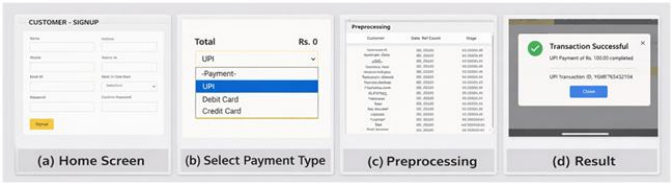
# Privacy-Preserving Multiple Payment Fraud Detection Using LSTM-Based Federated Learning

**Mr. Arokia Nathan[1], Prakash. P[2], Prakash. R[3], Sabari. K[4]**
[1]Assist prof, Dept of Artificial Intelligence and Data Science
[2, 3, 4] Dept of Artificial Intelligence and Data Science
[1, 2, 3, 4] AVS Engineering College, Salem, India

***Abstract-*** *This paper presents a privacy-preserving framework for multiple payment fraud detection using Long Short-Term Memory (LSTM) and Federated Learning. The model captures temporal patterns in transaction data to identify fraudulent activities effectively. Federated Learning enables decentralized training across multiple clients without sharing sensitive data, ensuring privacy and security. Experimental results show that the proposed approach achieves over 95% accuracy with improved precision and recall compared to traditional methods. Additionally, it reduces data leakage risks while maintaining scalability and efficiency. The proposed system is suitable for real-time fraud detection in distributed financial environments.*

***Keywords:*** Fraud Detection, LSTM Networks, Federated Learning, Privacy-Preserving, Deep Learning




## I. INTRODUCTION

The rapid growth of digital payment systems and e commerce platforms has revolutionized financial transactions, offering enhanced speed and convenience. However, this transformation has also led to a significant increase in sophisticated financial fraud, creating critical challenges for financial institutions and consumers. Traditional fraud detection systems, which rely on centralized data processing, face limitations in scalability, real-time detection, and data privacy.

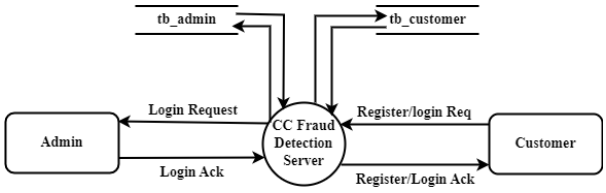
Deep learning techniques have shown great potential in addressing these challenges. In particular, Long Short Term Memory (LSTM) networks are highly effective in modelling sequential transaction data. Nevertheless, centralized training requires access to sensitive data. Federated Learning provides a decentralized framework that allows collaborative training without sharing raw data. By exchanging only model parameters, it ensures data privacy while improving model performance.

## II. RELATED WORK

Recent studies have explored various machine learning and deep learning techniques for financial fraud detection. Traditional methods like logistic regression and decision trees often fail to capture complex temporal patterns in transaction data. Deep learning models, particularly recurrent neural networks (RNNs), have demonstrated improved performance. Among them, LSTM networks have gained attention due to their ability to model sequential dependencies in time-series data. To address decentralized training paradigm that enables multiple clients to train a global model collaboratively.

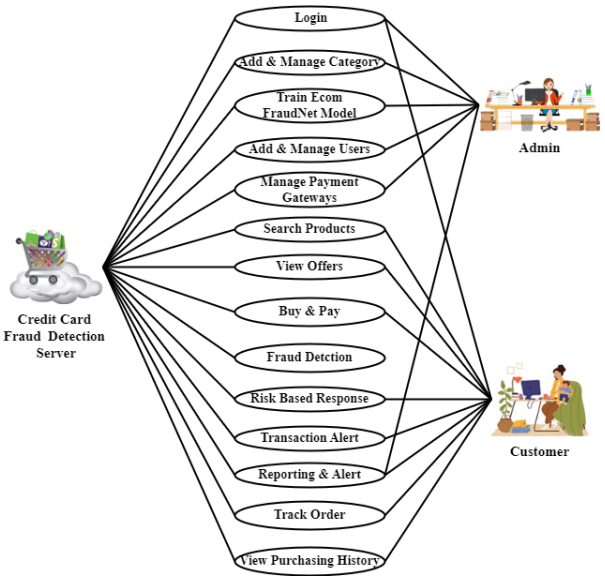
## III. METHODOLOGY

The proposed privacy-preserving framework focuses on capturing sequential transaction patterns while ensuring data confidentiality through decentralized model training.




### A. System Overview

The system consists of multiple distributed clients and a central server. Each client locally trains an LSTM model on its private transaction data. Instead of sharing raw data, only model parameters are transmitted to the central server for aggregation.



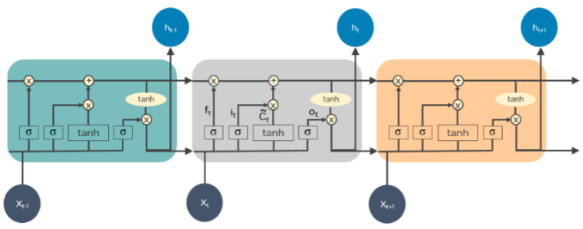

**B. Data Preprocessing**

Transaction data is pre-processed to improve model performance. This includes data cleaning, normalization, and feature extraction. Sequential transaction records are structured into time-series formats suitable for LSTM input.

**C. LSTM-Based Fraud Detection**

LSTMs can be defined as Recurrent Neural Networks (RNN) that are programmed to learn and adapt for dependencies for the long term. It can memorize and recall past data for a greater period and by default, it is its sole behaviour. LSTMs are designed to retain over time and henceforth they are majorly used in time series predictions because they can restrain memory or previous inputs. This analogy comes from their chain-like structure consisting of four interacting layers that communicate with each other differently. Besides applications of time series prediction, they can be used to construct speech recognizers, development in pharmaceuticals, and composition of music loops as well.

LSTM work in a sequence of events. First, they don't tend to remember irrelevant details attained in the previous state. Next, they update certain cell-state values selectively and finally generate certain parts of the cell-state as output. Below is the diagram of their operation.



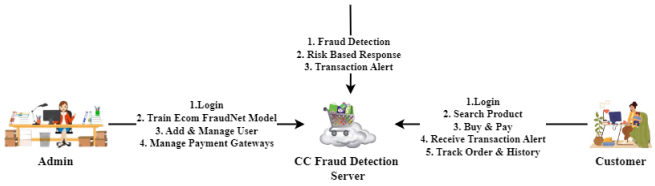
LSTMs retain information over time. They are useful in time-series prediction because they remember previous inputs. LSTMs have a chain-like structure where four interacting layers communicate in a unique way. Besides time-series predictions, LSTMs are typically used for speech recognition, music composition, and pharmaceutical development.

D. Federated Learning Framework

Federated Learning allows each client to update the model locally. The local updates are periodically sent to the central server, where they are aggregated using a weighted averaging mechanism (e.g., Feeding) to update the global model.

## IV. RESULTS AND DISCUSSION

The performance evaluation assessment shows that the proposed model achieves an accuracy of over 95%, demonstrating its effectiveness. The precision and recall values are significantly improved compared to traditional machine learning approaches, indicating a reduction in false positives and false negatives. Compared to centralized fraud detection systems, the proposed approach shows superior performance due to its ability to learn from distributed datasets while ensuring privacy.




## V. CONCLUSION

This paper presented a privacy-preserving framework for multiple payment fraud detection using LSTM-based Federated Learning. The approach effectively captures sequential patterns while ensuring data confidentiality.

Experimental results demonstrate that the model achieves high accuracy, outperforming traditional centralized methods. The framework is scalable, efficient, and suitable for real-time deployment in distributed financial environments.

## VI. FUTURE WORK

Future work can focus on enhancing the framework by incorporating advanced architectures such as hybrid models and attention mechanisms. Additionally, the integration of real-time streaming data can enable faster detection.

Improving the robustness of the Federated Learning framework against adversarial attacks is also a priority.

## REFERENCES

[1] Hochreiter, S., &Schmid Huber, J. (1997). Long Short-Term Memory. Neural Computation, 9(8), 1735–1780.
[2] McMahan, B., Moore, E., Ramage, D., Hampson, S., &Acras, B. A. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 1273–1282.
[3] Yurovsky, V., Granitzer, M., Ziegler, K., Calabretta, S., Portier, P. E., He-Galeton, L., & Caelen, O. (2018). Sequence Classification for Credit-Card Fraud Detection. Expert Systems with Applications, 100, 234–245.
[4] Shokri, R., & Shmatikov, V. (2015). Privacy-Preserving Deep Learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS), 1310–1321.
[5] Konečný, J., McMahan, H. B., & Ramage, D. (2016). Federated Optimization: Distributed Machine Learning for On-Device Intelligence. arid preprint arXiv:1610.02527.
[6] Bhattacharyya, S., Jha, S., Thara Kunnel, K., & Westland, J. C. (2011). Data Mining for Credit Card Fraud: A Comparative Study. Decision Support Systems, 50(3), 602–613.