https://www.frontiersin.org/articles/10.3389/fdgth.2025.1547208>
16. Li L, Chen C, Pan L, Tai Y, Zhang J, Xiang Y. Hiding Your Signals: A Security Analysis of PPG-Based Biometric Authentication. European Symposium on Research in Computer Security. 2023; 183-202.
https://link.springer.com/chapter/10.1007/978-3-031-51479-1_10
17. Kim JS, Pan S. Fake Electrocardiogram Signal Analysis to Detect Spoofing Attacks in Biometrics. IEEE Sensors Journal. 2025; 25(14): 27221 - 27229.
<https://doi.org/10.1109/JSEN.2025.3577311>
18. Garg A, Karimian N. ECG Biometric Spoofing Using Adversarial Machine Learning. IEEE International Conference on Consumer Electronics. 2021.
<https://par.nsf.gov/servlets/purl/10333140>
19. Abdullahi SM, Sun S, Wang B, Wei N, Wang H. Biometric template attacks and recent protection mechanisms: A survey. Information Fusion. 2024; 103: 102144.
<https://www.sciencedirect.com/science/article/pii/S1566253523004608>
20. Wang W, Zhang X, Du J, Zhao W. Robust continuous authentication via multi-channel photoplethysmography signals: A wearable wristband solution for uncontrolled environments. Computers & Security. 2025; 159: 104686.
<https://www.sciencedirect.com/science/article/abs/pii/S016740482500375X>
21. Gimba UA, et al. Enhancing biometric authentication through multimodal approach combining face and fingerprint recognition using convolutional neural networks (CNN). Discover Computing. 2025; 28: 246.
<https://link.springer.com/article/10.1007/s10791-025-09775-z>

22. Aguilar D, Martínez-Cruz A, Ramírez-Gutiérrez KA, Morales-Sandoval M. PPG-based biometric authentication: A review on architectures, datasets, attacks and security challenges. *Computational and Structural Biotechnology Journal*. 2025; 28: 511-528. <https://pmc.ncbi.nlm.nih.gov/articles/PMC12664393/>
23. Singh RP, Dash R, Mohapatra RK. Unveiling explainability in face anti-spoofing: Hybrid feature extraction with XAI-guided feature aggregation. *Pattern Recognition*. 2025; 169: 111905. <https://www.sciencedirect.com/science/article/pii/S0031320325005655>
24. Dataset source: <https://www.kaggle.com/datasets/bjoernjostein/ecgid-database>