

# Federated Learning-Based Credit Card Fraud Detection: Performance Analysis with Sampling Methods and Deep Learning Algorithms

Fatima Muhair Alketbi<sup>1</sup>, Fatih Kurugollu<sup>1</sup>, Sebti Foufou<sup>1</sup>, Isam Mashhour Al Jawarneh<sup>1</sup>

<sup>1</sup> Department of Computer Science, University of Sharjah, Sharjah P. O. Box 27272, United Arab Emirates  
U24102845@sharjah.ac.ae, fkurugollu@sharjah.ac.ae, sfoufou@sharjah.ac.ae, ijawarneh@sharjah.ac.ae

**Abstract**—Credit card fraud detection requires solutions that are accurate and also preserve privacy, given the sensitivity of financial data. This study investigates the degree to which deep learning models Convolutional Neural Network (CNN), Multi-Layer Perceptron (MLP), and Long Short-Term Memory (LSTM) perform throughout three learning frameworks Federated Learning (FL), Split Learning (SL), and Regular Learning (RL). Four sampling approaches are used to mitigate class imbalance: SMOTE, Random Over Sampling (ROS), Random Under Sampling (RUS), and NearMiss Under-sampling (NMU). Although accuracy, precision, and recall are conventional assessment measures, the Area Under the Receiver Operating Characteristic Curve (AUC-ROC) functions as the primary performance metric. FL and RL robustness was further assessed by simulations of clients that are noisy. Experimental findings indicate that FL surpasses RL, demonstrating enhanced stability under certain adversarial scenarios. AUC-ROC performance is additionally exceeded by the proposed FL model, in comparison to the Federated SDT model upon the same dataset. This research advances the development of privacy-preserving and robust fraud detection systems, facilitating future enhancements in decentralized machine learning frameworks.

**Keywords**—Credit card fraud, fraud detection system, federated learning, CNN, MLP, LSTM

## I. INTRODUCTION

Credit card fraud is a significant financial risk, requiring sophisticated detection techniques that provide both accuracy and data privacy. Traditional rule-based techniques are simple, but lack adaptability to evolving fraud, which leads to high false positive rates, causing inefficiencies, thereby necessitating the adoption of artificial intelligence (AI)-driven solutions[1]. Federated learning (FL) provides a privacy-preserving solution, allowing several institutions to collaboratively train a unified model without disclosing raw data [2]. This methodology conforms to data protection regulations, including GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act), enhancing its compliance for practical use in financial systems.

Federated learning enhances fraud detection by tackling challenges associated with data protection, regulatory adherence, and cooperative learning. However, issues such as class imbalance, concept drift, and adversarial assaults need more optimization. The integration of federated learning with deep learning models (such as LSTM and autoencoders) and

sampling techniques (like SMOTE and Approx-SMOTE) improves the effectiveness of fraud detection.

Building upon the framework proposed by Aurna et al. [3], this work introduces two key contributions. First, an AUC-ROC evaluation was integrated into the model assessment process to address limitations associated with relying solely on accuracy and recall, particularly under conditions of severe data imbalance. The addition of AUC-ROC score calculation and curve visualization provide a more reliable and comprehensive evaluation of model performance. Second, a robustness analysis was conducted by simulating noisy and malicious clients during federated learning rounds. This extension allows for an investigation of model resilience and performance degradation under adversarial conditions, offering practical insights into the reliability of the federated learning framework in real-world deployment scenarios.

The remaining parts of the paper are organized as follows: Section II explores recent research relevant to our topic. Section III discusses the methodology and experimental procedure. Section IV comprehensively illustrates the findings and analysis, taking into account multiple aspects. Section V presents the discussion and future directions of this study. The conclusion of the study is presented in Section VI.

## II. LITERATURE REVIEW

This section examines key research contributions in federated learning for fraud detection, emphasizing methods that improve data privacy, detection accuracy, management of class imbalance, scalability, explainability, and security. The studies examine deep learning architectures, sampling methodologies, privacy-preserving mechanisms, blockchain integration, and optimization strategies to enhance fraud detection in diverse financial sectors, such as credit card transactions, telecommunications, insurance claims, and cryptocurrency fraud.

Several studies have explored the use of federated learning (FL) to improve fraud detection while preserving data privacy across financial institutions. Paper [3] evaluates three deep learning architectures—Convolutional Neural Network (CNN), Multi-Layer Perceptron (MLP), and Long Short-Term Memory (LSTM)—in the context of the federated learning framework. Four unique sampling approaches are examined to mitigate data imbalance. The experimental results demonstrate high detection rates of 99.51% for CNN, 98.77% for MLP, and 98.20% for LSTM models [3]. This paper utilizes a dataset of credit card transactions conducted by

European cardholders. The dataset is publicly available on Kaggle and comprises transactions from September 2013 over two days. The dataset comprises 284,807 transaction samples, of which just 492 (0.172%) are fraudulent, making it highly imbalanced. Another research study integrated Approx-SMOTE with FL to tackle data imbalance [4]. The suggested framework enhances processing speed by about 30-fold without compromising performance, while simultaneously improving the privacy and security of the information system. Furthermore, it allocates room for future use of the system to accommodate data growth across several banks. It utilizes two public datasets for its experiments: ECC Dataset (European Credit Card dataset) and RA Dataset (Real-world Anonymous dataset). These datasets are used to evaluate the proposed framework in terms of accuracy, recall, precision, and F1-score. The AFLCS method outperforms previous approaches like FFD (Federated Learning for Fraud Detection) and traditional fraud detection systems, improving AUC by 2.71% in the ECC dataset and by 7% in the RA dataset over FlowScope, a prior model. [5] introduces a FedAvg-DWA algorithm (Federated Averaging with Distance-based Weighted Aggregation). This technique accounts for the weight of small class samples and introduces innovations in the model distance aspect of the aggregation strategy. The experiment had positive results, presenting a novel approach to addressing the issue of class imbalance. The paper uses the Credit Card Fraud Detection dataset from the ULB Machine Learning Group. FedAvg-DWA outperforms FedAvg and FedProx in accuracy and F1-score, balancing fraud detection and false positives. It achieves optimal performance with a fraud sample weight of 10, a learning rate of 0.15, and 2 local training rounds.

Federated learning extends beyond credit card fraud detection, including areas such as telecommunications, insurance, and cryptocurrency fraud. [6] proposes a cloud-native federated learning architecture designed to enhance fraud detection capabilities in telecommunications networks. By leveraging federated learning, the architecture enables collaborative model training across distributed data sources without compromising data privacy. This approach addresses challenges unique to telecom fraud detection, such as data heterogeneity and scalability. The paper uses Call Detail Records (CDRs) from telecom providers to detect roaming fraud, specifically International Revenue Share Fraud (IRSF). The experimental results demonstrate that the proposed architecture effectively detects fraudulent activities while maintaining the privacy and security of user data. The findings indicate that the globally trained model using federated learning enhances the F1-score by up to 23% in comparison to models trained locally [5]. Another research provides a systematic review of integrating blockchain technology with federated learning (FL) to enhance cryptocurrency fraud detection. It highlighted the potential of this integrated approach to improve the accuracy and efficiency of fraud detection systems in the cryptocurrency domain [7]. Paper [8] examined an automated approach to enhance the process of vehicle insurance claim fraud detection within the insurance industry. By leveraging a hybrid model, the authors aim to address challenges associated with data sharing among insurance companies and enhance collaborative efforts in identifying fraudulent claims. The findings show that the suggested hybrid model has an accuracy of 94.47% and that it

may be improved even further by using other nature-inspired algorithms that are only used for fraud detection. The dataset used for their study is a CSV dataset from Kaggle. The dataset is related to insurance fraud claims detection and contains a total of 40 columns with information on policy details, insured individual attributes, claim details, and fraud indicators.

Recent studies that focus on improving FL-based fraud detection by integrating supplementary approaches such as explainable AI (XAI) and blockchain security have been seen in papers [8] and [9]. In [8], a fraud detection mechanism that integrates machine learning (ML) and blockchain technology to enhance security, transparency, and real-time fraud detection in financial transactions. The study leverages Synthetic Minority Over-sampling Technique (SMOTE) to address class imbalance issues in fraud detection datasets. Multiple datasets were used in this study, including: the BankSim dataset (simulated bank transactions) for financial fraud detection, the insurance fraud dataset (Kaggle CSV) for detecting fraudulent insurance claims, and Crypto transaction datasets (Ethereum, credit card, and exchange records) for cryptocurrency fraud detection. The outcomes can be summarized as follows: CatBoost performed best in fraud detection with 99.46% accuracy (financial transactions), federated learning + blockchain improved security and privacy, and Genetic Algorithm + federated learning improved fraud detection in insurance claims (94.47% accuracy). [9] introduces a novel approach using Federated Learning (FL) and Explainable AI (XAI) to address the challenges of detecting fraudulent financial transactions, particularly focusing on data imbalance and privacy concerns. FL enables financial companies to collaboratively train models without revealing sensitive client data, hence maintaining privacy. Simultaneously, XAI ensures that the model's predictions are interpretable by human experts, adding transparency and trust to the system. The dataset is a real financial fraud dataset including 29,042 transactions. Outcomes: 93% accuracy, robust fraud detection, and clarity in AI decision-making processes. Paper [11] introduces FedFusion, an adaptive model fusion approach designed to address feature discrepancies in federated credit card fraud detection. The study tackles challenges arising from heterogeneous data distributions across financial institutions by dynamically adjusting model aggregation strategies. The proposed method improves fraud detection accuracy and convergence speed while maintaining data privacy. The study used three credit card fraud datasets (real and synthetic) and found FedFusion with MLP to be the best model, achieving 99.95% (Client 1), 99.53% (Client 2), and 99.06% (Client 3) accuracy, with a fraud detection rate of up to 99.74%. It outperformed FedAvg and SCAFFOLD, improving fraud detection and model convergence in heterogeneous data environments.

### III. METHODOLOGY

This research aims to enhance the framework proposed by Aurna et al. [3], which provides an approach that is both privacy-preserving and robust for the detection of credit card fraud. The methodology can be summarized in five steps, illustrated in Fig. 1. The credit card data first undergoes preprocessing, followed by the development of three distinct models based on MLP, LSTM, and CNN architectures. To guarantee data privacy, federated learning is

then integrated with the traditional deep learning models. Model validation is conducted through extensive experimentation, and the performance of the proposed models is evaluated against existing state-of-the-art approaches by tracking key metrics, including accuracy, recall, precision, and F1-score. In addition, a new evaluation metric, AUC-ROC, is introduced to provide a more comprehensive assessment of model performance under data imbalance. Furthermore, a noisy client simulation is performed to analyze the robustness of the framework and improve its reliability under adversarial conditions.

#### A. Data Analysis and Preprocessing

The dataset used in this work comprises credit card transactions conducted by European cardholders, publicly accessible in [12]. The transactions took place over two days in September 2013. There are 284,807 transaction examples, of which just 492 are fraudulent. The fraudulent transactions constitute just 0.172% of the whole dataset, indicating a

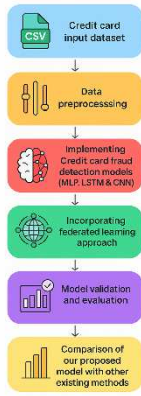


Fig. 1 The summarized workflow of the proposed method.

significant imbalance within the dataset. There are a total of 31 features: ‘Time’, ‘V1’ through ‘V28’, ‘Amount’, and ‘Class’. Features ‘V1’ to ‘V28’ are processed by Principal Component Analysis (PCA) to anonymize sensitive and private information; also, all features have been converted to numeric format. This dataset has been used in other comparable studies, permitting analysis and comparison with current models and benchmarks.

This study involves data preprocessing via three principal steps: resampling, normalization, and reshaping. The dataset used in this study demonstrates considerable imbalance, as seen in Fig. 2. The minority class signifies non-fraudulent data (benign), leading to a considerable probability of a diminished detection rate if the unprocessed data is used without any sampling methodology. Thus, four unique sampling methods are utilized: Random Oversampling (RO), Synthetic Minority

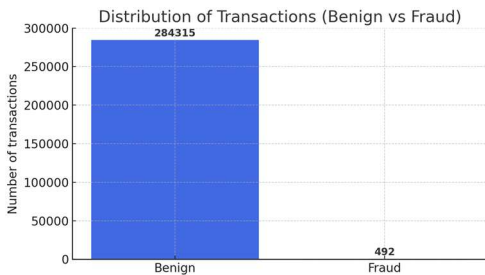


Fig. 2 Distribution of data among two classes (Benign and Fraud).

Oversampling Technique (SMOTE), Random Undersampling (RU), and Near Miss Undersampling (NMU). Following the dataset sampling, it is standardized using StandardScaler. Considering that the features of the credit card dataset are of varying types and exhibit significantly varied distribution ranges, standardization enhances the feasibility of training for machine learning models. The data is reshaped by including an extra dimension to guarantee compatibility with CNN and LSTM models.

#### B. Model Implementation

Three distinct algorithms are used in the experiments: CNN, MLP, and LSTM. These models are developed after extensive experimentation with various hyperparameters via trial and error. Keras Tuner and random search were first used to identify optimum designs. The most optimum candidates are selected for model implementation. The hyperparameter values used for the models are shown in TABLE I [2].

TABLE I. HYPER-PARAMETER VALUES USED IN PROPOSED MODELS[3].

Hyper-parameter	CNN	MLP	LSTM
Input activation function	ReLU	ReLU	ReLU
Output activation function	Sigmoid	Sigmoid	Sigmoid
Optimizer	Adam	Adam	Adam
Initial learning rate	0.0001	0.0001	0.001
Learning rate decay	0.2	0.3	0.2
Dropout rate	0.2, 0.4	0.5	0.5
Communication round	50	50	50
No of federated clients	3	3	2
Train test ratio	80%-20%	80%-20%	80%-20%

The CNN model used for credit card fraud detection has a total of 10 layers, as seen in Fig. 3(a). The architecture has 2 convolutional layers, 3 dropout layers, 2 batch normalization layers, 1 flatten layer, and 2 dense layers, with the first and second convolutional layers using 32 and 64 filters, respectively. This design seems sufficiently practical for this specific situation based on several trials and observations. The MLP model used in our experiment has a total of five layers for credit card fraud detection. As seen in Fig. 3(b), this model has 3 thick layers and 2 dropout layers. The first two thick layers consist of 65 units each, and the dropout rate is set at 0.5, determined via much experimentation and observation. The LSTM model used for credit card fraud detection has five layers: one LSTM layer with 50 units, two dropout layers with a rate of 0.5, and two dense layers, the first containing 65 units. The architecture is seen in Fig. 3(c). All appropriate hyperparameters are selected based on the experimental analysis.

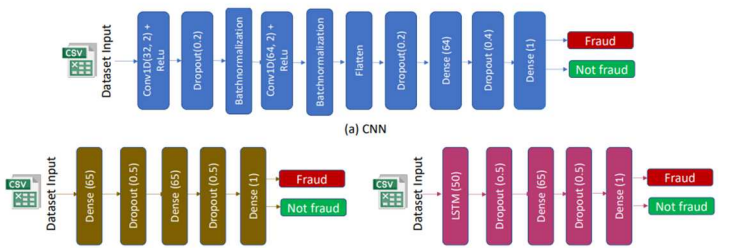


Fig. 3 Architecture of the proposed models (a) CNN model (b) MLP model (c) LSTM model [3].

### C. Federated Learning Integration

The suggested framework aims to thoroughly analyze the performance of all models after integrating them with a federated learning approach. Given that the conventional centralized method fails to ensure data privacy, there has been an increasing integration of federated learning alongside the conventional approach. Federated learning represents a decentralized approach to conventional machine learning. As illustrated in Fig.4, the central server transmits the initial model weights to the clients, where the model undergoes local training on each client. Subsequently, the revised weights are transmitted back to the central server, which consolidates all the model weights through the FedAvg method [13].

Through this process, the global model is refined during each communication round. Our experiments have been carried out with all three models utilizing the FedAvg approach. According to our experiments, 50 communication rounds appeared to be effective in achieving a higher detection rate for each of the models. Observations indicate that for CNN and MLP, the performance was superior with 3 clients, while for LSTM, the optimal performance was achieved with 2 clients. Based on the experimental analysis, a learning rate of 0.0001 has been selected for both CNN and MLP, while the default learning rate of 0.001 is applied for LSTM.

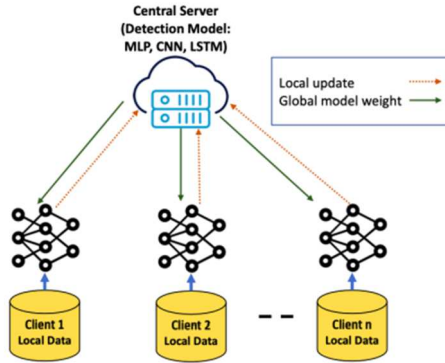


Fig. 4 Typical Federated Learning architecture[2].

## IV. RESULT ANALYSIS

Multiple aspects are addressed in the result analysis of this project. Initially, the AUC-ROC metric is employed to assess the performance of the Regular Learning (RL), Federated Learning (FL), and Split Learning (SL) models in various client configurations. Secondly, noisy client simulations are used to evaluate the resilience of the federated learning architecture and examine how adversarial behavior affects model performance. Lastly, the proposed models are compared to state-of-the-art methods, such as the Federated SDT approach, to verify the efficacy and resilience of the proposed solutions.

### A. Evaluation Metrics

In this study, the primary evaluation metric employed is the Area Under the Receiver Operating Characteristic Curve (AUC-ROC). Given a significant imbalance in credit card fraud datasets, AUC-ROC is a more reliable measure of model performance than raw accuracy. It assesses the trade-off between true positive and false positive rates across different thresholds, offering an extensive perspective on the models' discriminatory capabilities. Additionally, to measure robustness, simulations of noisy clients were implemented

during federated learning rounds to examine the model's resistance to malicious or damaged data inputs.

### B. Experimental Result: Area Under the Receiver Operating Characteristic Curve (AUC-ROC)

Three learning frameworks were implemented and evaluated: Federated Learning (FL): A decentralized training methodology that safeguards privacy by ensuring local client data stays secret. Split Learning (SL): A model partitioning methodology that divides the model across client and server, hence augmenting security. Regular Learning (RL): A traditional centralized model training methodology, functioning as the benchmark. The AUC-ROC performance across different client configurations is summarized in Table II. Fig.5 illustrates the AUC-ROC performance trends for Federated Learning (FL), Split Learning (SL), and Regular Learning (RL) across 50 training rounds and varying client configurations. In Fig. 5(a), FL demonstrates stable improvement as the number of clients increases, with 10 and 16-client setups achieving the highest AUC scores. Fig. 5(b) shows that RL maintains a consistent AUC-ROC value across rounds, but slightly underperforms compared to FL and SL. Fig. 5(c) displays SL's convergence behavior, where higher client configurations yield better performance, matching FL at 16 clients. Finally, Fig. 5(d) presents a comparative bar chart summarizing final AUC-ROC scores across all learning methods and configurations, highlighting that both FL and SL outperform the centralized RL approach, particularly in settings with 10 or more clients.

TABLE II. AUC-ROC PERFORMANCE ACROSS LEARNING

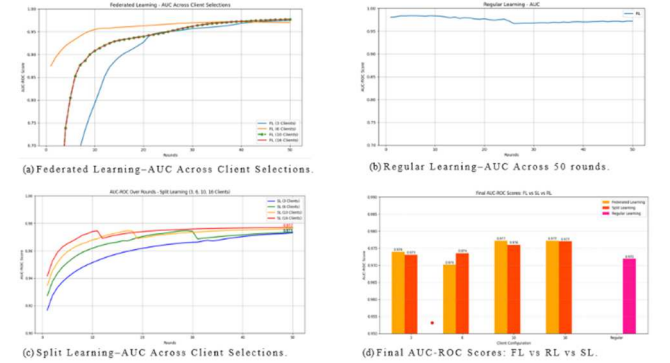


Fig. 5 The AUC-ROC performance trends for Federated Learning (FL), Split Learning (SL), and Regular Learning (RL) across 50 training rounds and varying client configurations.

APPROACHES AND CLIENT CONFIGURATIONS

Number of Clients	Federated Learning (FL)	Split Learning (SL)	Regular Learning (RL)
3	0.974	0.973	—
6	0.970	0.974	—
10	<b>0.977</b>	0.976	—
16	<b>0.977</b>	<b>0.977</b>	—
Centralized	—	—	<b>0.972</b>

### C. Experimental Result: Noisy Client Simulation

To assess robustness, a noisy client simulation was then conducted by means of injecting of corrupted updates into selected clients. In Fig. 6(a), the AUC-ROC scores are depicted for Federated Learning under both clean and also noisy settings across various client configurations. With six and ten clients in FL, the impact of noise was notably minimal

where AUC-ROC dropped by approximately 0.15% as well as approximately  $-0.44\%$ , respectively. However, the performance degraded more with fewer than (3) or more than (16) clients. It went as high as around 9.23% and about 4.27%. Fig. 6(b), by contrast, shows such impact upon Regular Learning (RL) under some noisy conditions, with the AUC-ROC dropping from 0.972 to 0.935 — a 3.81% decrease. These results show just how strong Federated Learning is, particularly in the case when balanced client diversity exists, as it consistently outperforms centralized training even among adversarial noise.

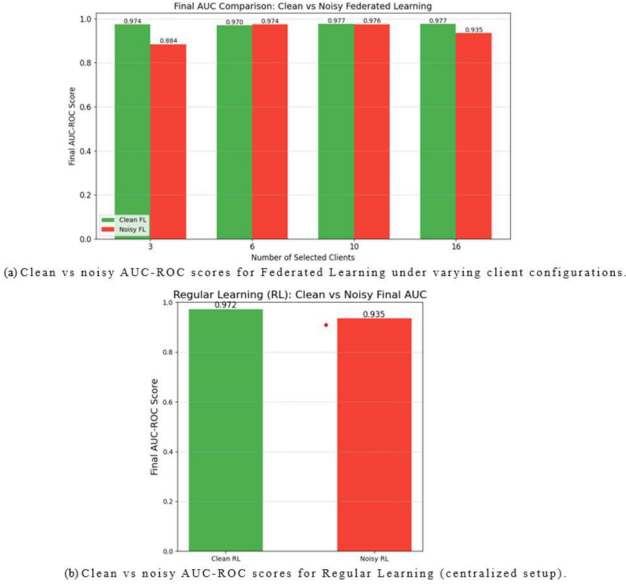


Fig. 6 Impact of noisy client simulation on model performance.

#### D. Comparison with Existing Methods

The proposed model outperformed the Federated SDT[14] model on the same dataset in terms of AUC-ROC score. The proposed Federated Learning (FL) model with 16 clients achieved an AUC-ROC score of 0.977, and the Federated SDT model scored 0.963 on the same dataset, demonstrating superior fraud detection capability. While both models achieved high overall performance, the proposed approach exhibited greater robustness and consistency across varying client configurations. In particular, under simulated noisy client conditions, the proposed model maintained stable AUC-ROC values, whereas the SDT-based model did not evaluate such adversarial scenarios. This highlights the practical reliability of the proposed framework in real-world deployments, where data corruption and malicious inputs may affect learning performance.

#### V. DISCUSSION AND FUTURE DIRECTIONS

The primary objective of this work was to develop a robust and privacy-preserving credit card fraud detection system by addressing three critical challenges of class imbalance, data privacy, and adversarial resilience. A number of sampling techniques were actually applied in order to reduce the class imbalance problem. These techniques included SMOTE, Random Oversampling (ROS), NearMiss Undersampling (NMU), and Random Undersampling of (RUS). These methods improved the distribution of fraud and non-fraud cases during training and enhanced the performance of the classification models.

Three deep learning models—Convolutional Neural Network (CNN), Multi-Layer Perceptron (MLP), and Long Short-Term Memory (LSTM)—were optimized and then implemented via various experiments. Federated Learning (FL), Split Learning (SL), and Regular Learning (RL) are three differing learning frameworks into which the models were integrated. Because of the ways that FL and SL frameworks can preserve data privacy when they train, people particularly stressed them. On account of its level of effectiveness in imbalanced scenarios, the AUC-ROC metric was used for model performance evaluation.

Additionally, the researchers simulated for themselves a noisy client so as to assess the robustness of the models, particularly under both federated and regular learning setups. As the results had demonstrated, FL outperformed both SL and also RL under both clean and noisy conditions. The count of clients had an increase, and yet high AUC-ROC scores were still maintained with the performance degradation being of a minimal level. This preserves privacy via FL, also handling adversarial disruptions effectively. In addition, confirming its reliability as well as practicality for real-world deployment, the proposed FL model achieved better AUC-ROC performance than the Federated SDT model on the same dataset.

Despite the promising results that were found, just a single publicly available dataset limited this study. Various data distributions across many institutions are frequently involved in actual environments. Future work can simulate realistic federated environments to a better degree. Several datasets from clients might be incorporated so as to extend this research. Furthermore, future improvements can explore clients adaptively, techniques aggregate in such an advanced manner, protocols aggregate securely, as well as they can analyze communication costs further in FL and SL frameworks. More scalable, secure, and more reliable fraud detection systems will be able to be built through these enhancements.

#### VI. CONCLUSION

Federated learning presents a good framework for fraud detection with credit cards because it improves privacy in data, ensures compliance to regulations, and enables training collaboratively across institutions that are distributed. Convolutional Neural Networks (CNN), Multi-Layer Perceptron (MLP), and Long Short-Term Memory (LSTM) deep learning models had individual performance evaluated by this project under both federated and centralized learning settings. The evaluation focused in particular on AUC-ROC since fraud datasets are highly imbalanced and it included such key metrics as accuracy, recall, and precision. Federated learning is able to achieve a performance that is comparable to centralized models as demonstrated by some experimental results especially if integrated with proper sampling strategies, and can in some cases exceed them. Whilst FL could greatly preserve data privacy without any compromising of detection effectiveness, researchers further explored several challenges, such as data imbalance as well as adversarial threats, via including noisy client simulations. The proposed FL model was of greater strength and stability as opposed to customary setups. It especially was showing of this at the time when corrupted clients were present. The current study is limited to just one dataset, but even so, the results are promising still. Fraud detection can be done effectively through deep learning in federated learning. Future research into federated systems

should adapt concept drift, interpret models through XAI, aggregate securely, and explore multi-source datasets to strengthen reliability and transparency further. These methodologies can be advanced by federated learning, greatly helping the construction of fraud detection solutions that are secure, scalable, and privacy-preserving.

## References

- [1] R. Yadavalli, R. Poliseti, and R. R. Kurada, "Analysis on AI-based Techniques for Detection of Banking Frauds: Recent Trends, Challenges, and Future Directions," in *2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)*, Jan. 2025, pp. 1–8. doi: 10.1109/ICISCN64258.2025.10934402.
- [2] K. D'souza, S. Puthusseri, and A. G. Samuel, "Scalable Federated Learning for Privacy-Preserving Credit Card Fraud Detection," in *2023 IEEE International Carnahan Conference on Security Technology (ICCST)*, Oct. 2023, pp. 1–6. doi: 10.1109/ICCST59048.2023.10726848.
- [3] N. F. Aurna, M. D. Hossain, Y. Taenaka, and Y. Kadobayashi, "Federated Learning-Based Credit Card Fraud Detection: Performance Analysis with Sampling Methods and Deep Learning Algorithms," in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, Jul. 2023, pp. 180–186. doi: 10.1109/CSR57506.2023.10224978.
- [4] J. Wang, W. Liu, Y. Kou, D. Xiao, X. Wang, and X. Tang, "Approx-SMOTE Federated Learning Credit Card Fraud Detection System," in *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, Jun. 2023, pp. 1370–1375. doi: 10.1109/COMPSAC57700.2023.00208.
- [5] K. Bian and H. Zheng, "FedAvg-DWA: A Novel Algorithm for Enhanced Fraud Detection in Federated Learning Environment," in *2023 4th International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, Aug. 2023, pp. 13–17. doi: 10.1109/ICBAIE59714.2023.10281317.
- [6] S. Talluri, Q. Zhang, and R. Chen, "A Cloud-Native Federated Learning Architecture for Telecom Fraud Detection," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, May 2023, pp. 1–3. doi: 10.1109/NOMS56928.2023.10154302.
- [7] A. A. Ahmed and O. O. Alabi, "Secure and Scalable Blockchain-Based Federated Learning for Cryptocurrency Fraud Detection: A Systematic Review," *IEEE Access*, vol. 12, pp. 102219–102241, 2024, doi: 10.1109/ACCESS.2024.3429205.
- [8] S. Y. N. Victor, G. Srivastava, and T. R. Gadekallu, "A Hybrid Federated Learning Model for Insurance Fraud Detection," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2023, pp. 1516–1522. doi: 10.1109/ICCWorkshops57953.2023.10283682.
- [9] S. Sultana, Md. S. Rahman, and M. Afroj, "An efficient fraud detection mechanism based on machine learning and blockchain technology," in *2023 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Nov. 2023, pp. 162–168. doi: 10.1109/3ICT60104.2023.10391306.
- [10] T. Awosika, R. M. Shukla, and B. Pranggono, "Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection," *IEEE Access*, vol. 12, pp. 64551–64560, 2024, doi: 10.1109/ACCESS.2024.3394528.
- [11] N. Ferdous Aurna, M. Delwar Hossain, L. Khan, Y. Taenaka, and Y. Kadobayashi, "FedFusion: Adaptive Model Fusion for Addressing Feature Discrepancies in Federated Credit Card Fraud Detection," *IEEE Access*, vol. 12, pp. 136962–136978, 2024, doi: 10.1109/ACCESS.2024.3464333.
- [12] "Credit Card Fraud Detection." Accessed: Apr. 28, 2025. [Online]. Available: <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>
- [13] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*, PMLR, 2017, pp. 1273–1282. Accessed: Apr. 28, 2025. [Online]. Available: <https://proceedings.mlr.press/v54/mcmahan17a?ref=https://githubhelp.com>
- [14] Y. Tang and Z. Liu, "A Credit Card Fraud Detection Algorithm Based on SDT and Federated Learning," *IEEE Access*, vol. 12, pp. 182547–182560, 2024, doi: 10.1109/ACCESS.2024.3491175.