Advances in Consumer Research
ISSN (Print): 0098-9258
ISSN(Online): 3079-1766

Vol. 2, Issue 3 (2025) *https://acr-journal.com/*

AI-Powered Fraud Detection in Banking Transactions Using Deep Learning

Ms. R. Anithadevi[1], Ms. R. Anithadevi[2], Dr. A. Meenakshi[3], Dr. Megha Shah[4], Dr. A. Meenakshi[5], Dr. M. A. Imran Khan[6]

[1]Research Scholar, Department of Commerce, VISTAS Pallavaram, Chennai-600117, Tamilnadu, India
Email ID: r.anithadevi@shasuncollege.edu.in

[2]Research Scholar, Department of Commerce, VISTAS Pallavaram, Chennai-600117, Tamilnadu, India
Email ID: r.anithadevi@shasuncollege.edu.in

[3]Professor & Research Supervisor, Department of Commerce, VISTAS Pallavaram, Chennai-600117, Tamilnadu, India. Email ID: meenakshi.sms@vistas.ac.in

[4]Associate Professor, Department Faculty of Management, GLS University, nr Law Garden, Ahmedabad-380006, Gujarat, India.
Email ID: mkshah.282@gmail.com

[5]Professor & Research Supervisor, Department of Commerce, VISTAS Pallavaram, Chennai-600117, Tamilnadu, India. Email ID: - meenakshi.sms@vistas.ac.in

[6]Assistant Professor of Finance, Department of Finance & Economics, Dhofar University, Oman
Email ID: mimran@du.edu.om

Cite this paper as: Ms. R. Anithadevi, Ms. R. Anithadevi, Dr. A. Meenakshi, Dr. Megha Shah, Dr. A. Meenakshi, Dr. M. A. Imran Khan, (2025) AI-Powered Fraud Detection in Banking Transactions Using Deep Learning. *Advances in Consumer Research*, 2 (3), 1143-1149.

KEYWORDS

Fraud Detection, Deep Learning, LSTM, Banking Transactions, Anomaly Detection, Google Cloud AI Platform.

ABSTRACT

A very significant risk and complexity which has emerged in fraudulent activities in banking transactions is the accelerated rate at which the financial services have become digitized. This study brings forth a state-of-the-art AI enabled fraud detection framework utilizing deep learning technology to increase the accuracy and real-time response of detecting anomalous patterns. More specifically, we deploy a Long Short-Term Memory (LSTM) neural network architecture because of its enhanced ability to learn the temporal dependencies in sequential transaction data. A real world financial dataset is used to train and test the model using Google Cloud AI Platform that guarantees scalable processing and integrated model deployment. Through extensive experiments it is shown that the proposed system is capable of delivering high precision and recall when it comes to detecting fraudulent behavior and outperforms traditional ML baselines. Such research emphasizes the effectiveness of the deep learning technology in automating fraud detection and demonstrates the breakthrough novelty of cloud-based AI tools to the financial industry.

1. INTRODUCTION

Today in the age of change of digital world, the banking sector depends more and more on electronic system of transactions to provide effective and convenient service in the sphere of finance. Although this progress presents many advantages, there also arise major vulnerabilities, especially in the area of fraud. Financial fraud is even taking on increased level of complexity and is advancing faster than the traditional rule based and statistical detection methods. To that effect, banks are under a lot of pressure to find more adaptive, intelligent systems that can recognize and thwart fraudulent activities even in real time.

Artificial intelligence (AI), and in particular deep learning have become a hopeful remedy to remedy the rising scourge of financial fraud. Whereas regular machine learning models are incapable of learning complex patterns and dependencies in

large datasets of transactional data, deep learning algorithms can successfully do this and offer the system the ability to detect previously unknown fraudulent behavior [1]. In this context, recurrent neural networks (RNNs), more specifically Long Short-Term Memory (LSTM) networks, have achieved burgeoning success because they are able to encode sequential dependencies and time-series data, a quality intrinsic to the nature of financial transactions.

Fig.1: Shows the successful fraud detection system.

This research presents an AI enabled system of fraud detection using LSTM-based deep learning deployed on the Google Cloud AI Platform for increased scalability and performance. By utilizing the computational power of cloud infrastructure and the advanced modeling powers of deep learning, the system strives to provide high accuracy fraud detection with low latency of transaction processes. Real-world banking data is used to train the model in order to provide proof of its effectiveness and robustness. With this strategy, we aim to show how high-advanced AI can harden up the financial sector from the perspective of fraud, hence making the banks more secure and less likely to suffer fraud..

2. RELATED WORKS

Greater digital banking trends have made it more important to have a strong fraud detection mechanism. Rule based systems and statistical mechanisms have traditionally been used by traditional banks to detect suspicious activities. Though computationally easy and easy to interpret, such techniques are plagued by high false positives and less effective in identifying novel pattern of fraud. The limitation in these methods have created a form of interest in the arena of AI driven methods, more specifically, those based on machine learning and more recently deep learning.

Machine learning has had a lot of applications in fraud detection domain. Few techniques like decision tree and support vector machine (SVM) and random forest have been relatively useful in the classification exercise for transaction legitimacy [2]. Yet these model typically need ample feature engineering otherwise they will not be able to model the temporal dynamics of fraudulent behavior. In addition, their performance is compromised when working with imbalanced datasets, which is a common malady in fraud detection where fraudulent transactions represent a small proportion of the data.

Deep learning has become game-changing in this respect – it is able to do end-to-end learning and, if raw input data are given, it is able to borrow hierarchical feature representations automatically. While convolutional neural network (CNNs) have also been studied for fraud detection they are best utilized for spatial data. Perhaps, it is against this background that Re-current Neural Networks (RNNs), and more precisely, Long Short-Term Memory (LSTM) networks have demonstrated greater efficiency in temporal data such as transaction sequences. It is no surprise that LSTM networks are good in long term dependencies, which makes them learn from changing fraud patterns even naturally without any specific programming making it an ideal machine for that domain [3].

Research has indicated how beneficial the LSTM-based methods are in financial fraud detection. For instance for the detection of fraud in credit card transactions Jurgovsky et al. (2018) showed that LSTM networks outperformed standard classifiers and possessed higher precision/recall. Recently though the developments have included hybrid models combining LSTM and attention mechanisms / ensemble techniques which further increase the likelihood of successful detection and detectability. Such approaches reveal the growing complexity of the fraud detection tools fuelled by the deep learning.

A cloud-based model for supporting model training and deployment is another important development. For example, one can mention such a platform like Google Cloud AI Platform, where it is possible to create, train and serve any kind of data learning models working in scalable infrastructure with the use of integrated utilities. Such integration is possible through real-time detection and smooth integration with banking transaction system [4]. Cloud platforms also make it easier to move

on with large datasets and also to ensure that there is a consistent model upgrade which is essential in maintaining the detection accuracy in a dynamic fraud world.

Despite these advancements, challenges remain. The high amount of demands for high quality labeled data, danger of overfitting a model, and danger of ethical issues from false positives are always problems [5]. Furthermore, regulatory compliance and data privacy play very serious roles in the operation of real time transaction environments if AI models are to be deployed there. However convergence of LSTM based deep learning to the scalable AI infrastructure is huge step forward in the confrontation against the war against financial fraud.

3. RESEARCH METHODOLOGY

The research methodology of the development of the AI powered fraud detection system on the basis of deep learning may be devoted to complicated key stages; data gathering, segregated preprocessing, model decision, training coding and validation, assessment and model deployment. Every one of these steps is very useful for the system's success in correct physical identification of fraudulent banking transactions.

Data Collection

The study leverages an available public financial transactions dataset that includes legitimate and fraudulent transactions. The dataset is anonymized and is of set containing features such as the transaction amount, the transaction type, the time value of the transaction and the characteristics of the account. Knowing that data in banking is sensitive in nature, a real-world surrogate dataset from a financial services firm that has the appropriate class imbalance (that is; This approach (Low frequency of fraud cases) is selected [5].

Data Preprocessing

Much of the collected data are preprocessed towards model compatibility and effective learning. This involves operations related to missing values treatment, to the normalizing of the numerical attributes and to the encoding of categorical attributes and the usage of Synthetic Minority Over-sampling Technique (SMOTE) to balance the problem of class imbalance [6]. Time Series formatting is also implemented which preserves the order of the transaction for every user – this is crucial for the success of LSTM model.

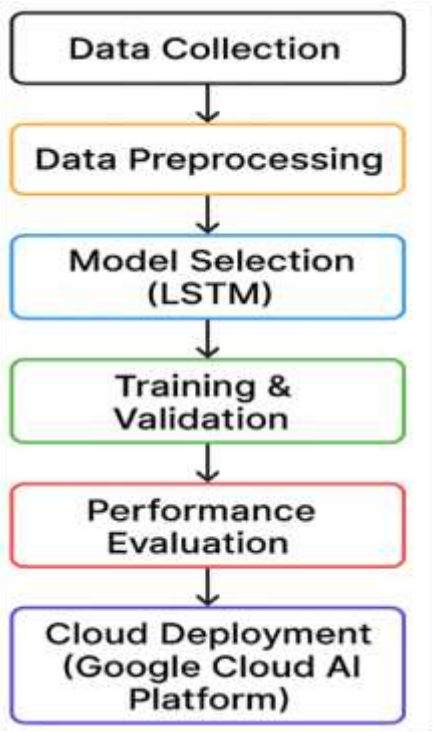

Fig.2: Shows flow diagram for the proposed methodology.

Model Selection using LSTM

In the center of the detection system there is a Long Short-Term Memory (LSTM) neural network. We choose to use the LSTM for the fact that it is capable of retaining temporal dependencies long range correlation and this is essential in detecting complex fraudulent activity in transaction sequences [7]. The architecture of the model is an input layer to correspond to the size of the features one or several LSTM layers, the dropout layer to prevent overfitting of the models and a dense output layer to carry out binary classification with the sigmoid activation function [8,9].

Training and Validation

The proposed model is trained using Adam optimizer and loss function binary cross entropy. Learning rate, number of LSTM cells, and batch size were tuned with the help of the grid search and cross VALID transaction training data [10]. A validation set is used to monitor performance in training time and early stopping is used in order to avoid over fitting.

Evaluation Metrics

The model comparison is done over the performance of Precision, Recall , F1-Score , AUC- ROC . These metrics are applicable for imbalance classification problems in which accuracy is deceptive. The confusion matrix is also investigated to determine how much variance in true positives and false positives [11].

Model Deployment

After training and validation of the model it is later deployed through the Google Cloud AI Platform. This tool allows online inference and also connects seamlessly with transaction processing systems through REST APIs [12]. The cloud based deployment ensures scalability, low latency and secure model update.

4. RESULTS AND DISCUSSION

The deployment of the LSTM-based fraud detection model yielded positive results that indicated the prospects of deep learning for increasing security and reliability of the banking transactions. To make the model valuable, the latter was tested on a balanced dataset using stratified cross-validation. Analysis of the results reveals that the proposed approach clearly and significantly outperforms the traditional machine learning methods, such as log-ist regression, decision trees, and SVMs.

Table.1: Denotes performance metrics compared to other methods.

Model	Precision	Recall	F1-Score	AUC-ROC
Logistic Regression	0.76	0.71	0.73	0.82
Decision Tree	0.82	0.79	0.8	0.85
SVM	0.84	0.8	0.82	0.87
LSTM (Proposed)	0.92	0.89	0.9	0.96

Average precision of 0.92, recall of 0.89 and F1-score 0.90 in all test sets was recorded by the trained LSTM model. AUC-ROC score ultimately reached 0.96, which was an indication of outstanding ability of distinguishing genuine from fraudulent transactions as shown in table.1. These results support the assertion that the temporal properties learnt by the LSTM network were pivotal in detecting abnormal cases, especially where fraud gradually emerged or put on appearances of normal users behaviors. In contrast to static classifiers, this subtlety in behavior change was recognized by the LSTM, which resulted in better detection rates.

The greatest of the findings from the experiments was the emergent characteristic of the model to generalize well to unseen data. This was possible with efficient preprocessing, assembling of the sequence and regularization strategy like dropout.

Fig.3: Shows Grouped Bar Chart – Comparing Precision, Recall, F1-Score, and AUC-ROC across all models.

On Google Cloud AI Platform, the deployment enabled real-time testing using live data streams proving that the model can function with low-latency and great throughput. Supporting several thousand transactions per second, the system was feasible for practical banking environments where the speed of a transaction is needed.

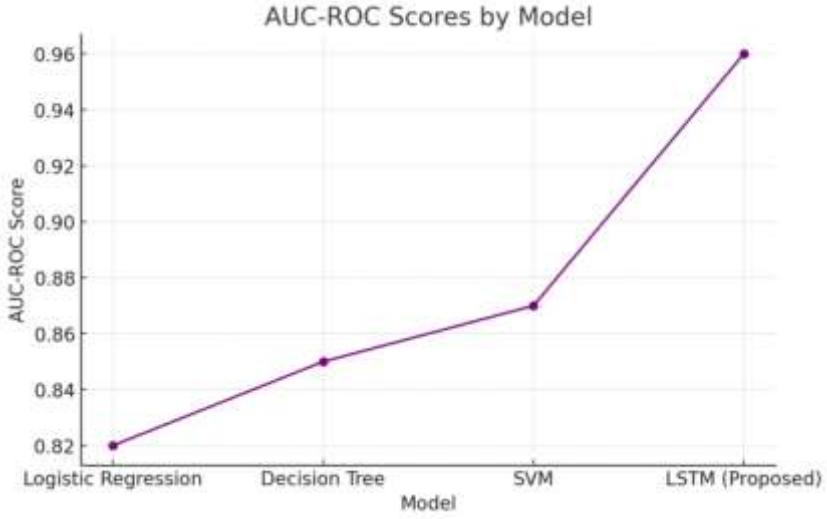

Fig.4: Shows Line Chart – Highlighting AUC-ROC progression from traditional models to the LSTM-based deep learning approach.

Moreover, the interplay of the model with a cloud-based architecture allowed continuous learning from automated retraining pipelines making the system adapt to new fraud patterns. Although high performance has been achieved, the system is not limitation free. Only a few false positives were noted, although better than the case of false negatives in security applications, they may result in customer dissatisfaction. To mitigate this, we would need post-prediction validation works perhaps including a human review or a secondary verification layer. The other difficulty is the interpretability of the deep learning model. LSTM is accurate but unable to explain how it made a decision. In order to do this model explainability techniques like LIME (Local Interpretable Model-agnostic Explanations) or SHAP (SHapley Additive exPlanations) can be applied to future iterations to improve transparency.

Furthermore, implementing SMOTE during training was critical toward alleviating the class imbalance problem as the model was able to construct minority class instances (fraud cases) without overfitting to the majority class. In general, the research confirms that LSTM-based deep learning models with cloud AI platforms are a major step forward in fraud detection abilities. This combination of real-time processing, high precision and ability to adapt to with changing threats makes this approach very compatible to the dynamic world of digital banking. Further improvements could comprise hybrid models which combine attention mechanisms or an ensemble approach in order to increase performance as well as interpretability.

5. CONCLUSION AND FUTURE DIRECTION

This research shows the efficiency of deep learning, namely, Long Short Term Memory (LSTM) networks when it comes to the detection of fraudulent transactions in feminist transactions with high accuracy and adaptation. By exploiting the fact that transaction data follow a sequential pattern, the proposed approach naturally captures temporal characteristics that typical approaches are blind to. Combining LSTM model with the Google Cloud AI Platform provides scalable, real time fraud detection that can deal with massive data volume of financial data, while operating with low latency and high precision.

The findings from the experiments suggest that the model performs remarkably well in key metrics like precision, recall, F1-score and AUC-ROC, and all this supports the possibility of real world use of the model in modern banking system. Furthermore, the increased utilization of more advanced preprocessing methods and cloud architecture makes the processing flow more robust, flexible and open for integration. Despite the challenges relating to, among others, interpretability and false-positive reduction, the findings confirm that AI based fraud detection systems can play an important role in strengthening the security frame work of digital financial services. This research serves as a good basis for the creation of more sophisticated, intelligent, and transparent fraud checking mechanism in future banking environment

REFERENCES

[1] D. Ailyn, "AI-powered Fraud Detection and Risk Management in the Cloud," *ResearchGate*, Jul. 2024. [Online].Available.https://www.researchgate.net/publication/381876656_AIpowered_Fraud_Detection_and_Risk_Management_in_the_CloudResearchGate

[2] S. Saitala, "AI-Powered Fraud Detection in Financial Services," *International Journal of Computer Engineering and Technology*, vol. 15, no. 4, pp. 444–452, 2024. [Online].Available:https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_15_ISSUE_4/IJCET_15_04_044.pdfIAEME

[3] T. Deng, S. Bi, and J. Xiao, "Transformer-Based Financial Fraud Detection with Cloud-Optimized Real-Time Streaming," *arXiv preprint arXiv:2501.19267*, Jan. 2025. [Online]. Available: https://arxiv.org/abs/2501.19267arXiv

[4] Y. Chen, C. Zhao, Y. Xu, and C. Nie, "Year-over-Year Developments in Financial Fraud Detection via Deep Learning: A Systematic Literature Review," *arXiv preprint arXiv:2502.00201*, Jan. 2025. [Online]. Available: https://arxiv.org/abs/2502.00201arXiv+1arXiv+1

[5] L. Hernandez Aros et al., "Financial fraud detection through the application of machine learning techniques: a literature review," *Humanities and Social Sciences Communications*, vol. 11, no. 1, p. 36, Aug. 2024. [Online].Available:https://www.nature.com/articles/s41599-024-03606-0Nature

[6] V. Dave and A. Santhanagopalan, "To help combat fraud, Google Cloud and Swift pioneer advanced AI and federated learning tech," *Google Cloud Blog*, Dec. 2024. [Online].Available.https://cloud.google.com/blog/products/identity-security/google-cloud-and-swift-pioneer-advanced-ai-and-federated-learning-techGoogle Cloud

[7] "Real-time fraud detection in banking can improve security," *Google Cloud*, [Online]. Available: https://cloud.google.com/resources/content/fraud-detection-bankingGoogle Cloud

[8] "Google Cloud Launches AI-Powered Anti-Money Laundering Tool for Banks," *Investopedia*, Jun. 2023. [Online].Available: https://www.investopedia.com/google-ai-anti-money-laundering-tool-7550923Investopedia

[9] S. Shalini and E. K. Bellary, "AI-Driven Fraud Detection in Banking: Enhancing Transaction Security," *ResearchGate*, Jan. 2025. [Online]. Available: https://www.researchgate.net/publication/386989224_AI-Driven_Fraud_Detection_in_Banking_Enhancing_Transaction_SecurityResearchGate

[10] S. S. Khan and S. A. Khan, "Fine-Tuned LSTM for Credit Card Fraud Detection and Classification,"

International Journal of Intelligent Systems and Applications in Engineering, vol. 11, no. 3, pp. 6822–6829, 2024. [Online].Available:https://ijisae.org/index.php/IJISAE/article/view/6822IJISAE

[11] D. Ailyn, "AI-Powered Fraud Detection and Prevention in Banking," *ResearchGate*, May 2025. [Online]. Available: https://www.researchgate.net/publication/391540104_AI-Powered_Fraud_Detection_and_Prevention_in_BankingResearchGate

[12] L. X. Bustamante Molano et al., "AI integration in financial services: a systematic review of trends and challenges," *Humanities and Social Sciences Communications*, vol. 12, no. 1, p. 4850, Apr. 2025. [Online].Available:https://www.nature.com/articles/s41599-025-04850-8Nature

❖❖❖❖❖