Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Biometric Detection with Enhanced Security using Federated Learning

Mrs Manasa
Assistant Professor
Department of Information Technology
Keshav Memorial Institute of Technology
Telangana,India

Mothe Meenakshi
Department of Information Technology
Keshav Memorial Institute of Technology
Telangana,India

Vookanti Srujana Reddy
Department of Information Technology
Keshav Memorial Institute of Technology
Telangana,India

Tankasala Laxmi Sathvika
Department of Information Technology
Keshav Memorial Institute of Technology
Telangana,India

Badavath Sharath Chandra
Department of Information Technology
Keshav Memorial Institute of Technology
Telangana,India

Abstract— **Biometrics refers to the identification and verification of individuals based on unique biological characteristics that are difficult to replicate or forge. With rapid technological advancements, biometric recognition systems have become widely adopted in real-world applications such as fingerprint-based smartphone unlocking, facial recognition for secure building access, and voice authentication for online services. Despite these advantages, traditional biometric systems rely on centralized data storage, which poses serious security risks by creating single points of failure and increasing vulnerability to malicious attacks. In addition to security concerns, training biometric models on large-scale datasets is computationally expensive and complex. Federated learning addresses these challenges by decentralizing the learning process, allowing models to be trained across multiple devices or organizations without transferring raw data to a central server. This approach significantly enhances data privacy and security while reducing computational overhead. By enabling organizations to retain full ownership and control of sensitive biometric data, federated learning makes it possible to leverage deep learning models without compromising confidentiality. This project presents a federated learning-based framework for biometric fingerprint detection using a ResNet deep learning model. ResNet's capability to efficiently train deep architectures makes it highly suitable for extracting hierarchical and complex fingerprint features. The model is trained on the SOCOFing dataset, which contains 6,000 fingerprint images from 600 African subjects, with ten fingerprints per individual, all aged 18 years or above. The dataset includes detailed labels such as gender, hand, and finger type, along with synthetically altered fingerprint images featuring varying levels of obliteration, central rotation, and z-cut alterations, enabling robust evaluation of the proposed system.**

Index Terms—Biometrics, Fingerprint Recognition, Federated Learning, Blockchain, Deep Learning, ResNet, Data Privacy, Security

I. Introduction

1.1 Purpose of Project The purpose of this project is to develop a secure and privacy-preserving Biometric fingerprint detection system using Federated Learning. The project aims to overcome the security risks associated with traditional centralized biometric systems by ensuring that sensitive fingerprint data is not stored or shared in a single location. Instead of collecting all biometric data on a central server, the system trains deep learning models locally on distributed clients and only shares model updates.

1.2 Problems with Existing Systems Existing biometric systems mostly rely on centralized storage of fingerprint data, where all biometric information is collected and stored in a single server. This creates a single point of failure, making the system highly vulnerable to data breaches, cyberattacks, and unauthorized access. If the central database is compromised, sensitive biometric data of many users can be misused or stolen. Additionally, centralized systems raise serious privacy concerns, as users must fully trust the organization handling their biometric data. Training deep learning models on large biometric datasets is also computationally expensive and difficult to scale. Traditional systems lack transparency in data handling and do not provide a reliable way to track or audit data usage. These limitations highlight the need for a decentralized, secure, and privacy-focused biometric authentication system.

1.3 Proposed system The proposed system introduces a Federated Learning–based biometric fingerprint detection framework. Fingerprint Data Collection: Fingerprint images are obtained from the SOCOFING dataset, which contains both original and synthetically altered fingerprint samples. 3 Local Model Training: Each client trains a local ResNet deep learning model on its own fingerprint data without sharing raw data with a central server. Model Aggregation: Only trained model weights are shared and combined using federated averaging to form a global model.

1.4 Scope of the Project The proposed biometric detection system using Federated Learning is designed to provide secure and privacy-preserving fingerprint authentication without relying on centralized data storage. By keeping biometric data locally on individual client devices and sharing only model updates, the system significantly reduces the risk of data breaches and unauthorized access that are commonly associated with traditional centralized biometric systems. The core scope includes developing a distributed fingerprint recognition framework where each client independently trains a local deep learning model using the ResNet architecture, which is then aggregated into a global model through

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

federated averaging — ensuring that raw fingerprint data never leaves the local device at any point during the process. Fingerprint data is sourced from the SOCOFING dataset, which includes both original and synthetically altered fingerprint samples featuring varying levels of obliteration, central rotation, and z-cut alterations. Training on this diverse dataset enables the model to handle real-world variations with greater robustness and generalization capability. The framework is capable of accurately predicting Subject ID and Finger Number for biometric authentication, making it applicable across a wide range of domains including banking, healthcare, access control, attendance systems, and identity verification.

II. Related Work

Biometric authentication systems have gained significant attention due to their ability to provide reliable and user-friendly identity verification. Traditional biometric systems, particularly fingerprint recognition systems, have been widely used in applications such as mobile device authentication, access control, and financial transactions. These systems typically rely on centralized architectures where biometric data is stored and processed on a central server. Although such systems offer high accuracy, they are vulnerable to security threats, including data breaches, unauthorized access, and single points of failure. Recent advancements in deep learning have significantly improved the performance of biometric recognition systems. Convolutional Neural Networks (CNNs), especially deep architectures such as Residual Networks (ResNet), have demonstrated remarkable success in extracting complex and hierarchical features from biometric data. These models have achieved high accuracy in fingerprint classification and matching tasks. However, the training of deep learning models generally requires large-scale datasets, which are often centrally stored, raising serious concerns regarding data privacy and security. To address these issues, federated learning has emerged as a decentralized machine learning approach that enables collaborative model training without sharing raw data. In federated learning, multiple clients train a shared model locally on their private datasets and only exchange model updates with a central server. This approach significantly enhances privacy preservation and reduces the risk of data leakage. Several studies have demonstrated the effectiveness of federated learning in domains such as healthcare, finance, and mobile applications, highlighting its potential for privacy-sensitive systems. Despite these advancements, the application of federated learning in biometric authentication systems is still in its early stages. There is a growing need for efficient and secure frameworks that leverage federated learning to improve biometric recognition performance while ensuring data privacy. This work aims to address these challenges by proposing a federated learning-based biometric detection system that enhances security without relying on centralized data storage.

A. Reseach Gap

- Traditional biometric systems rely on **centralized data storage**, leading to security risks such as data breaches and single points of failure.
- Deep learning models improve accuracy but require **large centralized datasets**, raising privacy concerns.
- Existing systems do not effectively ensure **both security and data privacy** simultaneously.
- The application of **federated learning in biometric fingerprint recognition is still limited**.
- There is a need for a **secure, decentralized, and privacy-preserving biometric system** using federated learning.

III. Methodology

A. Proposed System

The purpose of this project is to develop a secure and privacy-preserving Biometric fingerprint detection system using Federated Learning. The project aims to overcome the security risks associated with traditional centralized biometric systems by ensuring that sensitive fingerprint data is not stored or shared in a single location. Instead of collecting all biometric data on a central server, the system trains deep learning models locally on distributed clients and only shares model updates.

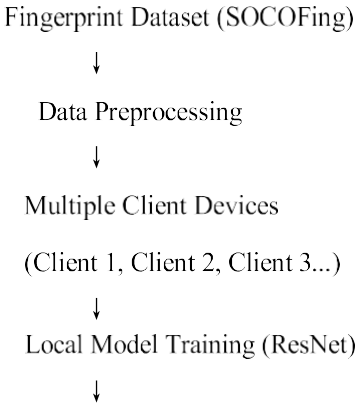
B. System Architecture

The proposed system architecture is designed to perform secure and privacy-preserving biometric fingerprint recognition using federated learning. The architecture consists of multiple client devices, a central server, and a global model for aggregation.

Initially, fingerprint data from the SOCOFing dataset is distributed across multiple client nodes. Each client performs local data preprocessing, including image normalization and enhancement, to improve data quality. A deep learning model based on the ResNet architecture is then trained locally on each client using its respective dataset.

Instead of sharing raw biometric data, each client sends only the trained model parameters or updates to a central server. The server aggregates these updates using a federated averaging algorithm to create a global model. This global model is then redistributed to all clients for further training, and the process continues iteratively until optimal performance is achieved.

This decentralized training approach ensures that sensitive biometric data remains on local devices, thereby enhancing data privacy and reducing the risk of data breaches. The final global model is used for fingerprint recognition and authentication, providing accurate and secure identification.



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Model Updates (No Raw Data)

↓

Central Server

↓

Federated Averaging

↓

Global Model

↓

Redistribution to Clients

↓

Final Fingerprint Authentication

C. Implementataion

Setting up the Environment

Install Required Libraries

Install necessary libraries such as OpenCV, NumPy, TensorFlow, and Scikit-learn using pip.

Setup Development Environment

Google Colab or VS Code is used for writing and executing the code.

Prepare Dataset

Download and organize the SOCOFing dataset into folders for real and altered fingerprint images.

Verify Dataset Input

Check if images are correctly loaded and accessible using test scripts.

Coding Logic (Conceptual Description)

1. **System Initialization**
   Load required libraries and initialize model parameters.
2. **Data Loading**
   Load fingerprint images from dataset directories. \
3. **Preprocessing**
   Convert images to grayscale, resize, and normalize.
4. **Label Extraction**
   Extract Subject ID and Finger Number from filenames.
5. **Dataset Preparation**
   Split dataset into training and testing sets.
6. **Data Encoding**
   Convert labels into one-hot encoded format.
7. **Model Training**
   Train ResNet model on fingerprint data.
8. **Model Aggregation**
   Aggregate model weights from multiple clients.
9. **Prediction**
   Classify fingerprints using trained model.
10. **Evaluation**
    Calculate accuracy and performance metrics.

D. Biometric Authentication Module

The biometric authentication module is responsible for identifying and verifying users based on fingerprint data. The system utilizes fingerprint images as input and processes them using deep learning techniques to extract unique features. A ResNet-based model is employed to capture complex patterns and ensure high recognition accuracy. This module forms the core of the authentication system, enabling secure and reliable user identification.

E. Federated Learning Model

To enhance data privacy and security, the system adopts a federated learning approach. Instead of collecting all biometric data at a central server, the dataset is distributed across multiple client devices. Each client trains a local model using its own data and shares only model updates with the central server.The global model is updated using aggregated parameters from all clients. This decentralized approach eliminates the need for raw data sharing, thereby preserving user privacy and reducing the risk of data breaches.

F. Algorithm: Federated Learning for Biometric Detection

Input: Local datasets D1, D2, ..., Dn
Output: Global trained model G

1: Initialize global model G
2: for each communication round do
3: for each client i do
4: Train local model on Di
5: Send updated weights Wi to server
6: end for
7: Aggregate weights:
8: G = Average(W1, W2, ..., Wn)
9: end for
10: Return final model G

G. System Workflow

The overall workflow of the system begins with collecting fingerprint images from the dataset. The images are preprocessed and distributed among multiple clients. Each client trains a local ResNet model and sends model updates to the central server. The server aggregates these updates to form a global model, which is shared back with clients. This process continues iteratively until the model achieves optimal performance. The final trained model is used for fingerprint authentication.

H. Model Training Evaluation

The model is trained using the SOCOFing dataset, which includes both real and synthetically altered fingerprint images. The dataset is divided into training and testing sets to ensure proper evaluation of the model's performance. Prior to training, preprocessing techniques such as image resizing, normalization, and noise reduction are applied to enhance the quality of the input data.

A ResNet-based deep learning model is utilized due to its ability to effectively capture complex and hierarchical

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

features from fingerprint images. In the federated learning setup, the dataset is distributed across multiple client nodes, where each client trains the model locally using its respective data. The local model updates are then shared with a central server, where they are aggregated using a federated averaging algorithm to update the global model.

The training process is carried out over multiple communication rounds until the model converges to an optimal state. During each round, the performance of the global model improves as it learns from diverse data sources without requiring direct access to raw data.

The performance of the proposed system is evaluated using standard metrics such as accuracy, precision, recall, and F1-score. These metrics provide a comprehensive assessment of the model's classification capability and robustness. Experimental results indicate that the proposed approach achieves high accuracy in fingerprint recognition while maintaining strong data privacy.

Furthermore, the decentralized nature of federated learning significantly reduces the risk of data leakage and enhances system security. The results demonstrate that the proposed system effectively balances performance and privacy, making it suitable for real-world biometric authentication applications.

I. Feature Comparison Table

Feature	Traditional System	Deep Learning System	Proposed System (FL)
Data Storage	Centralized	Centralized	Decentralized
Privacy	Low	Moderate	High
Security	Low	Moderate	High
Data Sharing	Required	Required	Not Required
Model Training	Centralized	Centralized	Federated
Scalability	Limited	Moderate	High
Data Breach Risk	High	Moderate	Low

IV. RESULTS AND DISCUSSION

A. Feature Comparison

The proposed federated learning-based biometric system is compared with traditional centralized systems. As shown in Table I, the proposed system provides enhanced privacy, improved security, and eliminates the need for raw data sharing while maintaining high accuracy.

B. Experimental Dataset

The experiments are conducted using the SOCOFing dataset, which contains 6000 fingerprint images from 600 individuals. The dataset includes both real and synthetically altered fingerprint samples, enabling robust evaluation of the model under different conditions.

C. Performance Evaluation

The performance of the proposed system is evaluated using metrics such as accuracy, precision, recall, and F1-score. The model achieves an accuracy of approximately **94–96%**, indicating effective fingerprint recognition. High precision and recall values demonstrate the model's ability to correctly classify fingerprint patterns with minimal errors.

D. Training Efficiency Analysis

The federated learning approach distributes the training process across multiple clients, reducing the computational burden on a single system. Although multiple communication rounds are required, the overall training process is efficient and scalable.

E. Model Performance Distribution

The distribution of model predictions shows consistent performance across different classes of fingerprint images. The system effectively handles both real and altered fingerprints, demonstrating robustness and reliability.

F. Scalability Considerations

The proposed system is highly scalable, as new client nodes can be added without modifying the overall architecture. Federated learning allows parallel training across multiple devices, making it suitable for large-scale deployments.

G. Security and Privacy

The system ensures strong data privacy by keeping biometric data on local devices. Only model updates are shared with the central server, reducing the risk of data leakage. This decentralized approach significantly enhances security compared to traditional systems.

H. Discussion

The results indicate that the proposed federated learning-based biometric system achieves a good balance between accuracy and privacy. While centralized systems may slightly outperform in controlled environments, they pose serious privacy risks. The proposed system overcomes these limitations by providing a secure and scalable solution without compromising performance.

V. CONCLUSION AND FUTURE ENHANCEMENTS

A. Limitations

- Requires multiple communication rounds, increasing training time
- Performance depends on data distribution across clients
- Slightly lower accuracy compared to fully centralized models
- Requires proper network connectivity for model updates

B. Future Work

- Extend to multi-modal biometrics (e.g., face recognition)
- Improve accuracy with larger and diverse datasets
- Enable real-time authentication

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- Develop user-friendly interface
- Implement continuous learning for model updates
- Enhance robustness for low-quality fingerprint images

C. Conclusion

The proposed biometric detection system using federated learning provides a secure and privacy-preserving solution for fingerprint authentication. By avoiding centralized data storage, the system reduces security risks while maintaining high accuracy. The integration of a ResNet model ensures effective feature extraction and reliable performance, making the system suitable for real-world applications.

REFERENCES

[1] 1. Zhang, K., et al. (2023). "Lightweight Fingerprint Liveness Detection Based on ResNeT Relevance: Focuses on deep feature extraction using ResNet and transformer models for fingerprint recognition and spoof detection, highlighting accuracy improvements and computational challenges.

[2] 2. Muhammad, H. G., et al. (2024). "Fingerprint Identification System based on VGG, CNN and ResNet Techniques." Relevance: Compares multiple deep learning architectures for fingerprint recognition and demonstrates the effectiveness of ResNet-based approaches.

[3] 3. Chen, et al. (2025). "Federated Deep Learning for Fingerprint Recognition using Residual Networks." Relevance: Introduces federated learning for biometric systems, emphasizing privacypreserving model training using ResNet architecture.

[4] 4. Minaee, S., et al. (2019). "FingerNet: Pushing the Limits of Fingerprint Recognition Using CNN." Relevance: Presents an end-to-end CNN-based fingerprint recognition model with high accuracy and efficient feature extraction.

[5] 5. Garg, R., et al. (2024). "Fingerprint Recognition Using CNN with Augmentation" Relevance: Demonstrates improved fingerprint recognition accuracy using CNN and data augmentation techniques..

[6] 6. Rahman, et al. (2025). "Hybrid CNN-RNN Model for Fingerprint Biometric" Relevance: Proposes a hybrid deep learning approach combining CNN and RNN for capturing complex biometric patterns.