A
Project Report Submitted
in Partial Fulfilment of the Requirements
for the Degree of
BACHELOR OF TECHNOLOGY

Under the supervision of

Prof. Prasanta K. Jana

(Professor & IEEE Senior Member)

Department of Computer Science and Engineering
INDIAN INSTITUTE OF TECHNOLOGY
(INDIAN SCHOOL OF MINES)
DHANBAD

By

Avinesh Pratap Singh (20JE0219)
Brijesh Kumar (20JE0279)
Rahul Agrawal (20JE0744)

Table of Contents

Acknowledgements

We would like to express our deepest gratitude to our project supervisor, **Prof. PRASANTA K. JANA.** Your expertise and encouragement were invaluable in shaping the direction and success of this project.

We appreciate the time and effort you invested in reviewing and providing constructive feedback on our work. Your insights have significantly contributed to the improvement of the project and our overall understanding of the subject matter.

Thank you for fostering an environment of learning and for being approachable whenever we sought clarification or assistance. Your mentorship has been instrumental in our academic and professional development.

Certificate

This is to certify that the project report titled **‘Credit Card Fraud Detection using Federated Learning’** submitted by **Avinesh Pratap Singh (20JE0219), Brijesh Kumar (20JE0279) and Rahul Agarwal (20JE0744)** to the Indian Institute of Technology (ISM), Dhanbad towards partial compliance with the requirements for obtaining the bachelor of technology in Computer Science and Engineering title is a record of the good faith work done by them under my Supervision and guidance during the Monsoon Semester (2023-24).

Prof. PRASANTA K. JANA
(Professor & IEEE Senior Member)
Project Guide

DR. Sachin Tripathi
(Associate Professor)
CSE Head of Department

Abstract

This research project addresses the rising challenge of credit card fraud within the digital transformation landscape of the financial sector. Despite advancements in traditional banking systems, the surge in fraudulent credit card transactions poses a significant threat. With billions of dollars reported as losses due to credit card fraud annually, there is a pressing need for an end-to-end solution.

Our approach encompasses the implementation of a robust credit card fraud detection system, leveraging federated learning (FL) techniques, machine learning (Decision Tree, Ensemble Learning) and deep learning models (CNN, MLP, LSTM). The project aims to overcome challenges such as data privacy concerns, data imbalance, and evolving fraud patterns inherent in traditional machine learning (ML) approaches.

Key aspects of the project include:

1. Development of an end-to-end fraud detection system: Ensuring privacy through FL, we aim to create a comprehensive solution that addresses the entire process, from data collection to model deployment.

2. Evaluation of DL and ML models: Decision tree, CNN, MLP, and LSTM models will be evaluated in FL-based approach. This comparative analysis will provide insights into the effectiveness of our proposed solution.

3. Experimentation with various sampling methods: Diversified sampling techniques, including Random Oversampling, Synthetic Minority Oversampling Technique, Random Under sampling, and Near Miss Under sampling, will be explored to enhance detection rates and reduce false positives in the presence of imbalanced datasets.

Problem Statement

The surge in digital transactions and the widespread adoption of cashless systems have led to an alarming increase in credit card fraud within the financial sector. Despite significant advancements in traditional banking systems, the existing approaches to credit card fraud detection grapple with challenges related to data privacy, data imbalance, and evolving fraud patterns. The need of the hour is a comprehensive solution that not only addresses these challenges but optimizes key stages of the fraud detection process.

This research project seeks to develop and optimize a credit card fraud detection system by focusing on three critical steps: data preprocessing, local model selection, and global model selection with an optimized aggregation function. The primary hurdles include the lack of huge, labelled datasets, skewed data distributions, and the dynamic nature of fraud patterns. The research aims to bridge these gaps through rigorous experimentation with various models and algorithms, striving for an optimal and efficient solution that ensures data privacy, tackles data imbalance, and adapts to emerging fraud patterns.

Background & Literature Survey

Credit card fraud detection holds immense financial significance, prompting continuous research efforts [1]-[3] As the landscape of fraudulent activities evolves, there remains a persistent need for advancements in existing methodologies. The following literature review discusses prominent contributions in this field and highlights opportunities for improvement.

Asha et al. [4] proposed a deep learning-based approach utilizing a neural network for fraud detection. Although achieving a commendable 99% accuracy with Artificial Neural Network (ANN), the detection rate stood at 76%. Similarly, Chen et al. [5] introduced a deep neural network, reaching 99% accuracy, yet the crucial metric of detection rate was not adequately addressed. Esenogho et al. [6] employed an ensemble-based approach using LSTM as the base classifier, achieving 99% sensitivity. However, the lack of detailed information on the base LSTM model limits its reproducibility. Fiore et al. [7] tackled data imbalance with a Generative Adversarial Network (GAN) but faced a trade-off, as improved sensitivity came at the cost of a high false positive rate. Varmedja et al. [8] explored various algorithms for fraud detection, highlighting Random Forest's impressive 95.5% accuracy but with a less satisfactory fraud transaction detection rate of 81.63%.

While credit card fraud detection with Federated Learning (FL) is emerging, there's limited literature on the topic. Yang et al. [9] utilized a federated average approach with a CNN as the shared global model, achieving a 10% better AUC score. Zheng et al. [10] employed federated meta-learning with ResNet-34 as the feature extractor and CNN for final classification, showing promise but leaving room for further analysis. Suvarna et al. [11] adopted Encoder and Restricted Boltzmann Machine in a FL setting, prioritizing data privacy over accuracy. However, providing the model architecture could enhance the method's investigatory potential.

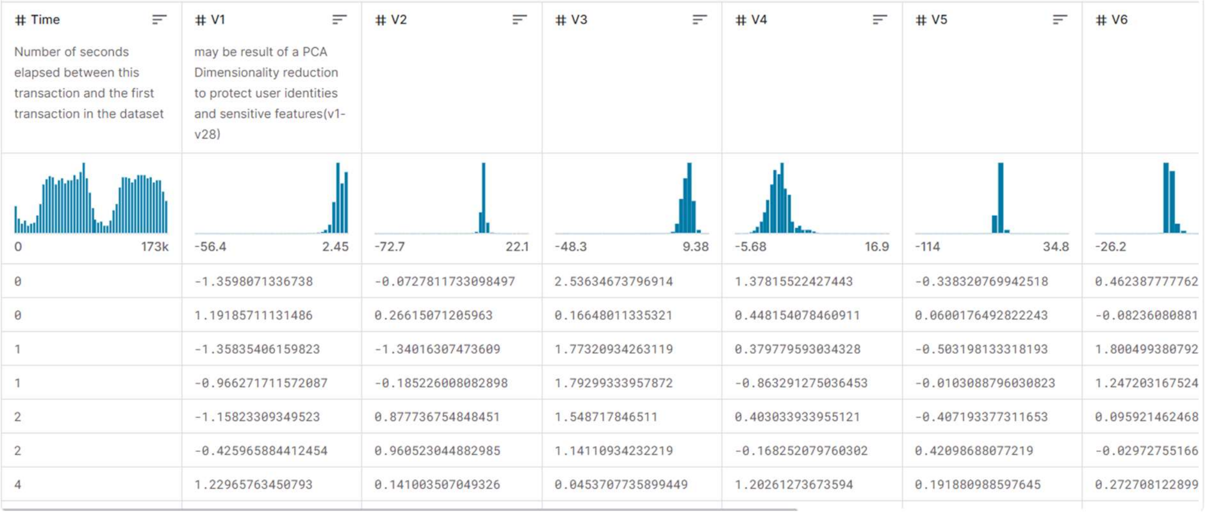
Despite these efforts, issues such as data privacy, detailed investigation of applied models, enhancement of detection rates, and experimentation with data sampling techniques persist in the literature. This work aims to address these gaps comprehensively, offering a holistic and improved approach to credit card fraud detection.

Dataset

The dataset contains transactions made by credit cards in September 2013 by European cardholders.

This dataset presents transactions that occurred in two days, where we have 492 frauds out of 284,807 transactions. The dataset is highly unbalanced, the positive class (frauds) account for 0.172% of all transactions.

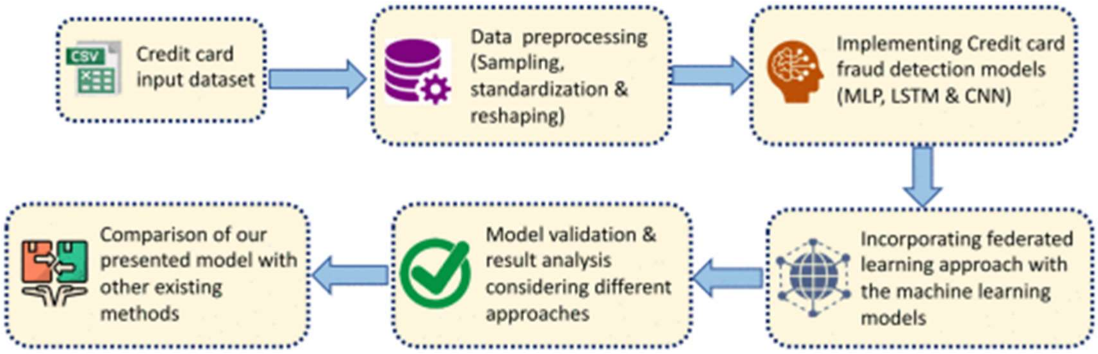
It contains only numerical input variables which are the result of a PCA transformation. Due to confidentiality issues, original features and more background information about the data is not available. Features V1, V2, … V28 are the principal components obtained with PCA, the only features which have not been transformed with PCA are 'Time' and 'Amount'. Feature 'Time' contains the seconds elapsed between each transaction and the first transaction in the dataset. The feature 'Amount' is the transaction Amount, this feature can be used for example-dependant cost-sensitive learning. Feature 'Class' is the response variable, and it takes value 1 in case of fraud and 0 otherwise.



# Time	# V1	# V2	# V3	# V4	# V5	# V6
Number of seconds elapsed between this transaction and the first transaction in the dataset	may be result of a PCA Dimensionality reduction to protect user identities and sensitive features(v1-v28)					
0 173k	-56.4 2.45	-72.7 22.1	-48.3 9.38	-5.68 16.9	-114 34.8	-26.2
0	-1.3598071336738	-0.0727811733098497	2.53634673796914	1.37815522427443	-0.338320769942518	0.462387777762
0	1.19185711131486	0.26615071205963	0.16648011335321	0.448154078460911	0.0600176492822243	-0.08236080881
1	-1.35835406159823	-1.34016307473609	1.77320934263119	0.379779593034328	-0.503198133318193	1.800499380792
1	-0.966271711572087	-0.185226008082898	1.79299333957872	-0.863291275036453	-0.0103088796030823	1.247203167524
2	-1.15823309349523	0.877736754848451	1.548717846511	0.403033933955121	-0.407193377311653	0.095921462468
2	-0.425965884412454	0.960523044882985	1.14110934232219	-0.168252079760302	0.42098688077219	-0.02972755166
4	1.22965763450793	0.141003507049326	0.0453707735899449	1.20261273673594	0.191880988597645	0.272708122899

Methodology

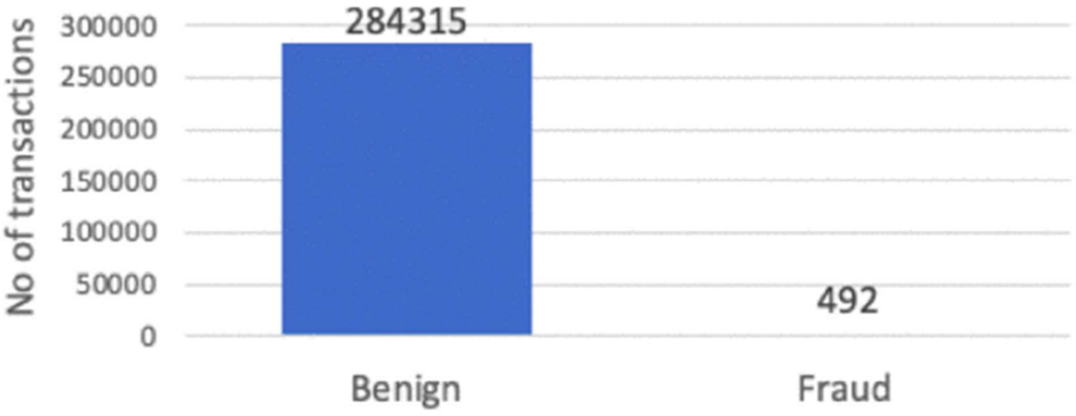
Our objective is to develop and evaluate a robust and privacy-preserving model for credit card fraud detection. The study unfolds in five phases, illustrated in Fig. below. Initially, credit card data undergoes preprocessing, and three distinct models are constructed based on MLP, LSTM, CNN and Random Forest architectures. Subsequently, to safeguard data privacy, we integrate the federated learning approach with these conventional models. Following this, model validation is conducted through various experiments. Finally, we compare our proposed models with recent state-of-the-art alternatives.



Credit card input dataset
CSV
Data preprocessing (Sampling, standardization & reshaping)
Implementing Credit card fraud detection models (MLP, LSTM & CNN)
Incorporating federated learning approach with the machine learning models
Model validation & result analysis considering different approaches
Comparison of our presented model with other existing methods

Dataset Analysis and Preprocessing

The dataset employed consists of credit card transactions by European cardholders, publicly available [12], occurring in September 2013 over two days. With 284,807 transaction samples, only 492 are identified as fraud, constituting 0.172% of the dataset, indicative of its highly imbalanced nature. Comprising 31 features, including 'Time,' 'V1' to 'V28,' 'Amount,' and 'Class,' features 'V1' to 'V28' are PCA-transformed for anonymization. All features are in numeric form.



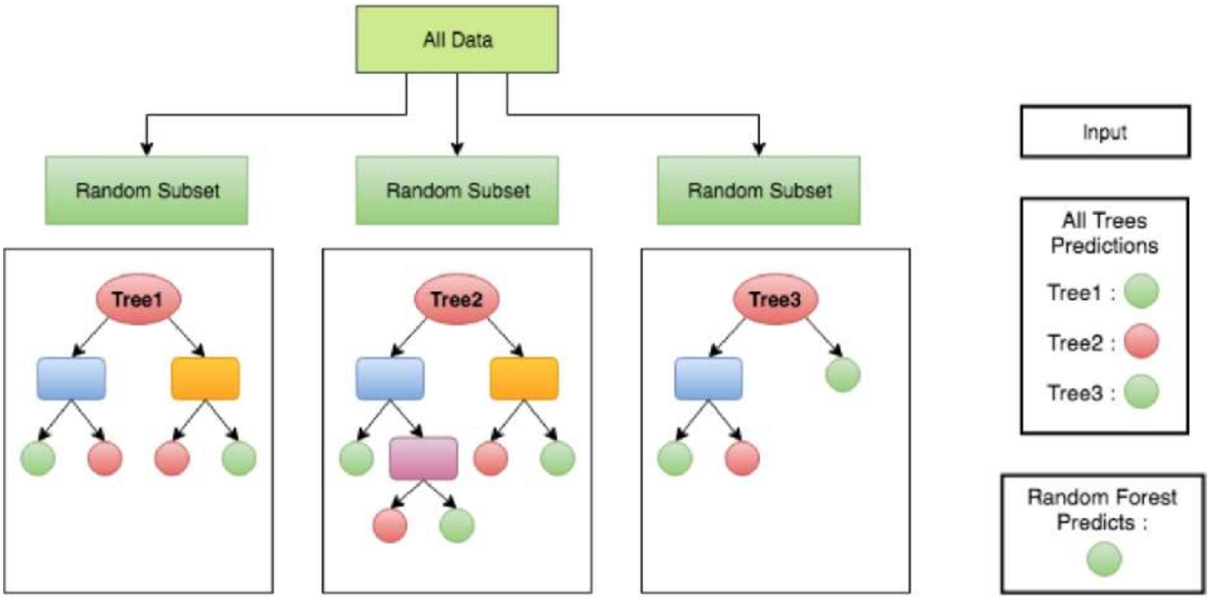
Data preprocessing involves three main steps: resampling, standardization, and reshaping. The imbalanced nature of the dataset is addressed using four sampling methods: Random Oversampling (RO), Synthetic Minority Oversampling Technique (SMOTE), Random Under sampling (RU), and Near Miss Under sampling (NMU). Post-sampling, the dataset is standardized using StandardScaler, enhancing compatibility with machine learning models by aligning feature distributions. Additionally, data reshaping, involving the addition of an extra dimension, ensures compatibility with CNN and LSTM models.

Machine Learning & Deep Learning Algorithms

Random Forest in machine learning and three algorithms—CNN, MLP, and LSTM in deep learning—are employed for experiments following extensive trial and error sessions involving different hyperparameters. Keras tuner and random search were initially utilized to explore optimal architectures, and the most effective configurations were selected for implementation.

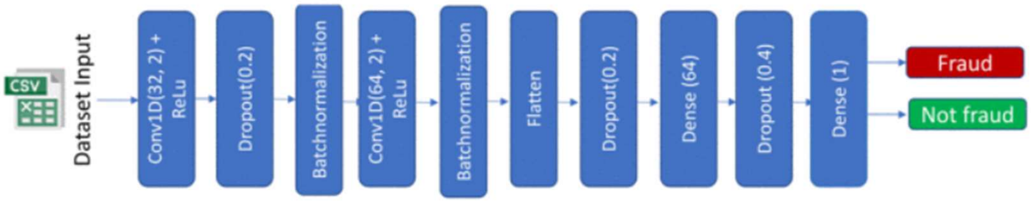
1) Random Forest for Credit Card Fraud Detection:

Random Forest for Credit Card Fraud Detection employs an ensemble learning approach, comprising multiple decision trees. During training, each tree is constructed using a random subset of the credit card transaction data and a random subset of features, introducing diversity among the trees. This ensemble of trees collectively makes predictions, and the final decision is determined by a majority vote. The strength of Random Forest lies in its ability to mitigate overfitting and enhance generalization by leveraging the diverse perspectives of individual trees. In the context of credit card fraud detection, this method offers a robust and effective means of identifying fraudulent transactions by leveraging the collective wisdom of multiple decision trees.



2) CNN for Credit Card Fraud Detection:

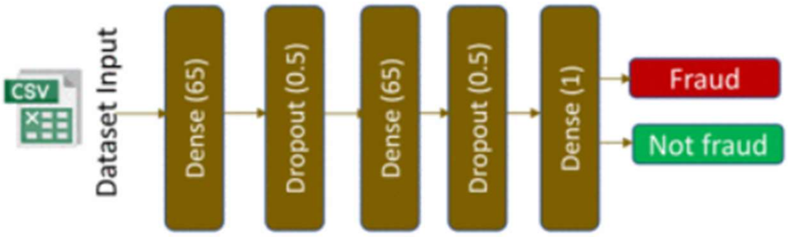
Applying Convolutional Neural Networks (CNN) to credit card fraud detection involves leveraging deep learning techniques tailored for image and sequence data to identify patterns indicative of fraudulent transactions. The CNN model for this task typically comprises layers designed to extract hierarchical features from the transaction data. This may include convolutional layers for feature extraction, pooling layers for down-sampling, and fully connected layers for classification. The unique architecture of CNNs allows them to automatically learn relevant features from the raw transaction data, making them well-suited for the complex patterns associated with credit card fraud. The model is trained using labelled data, and its ability to capture intricate relationships within the transaction features enables it to discern between legitimate and fraudulent activities, making CNNs a potent tool in the realm of credit card fraud detection.



(a) CNN

3) MLP for Credit Card Fraud Detection:

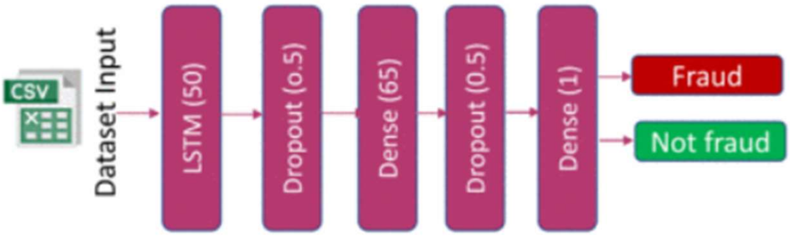
Utilizing Multilayer Perceptron (MLP) for credit card fraud detection involves deploying a neural network architecture designed to handle complex relationships within the transactional data. The MLP model typically consists of multiple layers, including input, hidden, and output layers. During training, the model learns the intricate patterns and relationships in the credit card transaction features, making it adept at distinguishing between genuine and fraudulent transactions. The hidden layers serve as nonlinear mapping functions, enabling the network to capture and understand the underlying structures in the data. The flexibility and expressive power of MLPs make them suitable for tasks like credit card fraud detection, where the detection of subtle patterns is crucial. Through iterative learning and fine-tuning of weights, MLPs contribute significantly to the identification of fraudulent activities in credit card transactions.



(b) MLP

4) LSTM for Credit Card Fraud Detection:

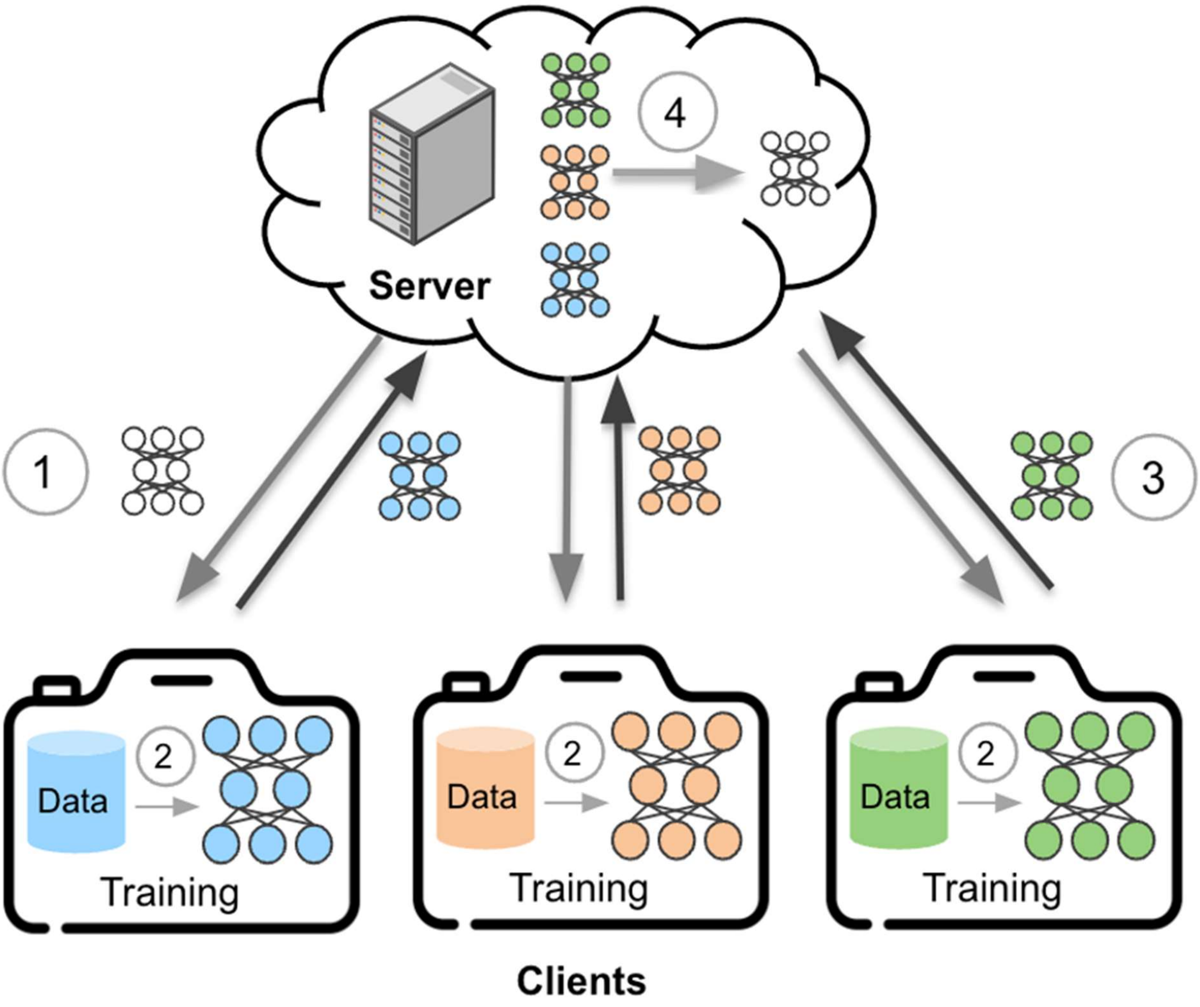
Implementing Long Short-Term Memory (LSTM) for credit card fraud detection involves leveraging recurrent neural network (RNN) architecture, specifically designed to handle sequential data. LSTMs excel in capturing long-term dependencies, making them well-suited for the dynamic nature of credit card transactions. The model typically consists of memory cells and gates that regulate information flow, allowing it to selectively remember or forget patterns over extended sequences. In the context of fraud detection, LSTMs can effectively capture evolving patterns and detect anomalies by learning from the sequential nature of transaction data. The ability to retain information over extended periods equips LSTMs to identify subtle deviations indicative of fraudulent activities. Through training on historical transaction sequences, LSTM models can contribute to robust and accurate credit card fraud detection, particularly in scenarios where temporal dependencies play a crucial role.



(c) LSTM

Incorporating Federated Learning:

This study places a pivotal emphasis on assessing the performance of all models through the integration of the federated learning approach. Addressing the privacy limitations inherent in conventional centralized methods, federated learning is seamlessly amalgamated into the existing framework.



With Deep Learning Algorithm:

Federated learning, exemplified in previous Fig., operates as a decentralized variant of traditional machine learning. The central server initiates the process by disseminating initial model weights to individual clients. Each client then independently trains its model locally on its respective dataset. Updated weights are subsequently transmitted back to the central server, where the FedAvg aggregation method harmonizes all individual model weights. This iterative process refines the global model across communication rounds. Experiments incorporating the FedAvg approach are conducted with the CNN, MLP, LSTM.

With Ensemble Learning:

Incorporating Random Forest into federated learning for credit card fraud detection involves extending the federated approach to ensemble learning. The central server initiates the process by distributing initial Random Forest model weights to individual clients. Clients independently train the Random Forest locally on their distinct subsets of credit card transactions. After local training, the central server aggregates the updated decision trees through ensemble techniques, forming the refined global model. This iterative process ensures collaborative model improvement across clients while preserving data privacy. The ensemble nature of Random Forest enhances the fraud detection system's accuracy and robustness, making it effective in discerning fraudulent transactions while mitigating privacy concerns.

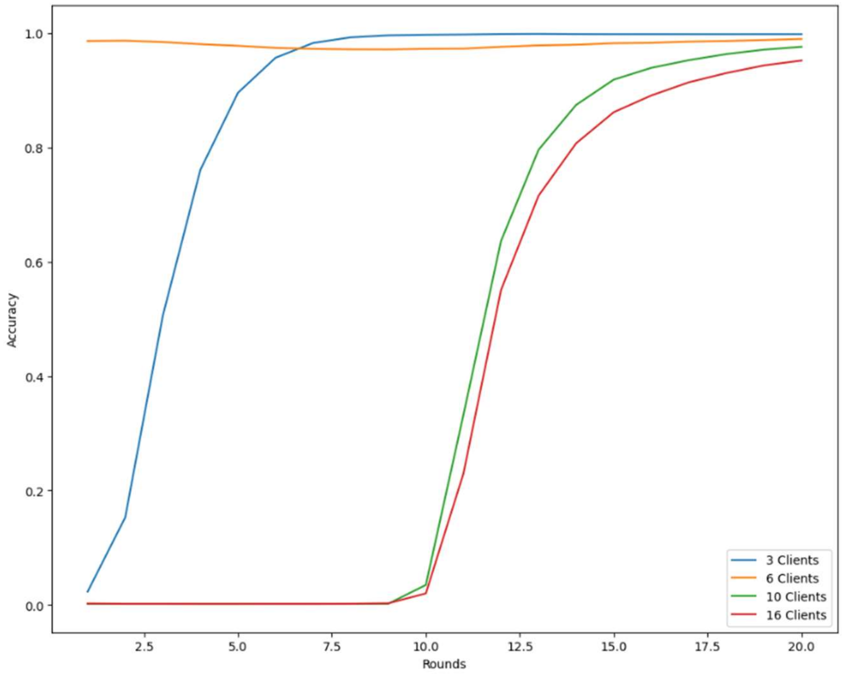
Results

For MLP (Multi-Layer Perceptron) model:

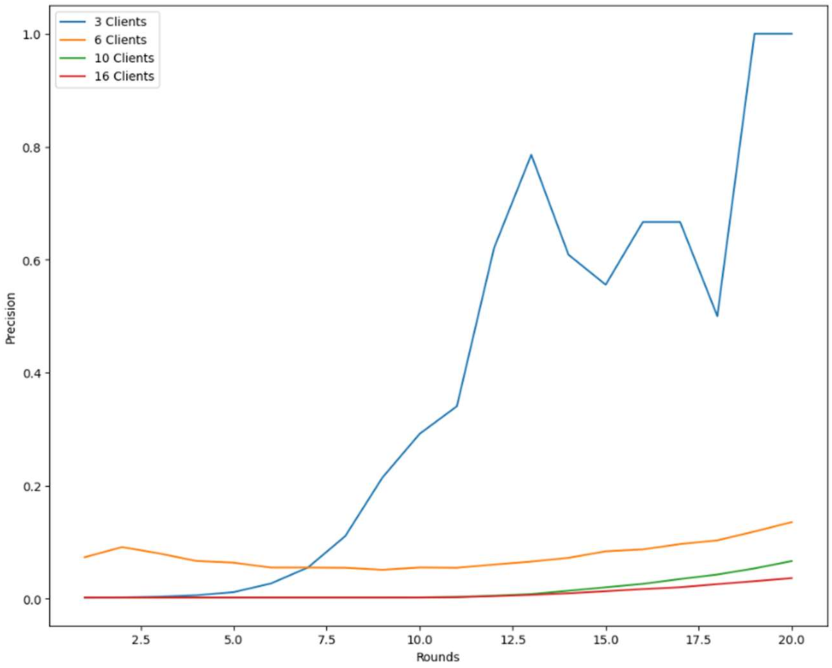
- Number of Clients: [12,16,24,32]
- Number of Clients Selected per Round: [3,6,10,16,32]
- Number of Communication Rounds: 20
- Aggregation Method: Mean
- Performance Metrics: Accuracy, Precision, Recall, F1-Score

1) Total Number of clients = 32

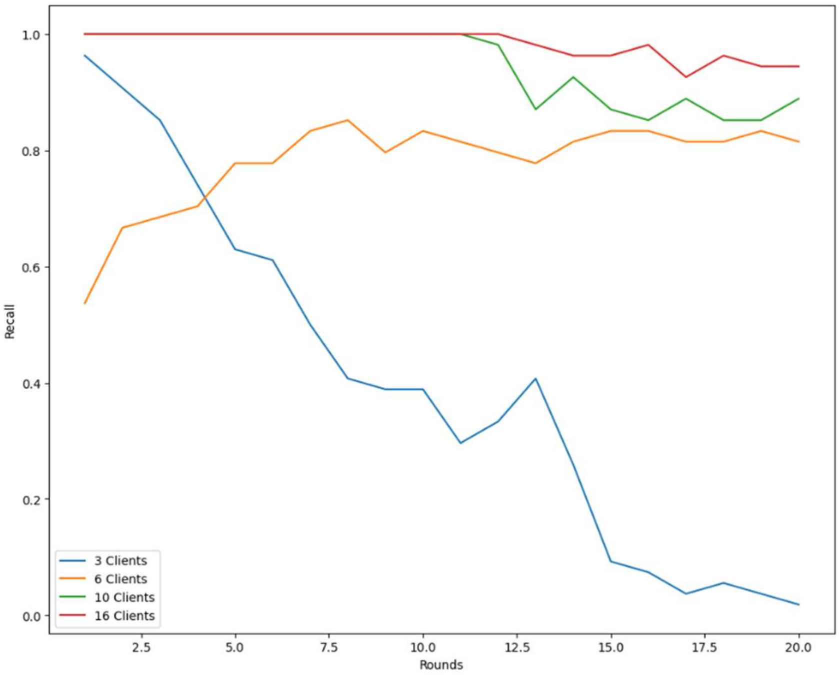
a) Accuracy vs Number of Rounds Plot:



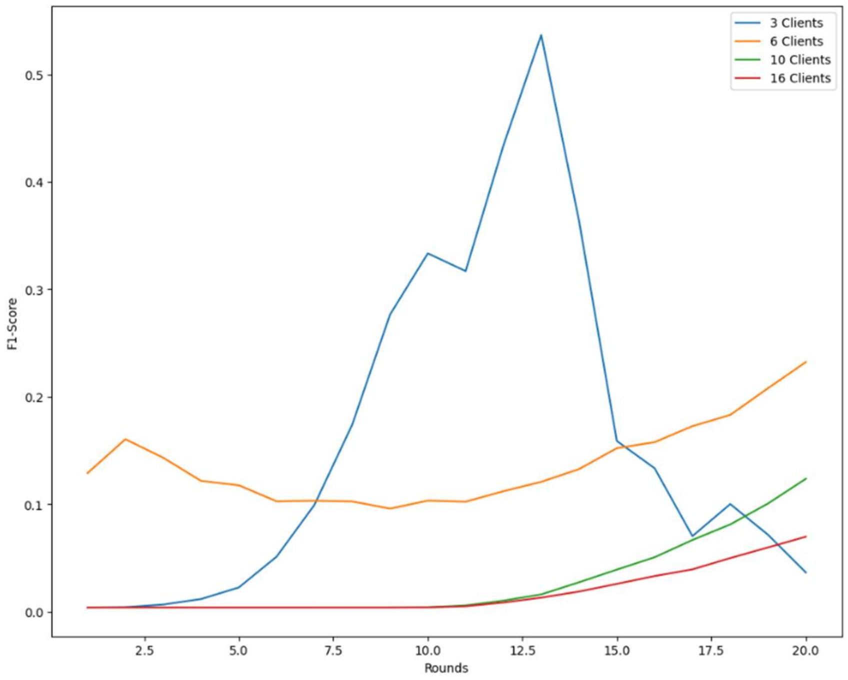
b) Precision vs Number of Rounds Plot:



c) Recall vs Number of Rounds Plot:

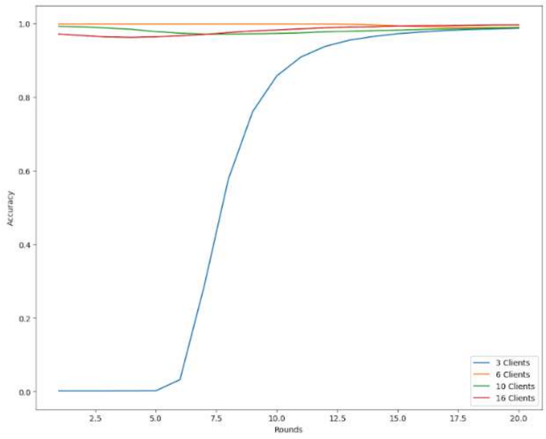


d) F1-Score vs Number of Rounds Plot:

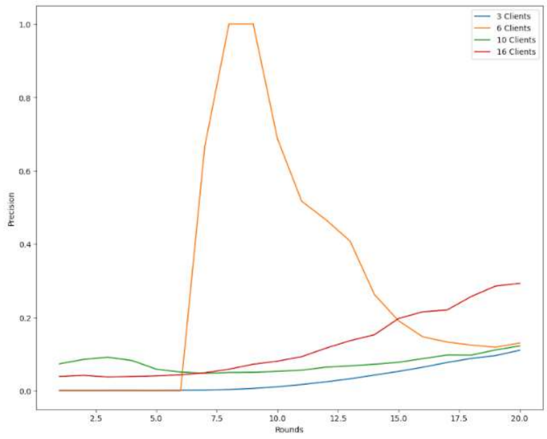


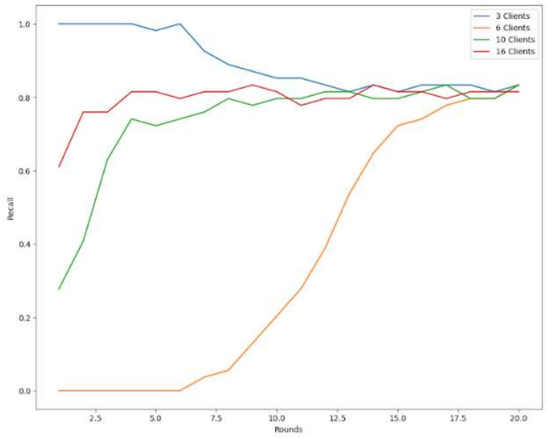
2) Total Number of clients = 24

Accuracy vs Rounds

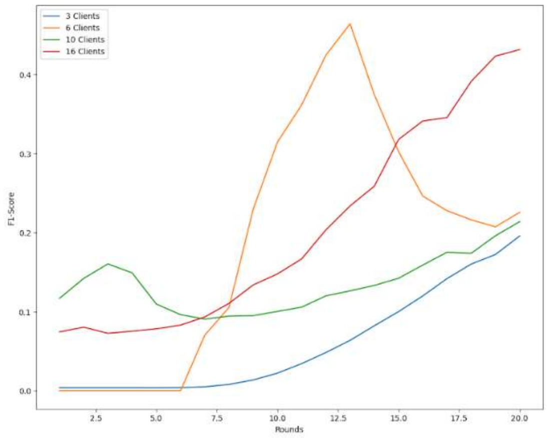


Precision vs Rounds





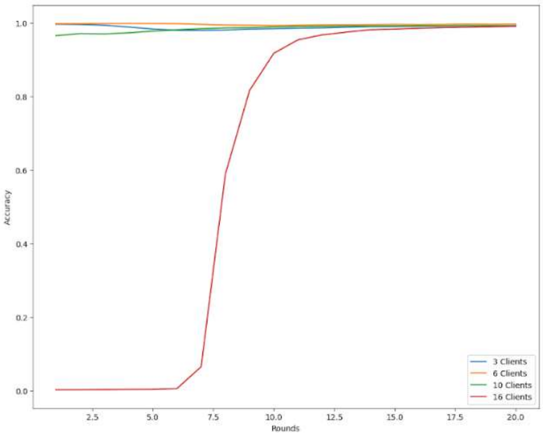
Recall vs Rounds



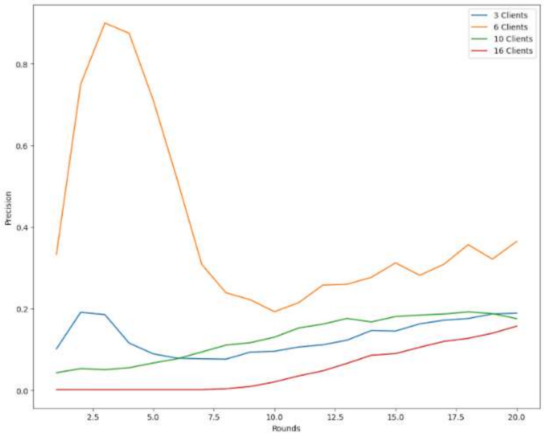
F1-Score vs Rounds

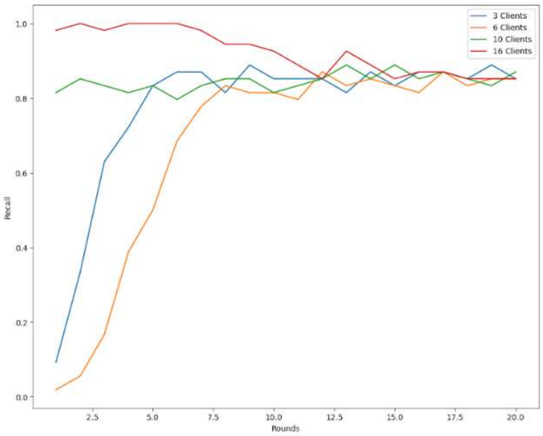
3) Total Number of clients = 16

Accuracy vs Rounds

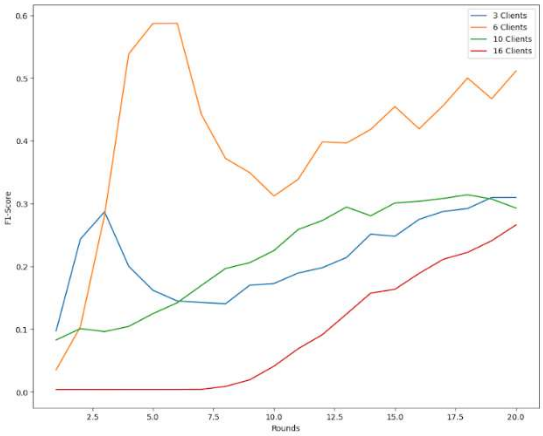


Precision vs Rounds





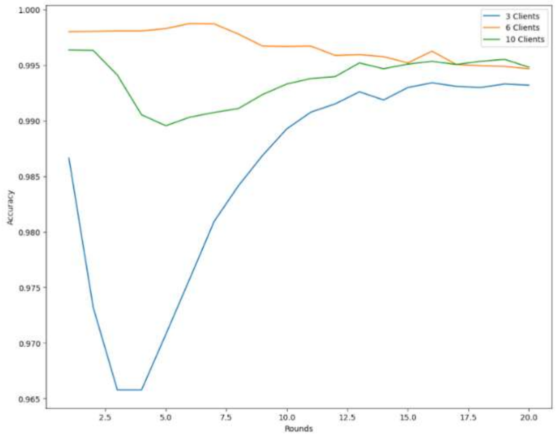
Recall vs Rounds



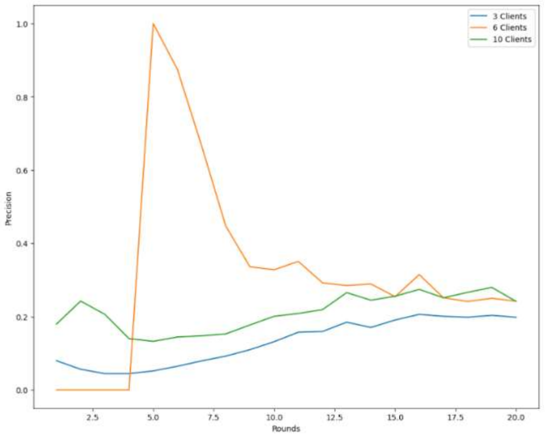
F1-Score vs Rounds

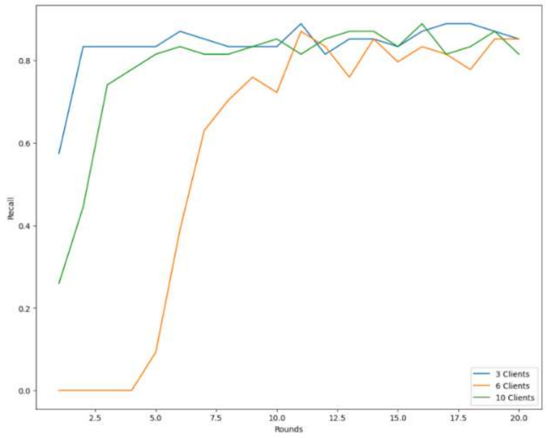
4) Total Number of clients = 12

Accuracy vs Rounds

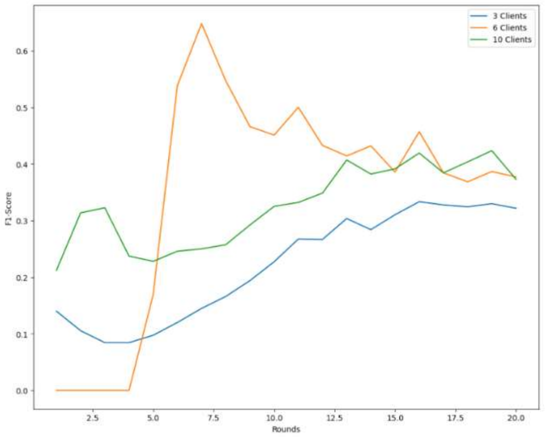


Precision vs Rounds





Recall vs Rounds



F1-Score vs Rounds

For LSTM (Long Short-Term Memory) model:

Currently work is undergoing for the parameters tuning for LSTM model.

Future Work

1. Handling Different Parameters in Data from Different Banks:

- **Data Normalization:** Implement normalization techniques to standardize parameter values across datasets, ensuring consistency.
- **Dynamic Parameter Handling:** Develop adaptive algorithms capable of dynamically adjusting model parameters based on the characteristics of the specific bank's dataset.
- **Bank-Specific Models:** Consider building models tailored to each bank's unique parameters, optimizing performance for individual datasets.

2. Implementation of Ensemble Learning-Based Federated Learning Model:

- **Integration of Ensemble Techniques:** Combine multiple machine learning models, such as CNN, MLP, LSTM, and Random Forest, in a federated learning framework for a diverse and robust fraud detection system.
- **Voting Mechanism:** Implement ensemble voting mechanisms to aggregate predictions from individual models, enhancing overall system accuracy.
- **Adaptive Weighting:** Explore adaptive weighting schemes for ensemble members, assigning more weight to models with better performance on specific datasets.

3. Parameter Tuning and Accuracy Enhancement:

- **Hyperparameter Optimization:** Conduct in-depth parameter tuning for each model (CNN, MLP, LSTM, Random Forest) to fine-tune learning rates, layer configurations, and other hyperparameters.

- **Grid Search and Random Search:** Utilize techniques like grid search and random search to systematically explore the hyperparameter space and identify optimal configurations.
- **Cross-Validation:** Implement cross-validation methods to assess model performance across different subsets of the data, ensuring robustness and preventing overfitting.

4. Checking Performance with Different Aggregation Alternatives in Federated Learning:

- **FedAvg Variants:** Experiment with different variants of the FedAvg algorithm for model aggregation, such as weighted FedAvg or Federated Stochastic Variance Reduced (FedSVRG).
- **Secure Aggregation:** Investigate secure aggregation techniques to preserve data privacy during the federated learning process.
- **Comparative Analysis:** Conduct a comparative analysis of the performance of each aggregation alternative, considering factors like convergence speed, communication efficiency, and model accuracy.

These future work components collectively aim to enhance the adaptability, accuracy, and scalability of the credit card fraud detection system in the context of diverse datasets and federated learning scenarios.

References

1. N. S. Alfaiz and S. M. Fati, "Enhanced credit card fraud detection model using machine learning", *Electronics*, vol. 11, no. 4, pp. 662, 2022.
2. A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga and N. Kuruwitaarachchi, "Real-time credit card fraud detection using machine learning", *2019 9th International Conference on Cloud Computing Data Science & Engineering (Confluence)*, pp. 488-493, 2019.
3. N. K. Trivedi, S. Simaiya, U. K. Lilhore and S. K. Sharma, "An efficient credit card fraud detection model based on machine learning methods", *International Journal of Advanced Science and Technology*, vol. 29, no. 5, pp. 3414-3424, 2020.

4. R. Asha and S. K. KR, "Credit card fraud detection using artificial neural network", *Global Transitions Proceedings*, vol. 2, no. 1, pp. 35-41, 2021.

5. J. I.-Z. Chen and K.-L. Lai, "Deep convolution neural network model for credit-card fraud detection and alert", *Journal of Artificial Intelligence*, vol. 3, no. 02, pp. 101-112, 2021.

6. E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection", *IEEE Access*, vol. 10, pp. 16400-16407, 2022.

7. U. Fiore, A. De Santis, F. Perla, P. Zanetti and F. Palmieri, "Using generative adversarial networks for improving classification effectiveness in credit card fraud detection", *Information Sciences*, vol. 479, pp. 448-455, 2019.

8. D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic and A. Anderla, "Credit card fraud detection-machine learning methods", *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1-5, 2019.

9. W. Yang, Y. Zhang, K. Ye, L. Li and C.-Z. Xu, "Ffd: A federated learning-based method for credit card fraud detection", *Big Data-BigData 2019: 8th International Congress Held as Part of the Services Conference Federation SCF 2019*, vol. 8, pp. 18-32, 2019.

10. W. Zheng, L. Yan, C. Gou and F.-Y. Wang, "Federated meta-learning for fraudulent credit card detection", *Proceedings of the TwentyNinth International Conference on International Joint Conferences on Artificial Intelligence*, pp. 4654-4660, 2021.

11. R. Suvarna and A. M. Kowshalya, "Credit card fraud detection using federated learning techniques", *International Journal of Scientific Research in Science Engineering and Technology*, vol. 7, pp. 356-367, 2020.

12. M. L. G. Ulb, *Credit Card Fraud Detection*, December 2022, [online] Available: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud.