Journal of Soft Computing Paradigm (ISSN: 2582-2640)
www.irojournals.com/jscp/

Fraud Detection in Banking: A Deep Learning Approach with Explainable AI

Chandra Sekhar Koppireddy[1], Vivarjitha Devi R V D S.[2]

[1]Assistant Professor, [2]Student, Computer Science and Engineering, Pragati Engineering College, JNTUK, Kakinada, India.

E-mail: [1]chandrasekhar.koppireddy@gmail.com, [2]srivallir16@gmail.com

Abstract

The fraud in banking has increased considerably due to the increasing use of digital transactions as well as internet banking. Conventional fraud detection systems are unable to keep up with the changing trends and most of them are unable to detect fraud in time. The deep learning models have gained popularity as a potentially competent option because they can learn complicated patterns from massive transactional data. But they are also of a black-box nature, which hinders transparency and trust, especially in critical sectors such as banking. To address this shortcoming, XAI is being progressively added to fraud detection systems to make sure the decisions made by deep learning models are understandable to stakeholders. This paper describes the current state of the use of deep learning in fraud detection in the banking industry and how it can be augmented using XAI techniques like SHAP, LIME, and attention mechanisms to improve the reliability, interpretability, and efficacy of the resulting fraud detection systems. It is the first survey that summarizes publicly available datasets like Kaggle Credit Card Fraud Detection dataset and the IEEE-CIS Fraud Detection dataset, and compares deep learning models like CNNs, RNNs, LSTMs, Autoencoders, and GNNs. The key metrics through which these models are compared include Accuracy, Precision, Recall, F1-score and AUC-ROC. The uniqueness of this work lies in coupling deep learning techniques with XAI techniques (SHAP and LIME) to offer fraud detection that is transparent and friendly to regulators. It also takes a census of various deep learning models such as CNNs, RNNs, LSTMs, Autoencoders, and GNNs in transaction anomaly detection. Moreover, the paper also identifies existing datasets, performance benchmarks, issues to be addressed like data imbalance and adversarial fraud, and a future roadmap. The statistical data, performance charts, and model

DOI: https://doi.org/10.36548/jscp.2025.3.004
Received: 03.07.2025, received in revised form: 05.08.2025, accepted: 21.08.2025, published: 05.09.2025

comparison bar graphs will be incorporated as they will give visual evidence for the findings. The paper will attempt to close the gap between the accuracy and interpretability of AI, and consequently, ensure the responsible use of AI in the banking sector.

Keywords: Fraud Detection, Banking Sector, Deep Learning, Explainable AI (XAI), Digital Transactions, Internet Banking, SHAP, LIME, Attention Mechanisms, Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM).

1. Introduction

The banking business has experienced an increase in fraudulent practices, which take advantage of loopholes in technology and the weaknesses of its users. As the rest of the world moves to digital banking and online transactions, fraudsters have implemented sophisticated methods like phishing, identity theft, and synthetic accounts. The traditional fraud detection systems, consisting of rule-based engines or traditional machine learning models, have been known to be insufficient because they cannot be adjusted to the constantly changing patterns of fraud and big data. Deep learning (DL) provides a significant step forward because it can handle huge volumes of data and identify patterns that are hidden without the need for engineering features [Table1]. The data in Table 1 indicates a steep increase in reported fraud cases in India, with reported fraud cases peaking in 2021 at an estimated 15,845 in the year 2024, despite fluctuations in the total monetary loss. This trend not only indicates the rising number of digital transactions but also the rising level of cybercriminals sophistication. The reduction in reported total loss in 2022, although there were also the same number of reported fraud cases, suggests that fraudsters are moving to smaller and more difficult schemes. In the case of fraud detection models, this implies that they must be capable of adapting to both macro-level and micro-level trends of fraud and need deep learning models that can work with imbalanced data sets and spot anomalies in small groups. It underlines the necessity of real-time fraud detection, adaptive learning approaches, and a combination with Explainable AI that would improve auditing and compliance.

As an example, JPMorgan Chase was able to increase accuracy in detecting wire fraud by applying deep learning with explainable AI, and PayPal can identify fraud rings in the shadows using Graph Neural Networks, reducing undetected fraud by more than 15 percent. These practical scenarios show the superiority of DL-based systems over traditional ones in terms of detection speed and accuracy.

Table1. Understanding the Rise in India's Financial Frauds from 2021 to 2024

Year	Number of Reported Fraud Cases	Total Amount Involved (INR Crores)	Remarks
2021	9,103	₹1,38,211	Increase in digital fraud during COVID
2022	9,097	₹60,414	Focus shifted to digital trans
2023	13,530	₹30,252	Rise in UPI and phishing-related frauds
2024	15,845 (est.)	₹38,950(est.)	Projected rise with expanding digital banking

1.1 Background

The banking and financial services industry has been digitized at an alarming rate in the last decade, completely transforming the customer-bank interface. Digital platforms have presented a new level of convenience and accessibility through mobile banking applications, real-time online transactions, and more. However, there is a trade-off for this convenience, banks have never been more vulnerable to cyber-attacks and financial crimes. These services rely on a digital infrastructure that is efficient but has become a profitable target for malicious actors. Criminal actions like identity theft, account takeover, credit card fraud, synthetic identity formation, phishing, and unauthorized access to personal financial information have significantly increased in both frequency and sophistication. Advanced technologies, such as artificial intelligence and social engineering techniques, are actively used by cybercriminals to take advantage of banking systems and the customer behavior. Such fraudulent schemes not only result in substantial financial losses but also undermine customer confidence besides and can potentially causes long-term reputational damage to financial institution. The adoption of cashless economies and the increasing volume of online transactions further increase these risks, necessitating the development of real-time, highly effective fraud detection systems. This changing threat landscape means that financial organizations and digital banks should consider investing in smart, flexible, and scalable solutions to protect their financial resources and maintain customer confidence in their banking systems and services [1].

1.2 Objectives

The main aim of the given paper is to present an in-depth review of the use of deep learning methods in the area of banking fraud detection. It will investigate the potential benefits of using these more sophisticated models, which have the ability to learn complex and non-linear patterns from large quantities of transactional data, to greatly improve the accuracy and efficiency of detecting fraudulent activity. The paper also highlights the increasing need for transparency in AI-based systems, especially in regulated environments such as the banking system, by considering the contribution of Explainable Artificial Intelligence (XAI). It is based on explanations of several XAI approaches, including SHAP and LIME, to reveal the best way to incorporate interpretability into deep learning models to enhance trust, compliance, and usability. Furthermore, the paper aims to examine state-of-the-art solutions and real-world examples that integrate deep learning with XAI, providing an understanding of best practices, architecture, performance indicators, and deployment methods. Through the accomplishment of these goals, the paper will contribute to the creation of intelligent, ethical, and explainable fraud detection systems that are adapted to the continuously changing requirements of digital finance [2].

2. Types of Fraud in Banking

2.1 Unauthorized Card Transactions

Includes illegal credit card information and utilising it to make money. Lost/stolen card use, counterfeit card and card-not-present fraud are also covered.

2.2 Identity Theft

Stolen personal data is used by criminals to create false accounts or gain unauthorized access to those that already exist.

2.3 Account Takeover

Scammers acquire access to the account of a real client and conduct illegal actions.

2.4 Phishing & Social Engineering

Phishing users for sensitive information by means of fake e-mails or websites[Fig1].

Current statistics highlight the seriousness of such types of fraud. A report by RBI on frauds in 2023 indicates that unauthorized card frauds constitute a quarter of all frauds, identity theft cases have increased by 25 percent, and phishing/social engineering scams have been on the increase by 40 per cent. Cases in Indian banks indicate that financial losses are huge, including account takeover schemes where the loss is in the form of multi-crore unauthorized transfers. The given results underline a dire necessity for adaptive fraud detection systems that can address various types of fraud.

Figure 1. Various Types of Banking Fraud, Including Unauthorized Card Transactions, Identity Theft, Account Takeover, and Phishing [3].

3. Deep Learning Models for Fraud Detection

3.1 Convolutional Neural Networks (CNNs)

CNNs can be utilized in business transaction data even though they were initially applied in image processing as they can be considered spatial patterns. The transactions can be encoded as a structured matrix of features, which makes it possible to use convolutional layers to detect local patterns that are characteristic of fraudulent behavior. In this way, CNNs can identify minor correlations and abnormalities between various features that are not recognized by traditional models. Consequently, CNN-based fraud detection systems will be able to reach high accuracy levels in the detection of suspicious activities in bank transactions [4].

3.2 Recurrent Neural Networks (RNNs) and LSTMs

The models are particularly applicable to time series data whereby the data consists of a series of transactions that occur over time. They can identify patterns and trends as they are able to understand how a particular transaction is connected to the preceding transactions. This ability to consider the time and sequence of events can be used to determine abnormal or suspicious activity. In fraud detection, it implies that they will be able to detect minor changes in behavior that may represent a problem.

3.3 Autoencoders

With a lot of precision, these models are applied to reconstruct data added to them. They exhibit a significant reconstruction error when they encounter something strange- say a fraudulent transaction, they cannot reproduce it properly. Such a divergence between the original and reconstructed data helps in pointing out any suspicious activity. In fraud detection, this can be useful in identifying outlier behaviors that do not reflect normal behaviour.

3.4 Generative Adversarial Networks (GANs)

The models may often be used to create synthetic samples of fraud, which helps in training on how to identify fraud. They create more varied situations for the model can learn by generating realistic fake data. This strengthens the detectors and makes them more prepared to detect real world fraud.

3.5 Graph Neural Networks (GNNs)

Effective in detecting complex fraud through the simulation of relationships between the transactions and the users.

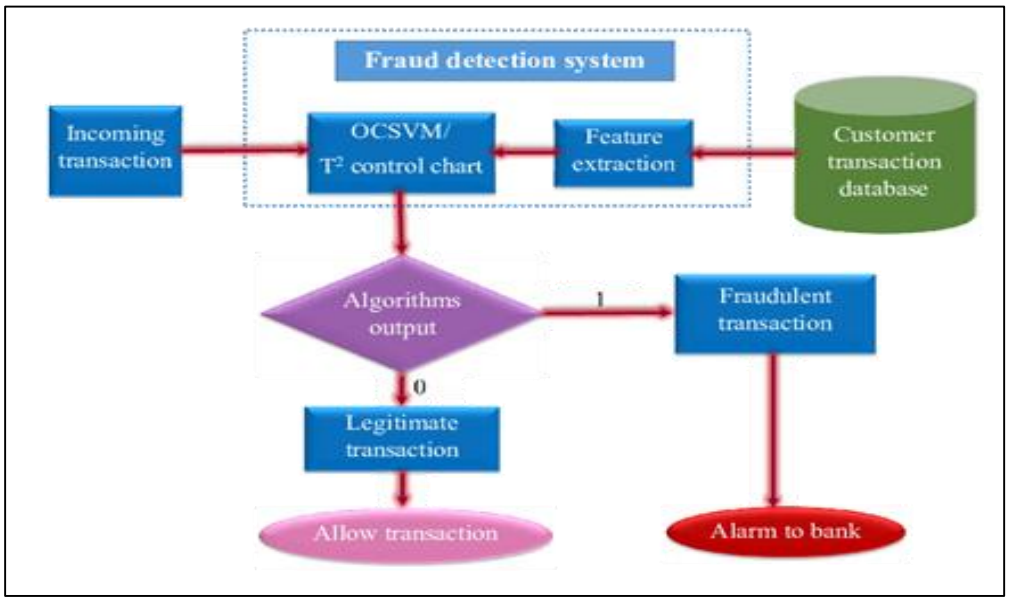

Figure 2. Comparative Architecture of Deep Learning Models for Fraud Detection [5]

4. Explainable AI (XAI) in Fraud Detection

4.1 The Interpretability Requirement

AI decisions need to be interpretable in order to be auditable, belief-worthy to the consumer, and compliant.

4.2 SHAP (SHapley Additive exPlanations)

SHAP (SHapley Additive exPlanations) is based on cooperative game theory where each feature is an agent that works together to make a model prediction. It assigns Shapley values in proportion to each attributes contribution to the output. For fraud detection, SHAP can assist the analyst in determining parameters like the amount of the transaction, device ID, or location that would increase or reduce the likelihood of a transaction being tagged as a fraud. This type of interpretability can enable SHAP to be used alongside compliance, auditing, and model fine-tuning to reduce false positives.

4.3 LIME (Local Interpretable Model-Agnostic Explanations

LIME (Local Interpretable Model-Agnostic Explanations) is based on the idea that, for every prediction, input examples are perturbed and on the perturbed examples, a model (such as a linear model or a decision tree) is trained that is interpretable (i.e., very easy to interpret).

This gives human-interpretable explanations for individual forecasts. To the extent that it determines fraud, LIME can explain why a specific transaction has been marked as fraud, enabling an investigator to follow trends such as the frequency of a suspect merchant ID or an anomalous swing in transaction volume [6]. With this model, SHAP assigns the weight of every feature to the prediction so that fraud analysts can see which features (e.g., transaction amount, device ID, time delta) were most likely to have resulted in a transaction being labeled as fraud. This is validated by LIME providing human-readable short explanations for every alerted case. Overall, these methods make deep learning models extremely accurate and insightful, thereby complying with transparency regulation standards.

4.4 Attention Mechanisms

Attention allows models, especially those dealing with sequential data like transactions, to highlight the most significant segments of an input sequence during prediction. Instead of treating all transactions equally, the model can learn to focus on which specific past activities matter most. Attention layers in fraud detection identify suspect segments within transactions, allowing for a deeper understanding of why a given customer profile or transaction behavior was triggered [Fig3].

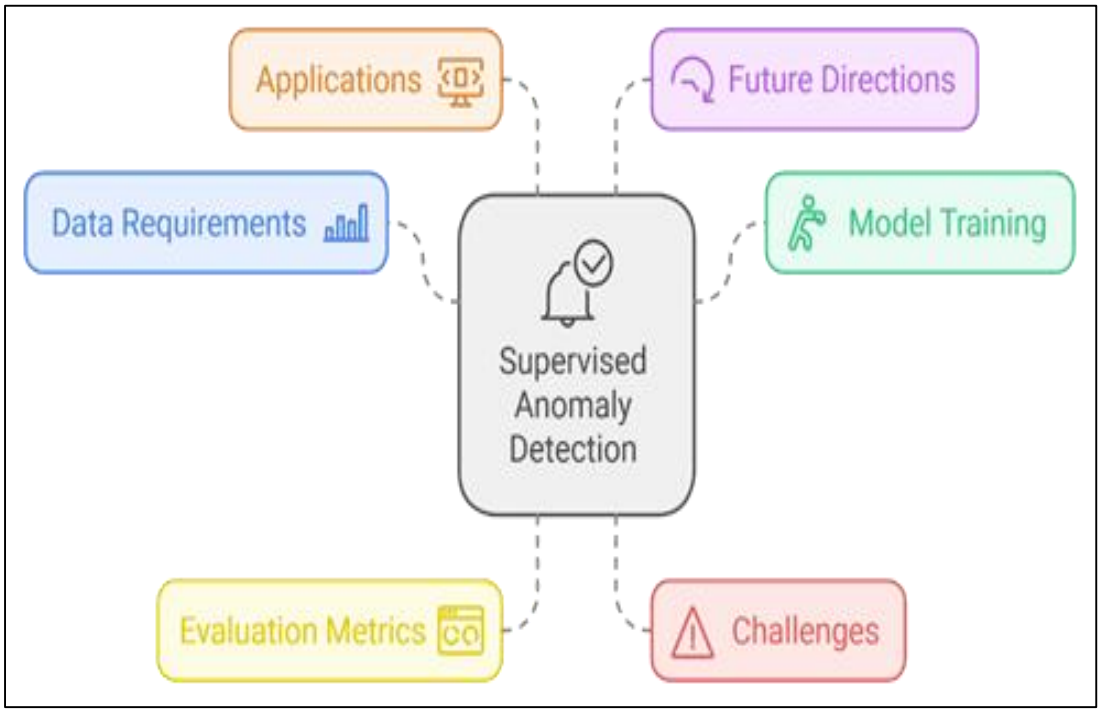

Figure 3. SHAP Explanation of Transaction Anomaly Detection [7]

4.5 Methodology

1. Dataset Selection: We have used public datasets and popular datasets (Kaggle Credit Card Fraud, IEEE-CIS, PaySim, IBM Synthetic Financial Dataset) to identify the most significant attributes of the dataset like size, fraud rate, and availability of features.

2. Model Review: The use of deep learning models in fraud detection algorithms for sequential, high-dimensional, and graph data is to be determined. We conducted a comprehensive review of deep learning models such as CNNs, RNNs, LSTMs, Autoencoders, and GNNs.

3.Explanation Assessment: We considered how much XAI methods (SHAP, LIME, Attention) can be embedded in these models and how interpretability can be augmented.

4.Evaluation Metrics: To assess the models against their strengths and weaknesses, we evaluated them using performance metrics like Accuracy, Precision, Recall, F1-score and AUC-ROC.

5.Critical Analysis: We attempted to generalize case studies and academic research works (JPMorgan, PayPal, HDFC Bank) in order to generalize findings to real fraud detection deployments.

This exercise will allow for the construction of a comprehensive review that is reproducible and meets modern industry standards

5. Data Sources and Preprocessing

5.1 Public Datasets

- Real-World Card Transaction Fraud Dataset (Kaggle).
- IEEE Fraud Dataset for ML Models.
- PaySim Database financial electronic PaySim

5.2 Data Preprocessing Steps

- Feature engineering.
- Normalization.
- Handling class imbalance using SMOTE/ADASYN.

- Splitting datasets into train/validation/test sets [Table2]

Table 1. Summary of Public Datasets for Banking Fraud Detection

Dataset Name	Source/Provider	Data Type	Size & Records	Key Features	Use Cases
Kaggle Credit Card Fraud Detection	Kaggle (UCI ML Repo)	Anonymized credit card transactions	~284,807 transactions (492 fraud cases)	V1–V28 PCA features, Time, Amount, Class (fraud/legit)	Binary classification, anomaly detection
IEEE-CIS Fraud Detection	IEEE + Vesta Corporation	Identity + transaction data	~1 million transactions	Includes device info, email, card IDs, time deltas	High-dimensional fraud classification
PaySim Financial Simulator	Kaggle	Simulated mobile financial data	~6.3 million records	Simulates M-Pesa mobile transactions, labeled fraud	Mobile money fraud, real-time detection
Synthetic Financial Datasets For Fraud	IBM (Watson)	Synthetic bank transaction data	~1 million records	Merchant codes, location, fraud flag	Training on imbalanced data
BankSim Dataset	UGR (University of Granada)	Simulated bank transactions	~600,000 transactions	Based on agent-based simulation of consumer behavior	Fraud analytics, test algorithms

6. Performance Evaluation Metrics

6.1 Accuracy and Precision

The most frequent measures used to assess classification models are accuracy and precision, yet they are not adequate in the situation of fraud detection because of class imbalance. In real world datasets, the percentage of fraudulent transactions is very small compared to the rest and this can lead to high accuracy even when the model is not able to identify fraud. Precision assists in determining the number of flagged cases that are indeed fraudulent but does not reflect the cases of fraud that have been missed. Thus, these metrics can give a misleading picture of the performance.

$$\text{Accuracy} = \frac{(TP+TN)}{(TP+TN+FP+FN)}$$

Where TP, TN, FP, FN represent true positives, true negatives, false positives, and false negatives.

6.2 Recall and F1 Score

Recall is the ability of a model to detect real instances of fraud and as such is very important in a high-risk situation where undetected fraud is expensive. The F1 score is more informative in cases of imbalanced classes and also gives a balance between precision and recall. In any fraud detection, a high F1 score indicates that the model has good performance in correctly detecting fraud without many false positives. It is a more credible measure for assessing real-life fraud detection models.

$$Precision = \frac{TP}{TP+FP}$$

$$Recall = \frac{TP}{TP+FN}$$

$$F1-Score = 2 \times Precision + RecallPrecision \times Recall$$

Where:

- TP = True Positives
- FP = False Positives
- FN = False Negatives

6.3 AUC-ROC and PR Curves

Area Under the Receiver Operating Characteristic Curve (AUC-ROC) and Precision-Recall (PR) curves, are good indicators to determine how well a given classification problem is performing with respect to various thresholds. Such curves facilitate the visualization of the trade-off between true positives and false positives that is highly important in imbalanced datasets such as fraud detection. The ROC curves are biased against the imbalance in classes; hence, PR curves represent the performance more accurately in situations of imbalance. These visual tools help in the identification of the best thresholds for fraud detection models. The bar graph in Figure 4 shows that LSTM and GNN models outperform CNN, RNN, and Autoencoders. This is because LSTMs capture temporal dependencies in sequential transaction

data, identifying subtle behavioral patterns over time, while GNNs model complex relationships between entities (such as customers, merchants, and devices) to uncover fraud rings or collusive activities. These architectures adapt better to evolving fraud strategies, which explains their superior F1-scores compared to other models [Fig4].

The AUC-ROC curve is used to quantify the area below the receiver operating characteristic curve, indicating how effectively a model separates fraud from non-fraud cases. PR curves concentrate on the tradeoff involving precision and recall, which is a more informative measure in cases of uncommon fraud. Accuracy and Precision are helpful but Recall and F1-score are essential to fraud detection since it is much more expensive to miss a fraud case (false negative) than to raise a false alarm (false positive). The use of AUC-ROC and PR curves also indicates the extent to which models differentiate between fraudulent and legitimate classes with different thresholds which is important in an unbalanced dataset.

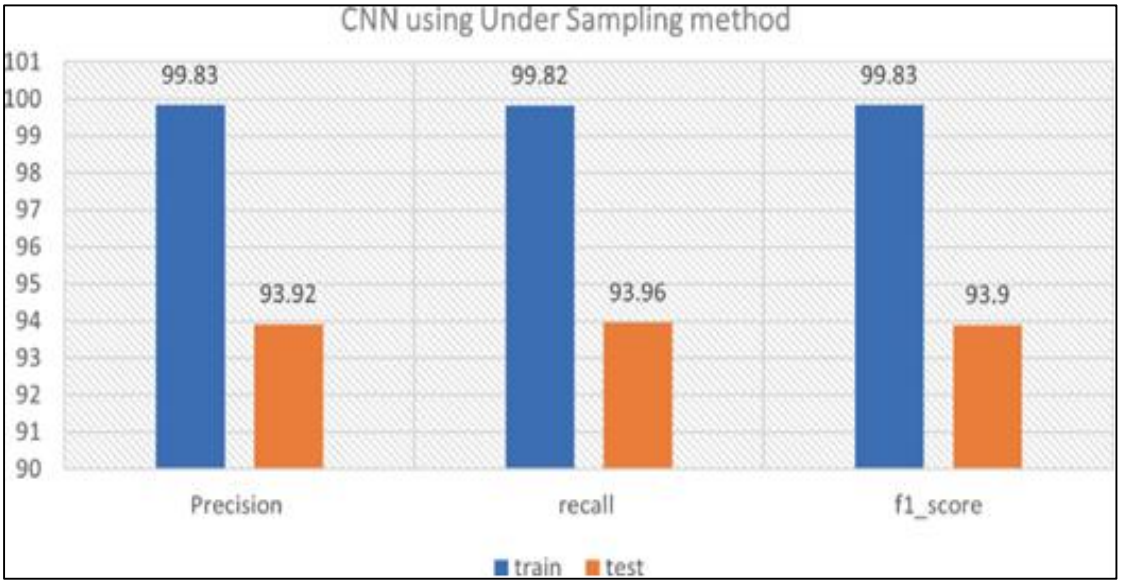

Figure 4. F1-Score Comparison of DL Models on Fraud Datasets [8]

7. Hybrid and Ensemble Approaches

7.1 Combining ML and DL

Deep learning (DL) and machine learning (ML) hierarchical architecture allow top-level pattern learning and bottom-level sequential dependence learning by the system. For instance, LSTM layers may be utilized to process time-series transactional data for tracking users' behavior over time, and XGBoost can be utilized as an effective classifier on features learned

by LSTM. Such a model's generalization capability and versatility are enhanced using this multilevel approach to complex fraud patterns. These ensemble techniques prove to be immensely useful in circumstances wherein the fraudulent behaviors of the context prove to be adaptive in nature and cannot be distinguished by virtue of any form of approach.

7.2 Bagging and Voting Techniques

Voting and bagging can be termed general bagging and ensemble voting of various classifiers making an effort to obtain more authentic estimations. In an election setting, all models are forced to vote for the classification option and the result of the models is presumptively a majority or average of the models. Bagging is the process of training multiple models on multiple random subsets of the data in an attempt to reduce variance and prevent overfitting. These processes are also utilized in fraud detection, where model heterogeneity leads to a more extreme capacity of the system to detect rare and weak patterns of fraud.

8. Challenges in Deep Learning-Based Fraud Detection

8.1 Data Imbalance

The size of the collection of fraud cases is often very small relative to all the transaction data hence giving highly unbalanced data. The biases create a serious issue for deep learning models because they are biased towards the dominant class, thereby disregarding the rare, but crucial patterns that pertain to fraudulent activity.

8.2 Adversarial Attacks

The input characteristics can be slightly modified (increasing the amount of a transaction, changing physical location, or altering the time of day) to enable attackers to manipulate the model's predictions and evade detection. The weaknesses in deep learning models can be exploited through such minor applications of intentional manipulation, causing the models to identify fraud as legitimate.

8.3 Latency and Real-time Detection

Fraud detection models used in practical banking systems should provide predictions in a fraction of a second to ensure unauthorized transactions are prevented. Delayed processing

caused by high inference time adversely affects the user experience and the overall security of the system.

8.4 Privacy and Regulatory Compliance

Strict data protection laws such as GDPR in Europe and RBI policies in India must be adhered to by fraud detection systems to safeguard user data responsibly. Such regulations often require anonymization, transparency, and explainability of the models, making them more challenging to design and even more difficult to deploy.

9. Future Directions and Research Opportunities

9.1 Federated Learning

Federated learning provides a group of banks or other financial institutions with a chance to train a shared fraud detection model without exchanging sensitive customer information. Such an approach will not only prevent the violation of data privacy, but it will also help increase model accuracy since it will be trained on different transaction patterns between financial institutions.

9.2 Self-Supervised Learning

Self-supervised learning is a way of modeling that allows the model to learn useful information from unlabeled data by creating training signals automatically. This implies that the model does not require a large input of manually labeled cases of fraud, which are rather difficult to locate in the banking sector and are quite costly to label. Self-supervised learning can help develop an effective fraud detection system using few labeled data, as the factor that reduces the success of the system is the reliance on labeled data, which is minimized in self-supervised learning. It is also a solution that works well in financial institutions with large volumes of raw transaction data

9.3 Real-time XAI Dashboards

Real-time Explainable AI (XAI) dashboards help create interactive visual representations of how models detect fraud, and these can delve deeply using tools such as SHAP, LIME, and attention mechanisms. These dashboards empower fraud analysts and

compliance teams to comprehend, trust, and endorse model deliverables in rigorous financial situations.

10. Case Study: Real-World Implementation

10.1 JPMorgan Chase

JPMorgan Chase has been using deep learning models with explainable A.I. (XAI) to improve the capability of spotting wire fraud. With this combination, the bank can detect suspicious transactions with a high degree of accuracy and explain why a certain transaction was highlighted, creating transparency and compliance with laws.

10.2 HDFC Bank

HDFC Bank has incorporated deep autoencoders, along with business rules, to analyze customer transactions and identify fraudulent transactions. This combination of systems allows the system to identify both the known trends of fraud and subtle undetected anomalies. It makes the system more powerful in terms of detecting fraud.

10.3 PayPal

PayPal's Graph Neural Networks (GNNs) are applied to examine complicated entanglements between individuals, trades, and accounts, making it possible to expose planned fraud franchises. PayPal will be able to match such connections and trace fraudulent attempts that may otherwise not be related to any other activity on its platform by modeling these links [9].

11. Conclusion

The bank fraud detection is a game changing artificial intelligence case where one badly needs accuracy and the ability to interpret. The deep learning models have been found to be exemplary in detecting fraud patterns which are disguised in huge transactional data. Still, the lack of transparency in these models is a big barrier to their universal implementation in the sphere of finance, where the image of accountability and the sale of regulatory compliance is a must. The integration of Explainable AI techniques has been encouraging to curb such disadvantages by ensuring that black-box models are more explainable and defendable.

Methods like SHAP, LIME, and attention are not only interpretable but also establish trust between stakeholders of fraud analysts, auditors, and customers. The provided paper has conducted a survey on the existing studies on deep learning models, strategies toward XAI, datasets, performance metrics, and practical applications. Despite the current models proving quite effective, one cannot overlook issues including data imbalance, adversarial fraud or real time detection demands. The practice of performing fraud detection will change in the upcoming developments in both federated and self-supervised learning, as well as in real time explainability dashboards. Lastly, the digital financial ecosystem's security will be founded on a responsible, explicable AI strategy.

Regulatory agencies must also engage with developers of AI in the development of an open standard for evaluating fraud detection systems. As fraud schemes evolve, it will continue to be a differentiating factor in AI applications within the financial industries, where the power of prediction and interpretability has always been a touch-and-go in understanding the capabilities of AI.

References

[1] Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics, 6(1), 110-132.

[2] Mill, Eleanor Ruth, Wolfgang Garn, Nicholas F. Ryman-Tubb, and Christopher Turner. "Opportunities in real time fraud detection: an explainable artificial intelligence (XAI) research agenda." International Journal of Advanced Computer Science and Applications 14, no. 5 (2023): 1172-1186.

[3] BizNext. (2024, December 18). Digital fraud: India’s wild frontier. Retrieved August 28, 2025, from https://biznext.in/blog/digital-payment-frauds-in-india/

[4] Sai, Chaithanya Vamshi, Debashish Das, Nouh Elmitwally, Ogerta Elezaj, and Md Baharul Islam. "Explainable ai-driven financial transaction fraud detection using machine learning and deep neural networks." Available at SSRN 4439980 (2023).

[5] Tran, Phuong Hanh, Kim Phuc Tran, Truong Thu Huong, Cédric Heuchenne, Phuong HienTran, and Thi Minh Huong Le. "Real time data-driven approaches for credit card

fraud detection." In Proceedings of the 2018 international conference on e-business and applications, pp. 6-9. 2018.

[6] Aljunaid, Saif Khalifa, Saif Jasim Almheiri, Hussain Dawood, and Muhammad Adnan Khan. "Secure and transparent banking: explainable AI-driven federated learning model for financial fraud detection." Journal of Risk and Financial Management 18, no. 4 (2025): 179.

[7] Rapid Innovation. (n.d.). AI-Powered Anomaly Detection 2024 Ultimate Guide | Boost Efficiency. Retrieved August 28, 2025, from https://www.rapidinnovation.io/post/ai-in-anomaly-detection-for-businesses

[8] Illanko, Kandasamy, Raha Soleymanzadeh, and Xavier Fernando. "A big data deep learning approach for credit card fraud detection." In Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021, Singapore: Springer Nature Singapore, (2022): 633-641.

[9] Ahmadi, Sina. "Advancing fraud detection in banking: Real-time applications of explainable ai (xai)." Journal of Electrical Systems 18, no. 4 (2022): 141-150.

[10] Kute, Dattatray Vishnu, Biswajeet Pradhan, Nagesh Shukla, and Abdullah Alamri. "Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review." IEEE access 9 (2021): 82300-82317.

[11] Talaat, Fatma M., T. Medhat, and Warda M. Shaban. "Precise fraud detection and risk management with explainable artificial intelligence." Neural Computing and Applications (2025): 1-31.

[12] Manzoor, Muhammad Faraz, and Muhammad Faran Aslam. "Enhancing banking fraud detection: Role of machine learning and deep learning methods." Premier Journal of Artificial Intelligence 1, no. 1 (2025).

[13] Shrivastava, Vishesh, and Junaid Hussain Muzamal. "Enhancing Transparency and Privacy in Financial Fraud Detection: The Integration of Explainable AI and Federated Learning." In Software and Data Engineering: 33rd International Conference, SEDE 2024, San Diego, CA, USA, October 2024, Proceedings, vol. 2244, p. 139. Springer Nature, (2024): 21-22.

[14] Mazumder, Md Tanvir Rahman, Md Shahadat Hossain Shourov, Iftekhar Rasul, Sonia Akter, and Md Kauser Miah. "Fraud Detection in Financial Transactions: A Unified Deep Learning Approach." Journal of Economics, Finance and Accounting Studies 7, no. 2 (2025): 184-194.

[15] Babu, N. Sugumar, and M. Kotteeswaran. "AI-powered fraud detection in online banking: Using machine learning to improve security." International Journal of Scientific Research in Modern Science and Technology 4, no. 7 (2025): 01-13.

[16] Hashemi, Seyedeh Khadijeh, Seyedeh Leili Mirtaheri, and Sergio Greco. "Fraud detection in banking data by machine learning techniques." Ieee Access 11 (2022): 3034-3043.

[17] Saradha, J. "Application of Artificial Intelligence in Fraud Detection in the Banking Sector." EKSPLORIUM-BULETIN PUSAT TEKNOLOGI BAHAN GALIAN NUKLIR 46, no. 02 (2025): 637-649.