European Journal of Computer Science and Information Technology, 14(3), 42-53, 2026
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Federated Learning-Based Hybrid Model for Secure Fraud Detection in Distributed Rural Environments

Pham Nhat Minh
Hanoi-Amsterdam High School for the Gifted, Vietnam

doi: https://doi.org/10.37745/ejcsit.2013/vol14n34253 Published May 24, 2026

Citation: Minh P.N. (2026) Federated Learning-Based Hybrid Model for Secure Fraud Detection in Distributed Rural Environments, *European Journal of Computer Science and Information Technology*, 14(3), 42-53

Abstract: *Accurate and efficient detection of fraudulent financial transactions is essential for ensuring security, trust, and stability in modern digital financial systems. However, this task remains challenging due to highly imbalanced datasets, continuously evolving fraud strategies, heterogeneous data distributions across different financial institutions, and strict privacy constraints in distributed environments. To address these challenges, this research proposes a federated learning-based hybrid deep learning model for fraud detection across distributed rural financial environments. The evaluation was conducted using the Credit Card Fraud Detection Dataset (CCFD), which comprises 284,807 financial transactions with 492 fraudulent transactions. This dataset is severely skewed between valid and fraudulent classes. To mitigate class imbalance, the Synthetic Minority Oversampling Technique (SMOTE) was applied during preprocessing to improve the representation of minority fraud samples and enhance model learning capability. The proposed Pity Beetle Algorithm- driven Federated-tuned Recurrent Neural Networks (PBA-FederatedRNN) model integrates Recurrent Neural Networks (RNNs) for sequential transaction behavior learning and the Pity Beetle Algorithm (PBA) for optimized parameter tuning and faster convergence. Federated learning ensures robust data security and privacy preservation by allowing several financial nodes to cooperatively train a global model without exchanging raw data. The model was implemented using Python with TensorFlow/PyTorch in a distributed simulation environment. According to experimental results, the proposed model outperforms existing centralized and federated approaches with 97.8% recall, 98.0% F1-score, 98.7% accuracy, and 98.2% precision. With all factors considered, the proposed PBA-FederatedRNN model offers a flexible, dependable, and highly efficient fraud detection solution in distributed financial systems that protect privacy.*

Keywords: federated learning, fraud detection, hybrid model, privacy preservation, distributed systems, secure aggregation, rural environments

INTRODUCTION

Federated Learning enables effective privacy preservation and decentralized anomaly detection with minimal communication, whereas smart grid systems use smart meters and machine learning to enable effective energy management [1]. The conventional approach of detecting credit card fraud was becoming

ineffective due to its increasing frequency. Transformer-based Structured Data Federated Learning for fraud detection with efficient, privacy-preserving decentralized transaction history and minimal transmission can discover high-value, complicated transactions that earlier transaction detection systems would have overlooked [2]. Federated Learning and Blockchain are being used by a digitally mediated healthcare system utilizing the Internet of Medical Things to provide safe, privacy-preserving data sharing and intelligent anomaly detection in a decentralized healthcare setting [3]. Federated Learning and Deep Learning help to improve secure fraud detection in FinTech while protecting user transaction data privacy and identifying complex, fraud behavior [4]. Federated Learning enables several banks to share model parameters instead of sensitive client transaction data, allowing for cooperative privacy-preserving bank fraud detection [5].

To design an accurate, scalable and private PBA-FederatedRNN framework in a distributed rural financial context for fraud detection by using the federated learning approach, sequential transaction analysis using RNN model, SMOTE for handling data imbalance and PBA optimization in order to enhance the fraud detection accuracy, convergence rate, communication efficiency and data privacy protection. The major key contributions are as follows:

- Proposed a hybrid PBA-FederatedRNN model integrating Recurrent Neural Networks for sequential transaction analysis and Pity Beetle Algorithm for optimized parameter tuning in distributed rural financial environments.
- Enabled privacy-preserving collaborative fraud detection using federated learning without sharing raw financial transaction data among institutions.
- Addressed class imbalance and data heterogeneity issues using SMOTE-based preprocessing to improve minority fraud class learning and model robustness.
- Improved overall fraud detection accuracy, scalability, and convergence efficiency in distributed and resource-constrained financial systems compared to existing methods.

The sections of this research are organized as follows. Section 1 presents the introduction to fraud detection in distributed rural financial environments. Research gaps and related work are covered in Section 2. Section 3 outlines the proposed PBA-FederatedRNN model. The experimental findings and performance analysis are presented in Section 4. Section 5 summarizes the study's shortcomings and future directions.

RELATED WORK

The traditional fraud detection methods relied on centralized ML/DL models with huge computational load, weak privacy protection, bad scalability, and poor adaptability in the distributed rural financial

context. To secure fintech fraud detection using blockchain-based Federated Learning [6]. Several ML models were trained together to gain security and privacy. However, due to scalability constrains and computational cost, deployment problems remain.

To detect credit card fraud using Jellyfish Namib Beetle Optimization Algorithm (JNBO)-Spinal-Net was examined [7]. Quantile normalization, feature selection, bootstrapping, and optimization were employed, obtaining an accuracy of 89.10%. However, higher Root Mean Square Error (RMSE) and low scalability were its limitations.

To improve secure cloud-based fraud detection using Adaptive Secure Federated Learning (ASFL), it was investigated [8]within Secure Federated Cloud for Financial Analytics (SFC-FA), Homomorphic encryption, differential privacy, and Reinforcement learning demonstrated 12% resources and 97.5% accuracy. The issue of encryption latency remains.

To improve credit card fraud detection, FinGraphFL was analyzed [9]. Graph Attention Networks, federated learning, and differential privacy achieved 97.80% and 98.39% accuracy, respectively. Nevertheless, deployment complexity remained a limitation.

To develop privacy-preserving decentralized fraud detection using deep autoencoders was explored [10]. For Distributed Local Training and the threshold-based anomaly detection, both the Receiver Operating Characteristic (ROC) and Precision–Recall (PR) curves showed that there were good precisions, but the recalls were not so great. This was caused by the class imbalance.

To improve privacy-preserving fraud detection using Federated Learning-based Share–Private Feature Distillation for Fraud Detection (FED-SPFD) was assessed [11]. Using share-private segmentation and autoencoders with Gaussian alignment, the accuracy was 95.34% and F1-score was 80.90%, respectively, although the computational complexity remained a problem.

To improve secure Card Fraud Detection, federated learning and blockchain were utilized [12]. Optimization methods, Long Short-Term Memory (LSTM), Random Forest (RF), Convolutional Neural Network (CNN), and Synthetic Minority Oversampling Technique (SMOTE) achieved 97% accuracy and 96% recall. However, communication overhead remained a limitation.

Research Gap

To build a secure, scalable, and privacy-preserving federated fraud detection model for the distributed rural financial domain. The RMSE was found to be too high, computation was complex, scaling was difficult, and no large distributed financial dataset was used to validate [7]. Encryption overhead was one of the major issues. Similarly, prior approaches exhibit, complex computation reliance on cloud infrastructure, scalability restrictions, and difficulties in achieving large-scale distributed deployment [8].

The previous methods had computational overhead, poor scalability, communication costs, encryption delay, class-imbalance, resource-hunger, and installation problems, which resulted in low efficiency, poor adaptability, and inconsistent performance in distributed financial systems.

To overcome these limitations, this research proposed the PBA-FederatedRNN model, which combined federated learning, lightweight optimization, secure aggregation, and SMOTE-based imbalance handling to enable safe, scalable, and effective fraud detection in dispersed rural financial environments. It lowered computation, communication complexity and increases scalability, enabling efficient privacy preservation and better detection performance for diverse financial data.

METHODOLOGY

For reliable fraud detection in distributed rural financial environments, transaction data was processed using SMOTE for class imbalance handling. In the proposed PBA-FederatedRNN model, RNN was used for sequential transaction learning, PBA for parameter optimization, and federated learning for secure, privacy-preserving collaborative model training across multiple financial nodes. The proposed PBA-FederatedRNN model's general workflow is depicted in Figure 1.

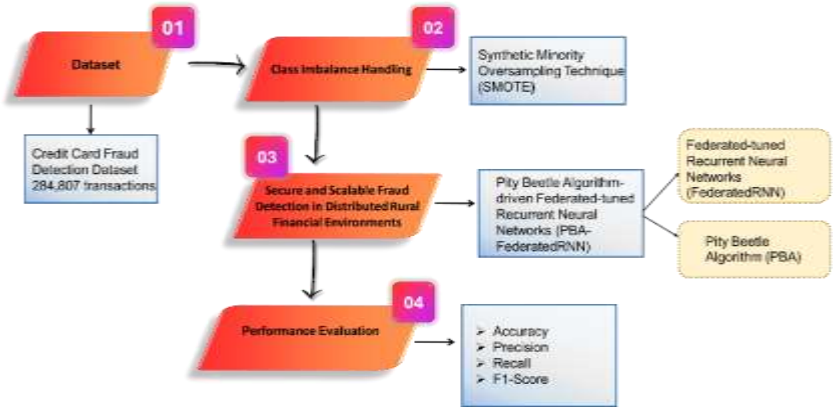

Figure 1. Process of the Proposed PBA-Federated RNN Model for Fraud Detection in Distributed Rural Financial Environments

Dataset Collection

The CCFD Dataset is a collection of anonymized financial transaction records obtained from publicly accessible resources (Kaggle) (https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud). It contains 284,807 financial transactions, containing 492 fraudulent transactions that were used for evaluation. The legal and fraudulent classes are extremely unbalanced. The dataset is extensively utilised for research on fraud detection in secure financial contexts using machine learning, deep learning, and federated learning.

SMOTE for Class Imbalance Handling in Federated Fraud Detection

The proposed PBA-FederatedRNN model is designed to address the type imbalances issue in credit card fraud detection datasets. By interpolating between real minority occurrences, SMOTE generates fake samples of the minority class (fraud cases), as fraudulent transactions are far less frequent than regular transactions. By doing this, the dataset is balanced without losing crucial data from the majority class. By distributing data more evenly among dispersed rural finance nodes, SMOTE enhances model training stability in the suggested federated learning context. As a result, fraud patterns are better learned, recall rates are higher, bias toward majority class transactions is decreased, and overall detection performance in privacy-preserving financial systems is increased.

A-FederatedRNN for Secure and Scalable Fraud Detection in Distributed Rural Financial Environments

The proposed PBA-FederatedRNN model has successfully identified the fraud of financial transaction in distributed rural financial environment by combining RNN and Pity Beetle Algorithm in Federated Learning scheme. RNN captures the dynamic behavior of the sequence transaction, the temporal characteristics and hidden fraudulent patterns without much human engineered features; while PBA tune the parameters to gain better convergence and better classification results. Federated Learning does secure collaborative training with multiple financial nodes without transmitting the raw data, and protecting the privacy of data. With this method, it achieves an efficient, powerful and correct fraud detection and better generalization.

Federated Learning for Secure and Privacy-Preserving Collaborative Fraud Detection

Federated Learning (FL) was a kind of distributed learning that allows many different financial institutions to train the whole country's fraud detection model without directly exposing the customers' transaction details to the other institutions. Every rural financial node in the proposed PBA-FederatedRNN paradigm uses its own transaction data to train the Recurrent Neural Network model locally, and it only sends the encrypted model update to the federated server, where a secure global model is created by averaging all received model modifications and sending it to every node. It not only protects user privacy but also cuts down communication cost, increases system scalability and reliability, and tolerates heterogeneous environments while improving fraud detection accuracy on a distributed rural financial system.

RNN-Based Fraud Pattern Detection

To analyze sequential transaction behavior and detect fraudulent financial activities in distributed rural environments, RNN is employed. RNN is capable of learning temporal dependency and behavioral patterns from stream transactions. Through this, it can detect abnormal behaviors that indicate fraudulent transactions, such as unusually high frequency of transactions, unexpected large amounts of money

transfer, and spending abnormalities. In the proposed model, the RNN is locally trained on the federated client by using the user's private transaction information, It improves user privacy protection while also assisting in reaching a high rate. The behavior on sequential transaction data is used in the hidden layers of the RNN model to learn the time-varying patterns of fraud, hence improving the fraud detection rate in a distributed environment. $W = (w_1, w_2, \ldots, w_m)$ is the input vector sequence. With $m = 1$ to M, a conventional RNN computes the hidden vector sequence $G = (G_{11}, G_{12}, \ldots, G_m)$ and output vector sequence $Z = (Z_1, Z_2, \ldots, Z_m)$ as shown in Eqs. (1) and (2). Two hidden layers make up the basic RNN architecture shown in Figure 2.

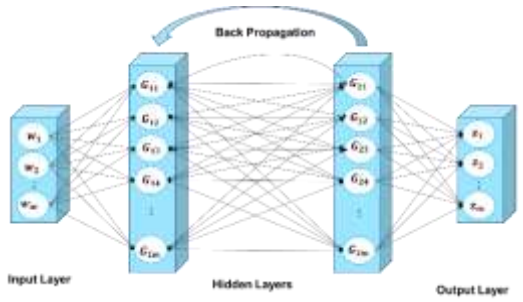

Figure 2. Fraud Detection Using a Basic RNN Architecture with Two Hidden Layers

$$h_t = \sigma(W_{xh}x_t + W_{hh}h_{t-1} + b_h) \quad (1)$$

$$y_t = W_{hy}h_t + b_y \quad (2)$$

Where h_t is the hidden state capturing fraud-related sequential transaction behavior at time t, σ is the activation function used for non-linear fraud pattern learning, W_{xh} is the weights between input financial features and the hidden layer. x_t is the input transaction data at time t, W_{hh} is the recurrent weights connecting previous and current hidden states, $and\ h_{t-1}$ is the previous hidden state representing past transaction behavior. b_h is the bias of the hidden layer, y_t is the output prediction indicating fraud or a normal transaction W_{hy}. The weights from the hidden layer to the output layer and b_y is the output bias term.

RNNs learn sequential financial transaction patterns through gradient-based learning techniques like Backpropagation Through Time (BPTT). However, basic RNNs may face the vanishing gradient problem while learning long-term financial transaction patterns, leading to slow convergence of the model to the fraud patterns and inefficiency in distributed financial transactions learning environments.

The federated learning model utilizing RNN achieved effective sequential transaction behaviors, enhanced fraud detection, maintained data privacy in a distributed rural environment, and detected time anomalies, with vanishing gradient limitations for learning long sequences.

PBA-Based Model Optimization for Fraud Detection

To optimize model parameters for robust and cost-effective fraud detection in rural distributed financial settings. It simulates the characteristics of a beetle, such as search, aggregate, and anti-aggregate, for exploring optimal solutions and exploitation. PBA initializes a set of initial populations in a random way, followed by using deterministic and memory-based search for parameter optimization. It helps to reduce the convergence rate, cost of computation, avoid local optimum, and achieve better accuracy, scalability, and privacy-based federated fraud detection performance.

Searching Strategies: It explores optimal model parameters using deterministic area search and memory-based search. It enhances fraud detection by efficiently balancing exploration and exploitation, improving convergence, reducing computation cost, and adapting to heterogeneous distributed financial data while preserving privacy in federated environments in Eq. (3)

$$MEM = \left[\frac{w_{1,1}}{w_{2,1} \vdots w_{Dim,1}} \frac{w_{1,2}}{w_{2,2} \vdots w_{Dim,2}} \frac{\cdots}{\cdots \ddots \cdots} \frac{w_{1,Mpop}}{w_{2,Mpop} \vdots w_{Dim,Mpop}}\right] \quad (3)$$

Where MEM represents the memory matrix storing the best optimized fraud detection model parameters from previous federated iterations, $w_{i,j}$denotes the optimized weight value of the i^{th} parameter in the j^{th} candidate solution, w_{Dim} indicates the total number of model parameters or feature dimensions, and M_{pop} represents the total number of candidate solutions maintained for optimization during federated fraud detection training. i is the index representing the parameter dimension, j is the index representing the candidate solution in the optimization population, and $[w_{1,1}, w_{2,1}, \ldots, w_{Dim,1}]$ and $[w_{1,1}, w_{2,1}, \ldots, w_{Dim,2}]$ represents the complete optimized parameter vector of the first and second fraud detection candidate solution stored in the memory matrix.

Update Strategy: It retains only the best-performing global and local model parameters from federated clients, discarding suboptimal updates to improve efficiency. This results in quick convergence, low communication costs and higher accuracy in detecting fraud while maintaining privacy in a distributed rural financial environment as given in Eq. (4).

$$x_{t+1} = \{pioneer_t, if\ f(pioneer_t) < f(x_{new})\ x_{new}, \qquad otherwise \quad (4)$$

Where x_{t+1} is the updated model solution, $pioneer_t$ is the best-performing solution at iteration t, $and\ x_{new}$ is the newly generated candidate solution from PBA search. $f(\cdot)$ is the fitness function measuring fraud detection performance, $f(pioneer_t)$ is the fitness value of the best current model, and $f(x_{new})$ is the fitness value of the newly generated model update.

The proposed PBA-FederatedRNN model effectively achieved secure, scalable, and privacy-preserving fraud detection in distributed rural financial environments by combining federated learning, RNN-based sequential behavior analysis, and PBA-based optimization. It improved detection accuracy, reduced communication and computational overhead, enhanced convergence speed, handled heterogeneous and imbalanced data efficiently, and maintained strong data privacy while identifying fraudulent transaction patterns in financial systems.

RESULT

For the purpose of reliable evaluation of the Proposed PBA-Federated RNN-based fraud detection model, the dataset was split into 70% training set and 30% testing set. All experiments were developed using the Python deep learning framework and in a federated simulation environment in a way that facilitates privacy-preserving financial analytics. The model was trained across several rural financial nodes using federated learning, which eliminates the need to transmit the actual transaction data. Table 1 displays the configuration of the proposed model.

Table 1: Experimental Setup and System Configuration

Component	Configuration
Programming Language	Python 3.10
Machine Learning Libraries	Scikit-learn, NumPy, Pandas
Operating System	Windows 11 (64-bit)
Processor	Intel Core i9
RAM	64 GB
GPU	NVIDIA RTX Series
Development Environment	Anaconda, Jupyter Notebook
Deep Learning Framework	TensorFlow

The proposed PBA-FederatedRNN model performed well on fraud classification with better privacy preservation, robustness, and flexibility on distributed finance systems.

Evaluation Metrics

Metrics such as F1-score, Precision, Recall and Accuracy were used to empirically show how well the constructed PBA-FederatedRNN model performed in detecting credit card fraud in scattered rural financial settings.

F1-score: evaluates a compromise between recall and precision to produce dependable fraud categorization performance. **Precision:** Is the proportion of fraud transactions which are fraud that are also fraud. This is a control over the false positives. **Accuracy:** The percentage is calculated on all of the transactions that are flagged either fraudulent or not, but correctly classified, showing how well the model performed in general. **Recall:** Checks the model for its accuracy in detecting genuine frauds: it will test the accuracy of fraud capture by the model.

Comparative Analysis

According to the performance, when detecting the credit card fraud, the proposed PBA-FederatedRNN model could achieve better performance than all existing machine learning and federated learning methods. The suggested PBA-FederatedRNN model, FED-SPFD [11], and CCFD framework [12] are trained by Credit Card Fraud Detection Dataset. The suggested model can provide trustworthy, scalable, and robust credit card fraud detection results within the distributed finance world. The performance comparison between FED-SPFD and CCFD framework and the proposed PBA-FederatedRNN model are showed in Table 2, where the evaluation has been conducted under the federated learning condition for a fair comparison.

Table 2: Performance Comparison of Federated Learning-Based Fraud Detection Models

Methods	Metrics(%)			
	Accuracy	Precision	Recall	F1-Score
FED-SPFD	95.3	89.7	73.6	80.9
CCFD Framework	97.0	97.0	96.0	97.0
PBA-FederatedRNN [Proposed]	98.7	98.2	97.8	98.0

This indicates that the proposed model achieves optimal fraud detection results in distributed rural financial environments, achieving an overall accuracy, recall, F1-score, and precision of 98.7%, 97.8%, 98.0%, and 98.2% respectively. Figure 3 illustrates the comparison of the proposed PBA-FederatedRNN model and existing models on the basis of the different fraud detection performance metrics.

European Journal of Computer Science and Information Technology, 14(3), 42-53, 2026
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

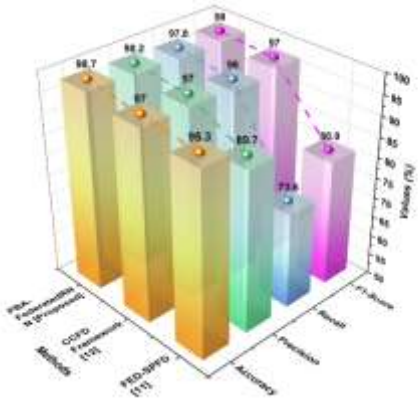

Figure 3. Comparative Analysis of Fraud Detection Performance Metrics

The proposed PBA-FederatedRNN model showed higher and better accuracy, precision, recall and F1 score compared to others and was secure, scalable and efficient for the distributed rural financial surroundings.

DISCUSSION

The objective is to provide a federated fraud detection model for remote rural financial settings that is safe, scalable, and privacy-preserving. The drawbacks of FED-SPFD systems are computation complexity, communication expense, lack of robustness to heterogeneity of data, lack of scalability and higher consumption if using federated feature alignment and privacy preservation techniques [11]. CCFD framework's weaknesses are the communication cost, latency in blockchain, high resource requirement for computation, scalability challenges, dependencies on cloud-fog infrastructure, and escalated complexity during federated collaborative learning [12].

The proposed PBA-FederatedRNN overcomes these shortcomings by applying lightweight optimization, adaptive federated learning, secure aggregation, and SMOTE-based balancing, which lowers the computational complexity and communication costs, improves stable training, and also enhances scalability, privacy, and fraud detection accuracy for a distributed rural financial environment.

CONCLUSION

The PBA-FederatedRNN method can be used to detect credit card fraud in distributed rural financial scenarios with the help of federated learning (FL) for privacy, RNN for analyzing sequential transaction behavior, and PBA for optimizing parameters. The PBA-FederatedRNN can take advantage of the temporal nature of transaction data and abnormal patterns like abnormal expenditure, high-speed transactions, fraudulent anomalies, and others. It acquired 98.7% Accuracy, 98.2% Precision, 97.8%

Recall, and 98.0% F1-Score, respectively, which outperforms the existing federated and deep learning approaches in many criteria, such as low communication overhead, scalability, and strong privacy.

However, the model also suffers from disadvantages, such as the sensitivity to severely unbalanced data, computational complexity of training in a federated setting and the inability of dynamic fraud patterns in different financial environments. For future work, enhancements can focus on real-time edge deployment, improved imbalance handling techniques, and stronger adaptability to evolving fraud strategies across large-scale financial systems.

REFERENCES

1. Jithish, J., Alangot, B., Mahalingam, N., and Yeo, K.S., 2023. Distributed anomaly detection in smart grids: a federated learning-based approach. *IEEE Access*, *11*, pp.7157-7179. 10.1109/ACCESS.2023.3237554
2. Tang, Y. and Liu, Z., 2024. A credit card fraud detection algorithm based on SDT and federated learning. *IEEE Access*, *12*, pp.182547-182560. https://doi.org/10.1109/ACCESS.2024.3491175
3. Lakhan, A., Mohammed, M.A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., Alkhayyat, A., and Wang, W., 2022. Federated-learning-based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. *IEEE Journal of Biomedical and Health Informatics*, *27*(2), pp.664-672. https://doi.org/10.1109/JBHI.2022.3165945
4. Abbassi, H., El Mendili, S., and Gahi, Y., 2025. Adaptive, Privacy-Enhanced Real-Time Fraud Detection in Banking Networks Through Federated Learning and VAE-QLSTM Fusion. *Big Data and Cognitive Computing*, *9*(7), p.185. https://doi.org/10.3390/bdcc9070185
5. Awosika, T., Shukla, R.M., and Pranggono, B., 2024. Transparency and privacy: the role of explainable AI and federated learning in financial fraud detection. *IEEE Access*, *12*, pp.64551-64560. https://doi.org/10.1109/ACCESS.2024.3394528
6. Rabbani, H., Shahid, M.F., Khanzada, T.J.S., Siddiqui, S., Jamjoom, M.M., Ashari, R.B., Ullah, Z., Mukati, M.U., and Nooruddin, M., 2024. Enhancing security in financial transactions: a novel blockchain-based federated learning framework for detecting counterfeit data in fintech. *PeerJ Computer Science*, *10*, p.e2280. https://doi.org/10.7717/peerj-cs.2280
7. Reddy, V.V.K., Reddy, R.V.K., Munaga, M.S.K., Karnam, B., Maddila, S.K., and Kolli, C.S., 2024. Deep learning-based credit card fraud detection in federated learning. *Expert Systems with Applications*, *255*, p.124493. https://doi.org/10.1016/j.eswa.2024.124493
8. Sivasundaram, M., Selvam, M., Venkatachalam, P. and Rajasekaran, R.T., 2026. Adaptive secure federated cloud framework for high-accuracy fraud detection in financial systems. *Automatika*, *67*(1), pp.452-466. https://doi.org/10.1080/00051144.2026.2668191
9. Xia, Z. and Saha, S.C., 2025. Fingraphfl: Financial graph-based federated learning for enhanced credit card fraud detection. *Mathematics*, *13*(9), p.1396. https://doi.org/10.3390/math13091396

10. AbouGrad, H. and Sankuru, L., 2025. Online banking fraud detection model: Decentralized machine learning framework to enhance effectiveness and compliance with data privacy regulations. *Mathematics*, *13*(13), p.2110. https://doi.org/10.3390/math13132110
11. Chen, Y., Zhang, K., Zhu, H., and Qiu, Z., 2025. A Novel Federated Transfer Learning Framework for Credit Card Fraud Detection Under Heterogeneous Data Conditions. *Risks*, *13*(11), p.208. https://doi.org/10.3390/risks13110208
12. Baabdullah, T., Alzahrani, A., Rawat, D.B., and Liu, C., 2024. Efficiency of federated learning and blockchain in preserving privacy and enhancing the performance of credit card fraud detection (CCFD) systems. *Future Internet*, *16*(6), p.196. https://doi.org/10.3390/fi16060196