Enhancing Banking Fraud Detection: Role of Machine Learning and Deep Learning Methods

Muhammad Faraz Manzoor and Muhammad Faran Aslam

ABSTRACT

Fraud detection in banking is a critical concern as financial institutions face increasing challenges in identifying and preventing fraudulent activities. With the rise of sophisticated fraud schemes, traditional detection methods have proven inadequate, prompting the adoption of machine learning (ML) and deep learning (DL) techniques. This review explores the application of ML and DL methods in banking fraud detection, examining their strengths, limitations, and potential for future improvements. We provide an overview of commonly used ML algorithms such as logistic regression, decision trees, random forests, and support vector machines, as well as advanced DL architectures, including feedforward neural networks (FNNs), convolutional neural networks (CNNs), and recurrent neural networks (RNNs). In this review, key issues are discussed in data preprocessing, such as handling imbalanced datasets, feature engineering, and ensuring data privacy. Emerging trends in fraud detection, including explainable AI, real-time and edge computing solutions, blockchain integration, and synthetic data generation, are highlighted as promising avenues for enhancing detection systems. Despite the significant progress, challenges such as computational complexity, model interpretability, and adversarial attacks remain. This review concludes by emphasizing the need for continued research and collaboration between academia and industry to develop more effective, transparent, and secure fraud detection systems for the banking sector.

Keywords: Banking fraud detection, Machine learning, Deep learning, Imbalanced datasets, Explainable AI

Department of Artificial Intelligence, School of System and Technology, UMT, Lahore, Pakistan

Correspondence to: Muhammad Faran Aslam, Faran.Aslam@umt.edu.pk

Additional material is published online only. To view please visit the journal online.

Cite this as: Manzoor MF and Aslam MF. Enhancing Banking Fraud Detection: Role of Machine Learning and Deep Learning Methods. Premier Journal of Artificial Intelligence 2025;3:100014

DOI: https://doi.org/10.70389/PJAI.100014

Received: 4 February 2025
Revised: 11 February 2025
Accepted: 14 February 2025
Published: 17 March 2025

Ethical approval: N/a
Consent: N/a
Funding: No industry funding
Conflicts of interest: N/a
Author contribution: Muhammad Faraz Manzoor and Muhammad Faran Aslam – Conceptualization, Writing – original draft, review and editing
Guarantor: Muhammad Faran Aslam
Provenance and peer-review: Commissioned and externally peer-reviewed
Data availability statement: N/a

Introduction

Fraud detection is essential for modern banking operations due to the complexity of fraudulent activities. With digital banking, online transactions, and global financial networks becoming more popular than ever before, banks are more exposed to fraud than they've ever been in the past.[1] Fraudulent activities like unauthorized transactions, identity theft, and money laundering lead to massive financial loss and chip away at customer trust and financial institutions' reputation. Industry reports suggest that the global financial industry loses billions of dollars to deception annually, emphasizing the necessity for actual fraud-finding mechanisms. Fraud detection systems effectively preserve the integrity of banking operations, protect the integrity of financial assets, and boost customer confidence in highly competitive markets.[2]

This study explores the application of machine learning (ML) and deep learning (DL) techniques in banking fraud detection, assessing their effectiveness in identifying fraudulent activities such as unauthorized transactions, identity theft, and money laundering. It examines commonly used fraud detection models, preprocessing strategies, and key challenges, including imbalanced data, privacy concerns, and adversarial threats. Additionally, the study highlights emerging trends like explainable AI, blockchain integration, and real-time detection to enhance fraud prevention.

Challenges in Detecting Banking Fraud

Detecting banking fraud is a complex and constantly evolving challenge because fraudulent schemes are dynamic. Fraudsters keep up with the changing technologies and find new ways to attack vulnerabilities in banking systems, which are hard to prevent and detect.[3] The primary challenges include the substantial daily transaction volume, the disproportionate datasets with genuine transactions significantly outnumbering fraudulent ones, and the imperative for real-time detection to mitigate losses by identifying fraud proactively. Furthermore, false positives (where legitimate transactions are reported as fraudulent) can result in losing the customer's trust and operational inefficiencies. The variations in fraud, from credit card fraud to elaborate money laundering schemes, make it problematic to create a one scope fits all solution.[4] These problems require adaptive tools and techniques for changing fraud patterns.

The rest of the paper is structured as follows: Section Background outlines the evolution of detection techniques from manual inspection to rule-based systems and the recent shift towards ML and DL applications. This section also covers the types of banking fraud and the need for advanced detection methods. Section Common Fraud Detection Methods covers key ML and DL models. Section Preprocessing Techniques discusses handling imbalanced data, feature engineering, and privacy concerns. Section Challenges and Limitations highlights computational complexity, interpretability, and adversarial attacks. Section Future Trends explores explainable AI, real-time computing, blockchain, and synthetic data. The paper concludes by stressing the need for further research and industry collaboration.

Role of ML and DL in Enhancing Fraud Detection Systems

In the battle against banking fraud, ML and DL have become transformative technologies. While traditional rule-based systems must be supplied with pre-defined rule and thresholds, ML and DL models can study from the facts and alter to new fraud patterns.[5,6] Random Forest and Gradient Boosting ML algorithms are good at finding anomalies and classifying transactions as

fraudulent or legitimate using historical data. However, DL models like convolutional neural network (CNN) and recurrent neural network (RNN) are powerful in analyzing complex patterns, sequential data, and high-volume datasets. These technologies allow banks to detect frauds with higher accuracy, lower false positives, and spot emerging fraud patterns in tangible time.[7] Furthermore, the combination of ML, DL, and big data analytics coupled with cloud computing has amplified the size and competence of fraud detection systems, which are essential in today's banking.

Objectives and Scope of the Review

This review is not just a summary but a comprehensive analysis of the application of ML and DL techniques in banking fraud detection. We delve into the strengths and limitations of different algorithms, outline the challenges of implementing them, and highlight future trends in this area. The review synthesizes recent studies and practical applications to deeply understand how ML and DL are revolutionizing fraud detection. We have covered all possible aspects of the subject, including supervised and unsupervised learning, hybrid models, and advancements in explainable AI. Our aim is not just to provide information but to empower scholars, practitioners, and policymakers with the knowledge they need to design and develop more effective and efficient fraud detection systems.

Background

Fraud detection in banking has evolved significantly with the rise of digital transactions and sophisticated financial crimes. Traditional rule-based systems have proven insufficient against rapidly changing fraud tactics, leading to the adoption of ML and DL techniques. These technologies enable banks to detect anomalies, predict fraudulent behavior, and enhance security in real-time.

Overview of Fraud Types in Banking

Banking fraud is more than one type of fraud activity that attempts to deceive banks, financial institutions, and their customers for financial advantage; it also does not have one category.[8] Credit card fraud is one of the most common types of fraud, in which someone uses stolen or counterfeit credit card information to make unauthorized transactions. With the expansion of e-commerce and contactless payments, this fraud is quickly becoming rampant. The other significant type of fraud is loan fraud, where people or others make false statements to get loans but not repay them, causing huge losses to the banks.[9] Another common problem is identity theft, in which fraudsters steal personal information to impersonate someone else, using their stolen identities to open new accounts or to expand unauthorized admittance to their accounts. Finally, banking institutes face the challenge of money laundering, which is concealing illegal proceeds obtained by moving them through legitimate financial channels.[10.] Detection of each of these fraud types requires specific methods tailored for the mechanism of each and the impact they have.

Traditional Fraud Detection Methods and Their Limitations

Banks have used rule-based systems to sense fraudulent activities. These systems work on fixed rules and thresholds, for example, marking off transactions above a certain value or coming from high-risk locations. Although these methods are easy to instrument and interpret, they are fundamentally reactive and do not possess the adaptivity to keep up with the ever-changing fraud tactics.[9] Moreover, rule-based systems are prone to producing many false positives, which can stop legitimate transactions and make customers unhappy. A traditional method is manual audits, in which experts check flagged transactions for potential fraud. However, this approach is laborious, resource-demanding, and infeasible to apply to the very large number of transactions that banks handle daily in the present day. Traditional methods cannot effectively detect sophisticated and dynamic fraud patterns, suggesting that other methods are necessary.[8]

Advantages of ML and DL Approaches in Fraud Detection

Traditional approaches for fraud recognition do not cover a wide spectrum of frauds. Unlike rule-based systems, ML algorithms can learn from past data and find patterns to identify fraud without predefined rules. Random Forest, Support Vector Machines (SVM), and Gradient Boosting are techniques that can procedure large datasets and can familiarize to novel fraud patterns over time.[11] CNN and Long Short-term Memory (LSTM) networks combine ML with DL models to enhance detection capabilities using complex relationships and sequential data, e.g., transaction histories.

ML and DL approaches provide one of the key advantages of handling imbalanced datasets, in which fraudulent transactions are dwarfed by legitimate ones. These models are made possible with advanced techniques, including synthetic data generation and anomaly detection, to concentrate on rare but critical fraud cases.[12] Further, these approaches can run in real-time, allowing for immediate alerts of potentially suspicious activities, which are key in preventing losses in the financial sector and protecting customer assets. ML and DL systems offer a proactive and scalable solution to continuously changing banking fraud problems.

Common Fraud Detection Techniques and Methods

ML and DL have transformed fraud detection in banking by allowing automated, data-driven decision-making, as shown in Figure 1. ML techniques, such as logistic regression, decision trees, random forests, and gradient boosting, excel in structured data analysis and pattern recognition, offering efficient fraud detection with interpretability. On the other hand, DL methods, including feedforward neural networks (FNN), CNN, RNN, and graph neural networks (GNN), leverage hierarchical feature learning to detect intricate fraud patterns in complex and unstructured data. While ML models are computationally efficient and interpretable, DL techniques better capture hidden correlations and evolving fraud patterns.

DOI: https://doi.org/10.70389/PJAI.100014 | Premier Journal of Artificial Intelligence 2025;3:100014

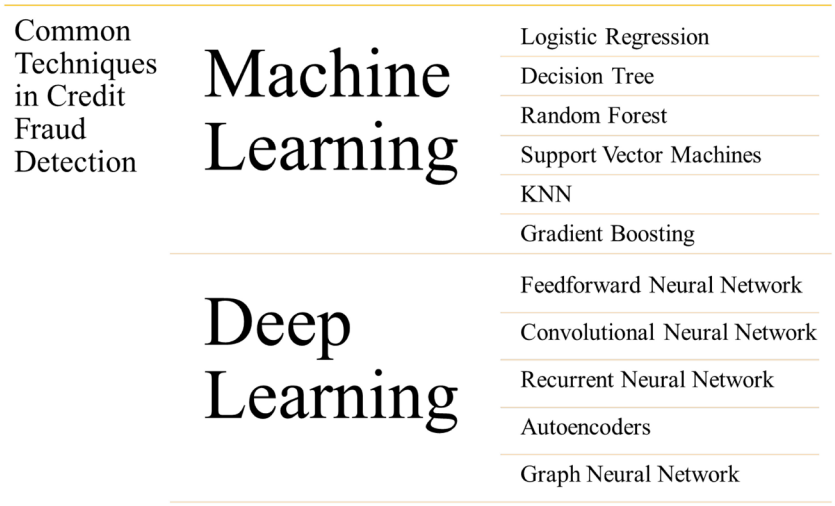

Fig 1 | Common techniques and methods in credit fraud detection

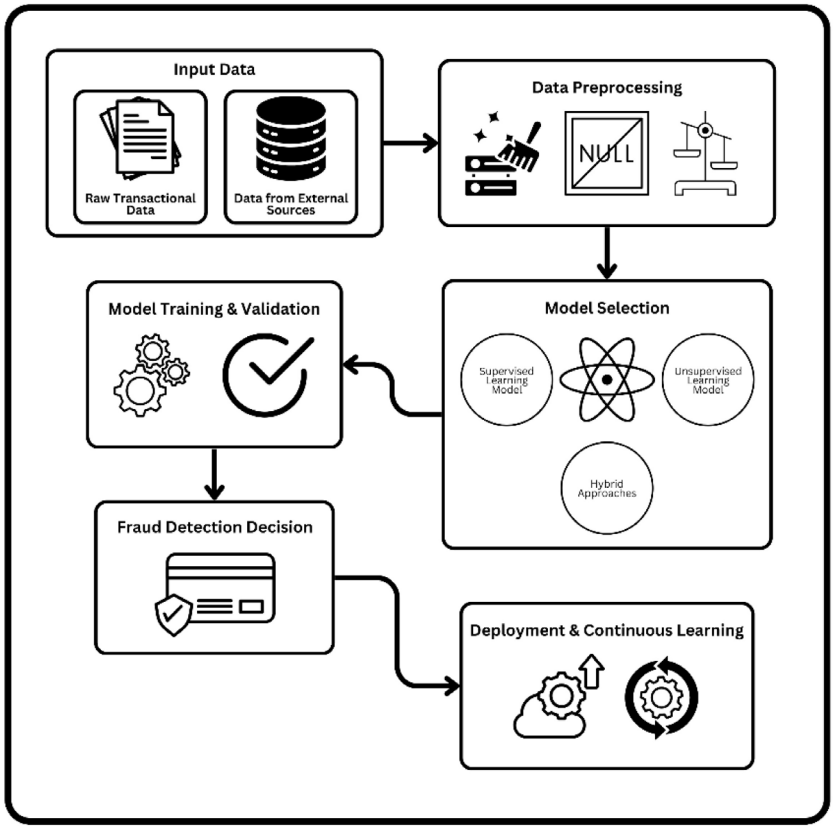

Fig 2 | General architecture of ML practices in credit fraud detection

ML Techniques for Fraud Detection

ML has transformed fraud detection in banking by allowing automated, data-driven decision-making, as shown in Table 1. Various ML algorithms, counting logistic regression, decision trees, random forests, support vector machines (SVM), K-nearest neighbors (KNN), and gradient boosting methods like XGBoost and LightGBM have been widely applied to identify fraudulent transactions. These techniques leverage past transaction data to notice irregularities and outlines related to fraudulent activities. ML models enhance fraud detection by refining accuracy, reducing false positives, and enabling real-time monitoring of banking transactions. The general process of ML techniques implementation in credit fraud detection is revealed in Figure 2.

Logistic Regression

We use logistic Regression in fraud detection because it is easy to interpret. A logistic function is used to model the probability of a binary outcome (e.g., fraudulent or legitimate).[13] The equation for Logistic Regression is:

$$P(y=1 \mid X)=\frac{1}{1+e^{-(\beta_0+\beta_1 X_1+\beta_2 X_2+\ldots+\beta_n X_n)}} \quad (1)$$

Where $P\ (y = 1|X)$ is the probability of a transaction being fraudulent; $X_1 + X_2 +...+ X_n$ are the input features; $\beta_0 + \beta_1 + \beta_2 +...+ \beta_n$ are the coefficients learned during training. Logistic regression is a perfect fit for linear relationships; it outputs a probabilistic value that can be used for making threshold-based decisions in case of fraud detection.[14] However, imbalanced datasets can be handled by a proposed reliable logistic regression model for credit card fraud detection, as proposed by Hmidy and Ben Mabrouk.[15] Worth mentioning is that Mohammed and Maram[16] also used logistic regression to discover credit card fraud, showcasing its simplicity of implementation and ease of interpretation. Further, Cheng[17] has compared logistic regression with other ML algorithms for credit card fraud detection, where logistic regression balances simplicity and predictive performance.

Decision Trees

Non-parametric supervised learning methods for classification and regression tasks are decision trees. They are recursive since they create a tree-like structure, splitting the data at each feature value.[18] For splitting criterion, we use metrics such as Gini Impurity or Information Gain. For Gini Impurity, the formula is:

$$Gini = 1 - \sum_{i=1}^{C} P_i^2 \quad (2)$$

Where P_i^2 is the proportion of samples belonging to class *i*; *C* is the entire quantity of classes. Moreover, Sahin and Duman[19] projected a cost-sensitive decision tree approach for detecting frauds whose performance was shown on imbalanced datasets. Moreover, Martins et al.,[20] present RIFF, a method to induce rules for fraud detection from decision trees, improving performance and interpretability. Decision Trees are an intuitive technique for identifying fraudulent transactions based on complex feature interactions and can capture nonlinear patterns.

Random forest

Random forest is an ensemble learning technique associating multiple decision trees to increase evolution

accuracy and reduce overfitting. The forest is trained by training each tree on some randomly particular subset of the data and then aggregating the outputs of all the trees (for example, by taking the average or using majority voting).[21] The formula for the aggregation is:

$$\hat{y} = \frac{1}{T}\sum_{t=1}^{T} h_t(X) \tag{3}$$

Where T is the number of trees; $h_t(X)$ is the prediction of the t tree; $\hat{y}$ is the aggregated output. Xuan and Liu[22] showed the effectiveness of Random Forest applied to credit card fraud detection, differentiating fraudulent transactions from normal ones. Liu et al.,[23] built a financial fraud detection model using Random Forest, outperforming other methods to detect fraudulent activities. Random Forest is a popular choice for fraud detection since it is robust to noisy data and can operate on high-dimensional datasets.

Support Vector Machines (SVM)

Since SVM is a powerful algorithm for classification tasks, it works best in cases where data points are not linearly separable. It finds a hyperplane that has a maximum margin between the two classes.[24] The optimization problem for SVM is:

$$\min_{w,b} \frac{1}{2} \vee \| w \| \, y_i \left(w^T x_i + b \right) \geq 1, \forall i \tag{4}$$

Where $\frac{\| \vee \|^2}{\| \vee w \|}$ is the weight vector; bb is the bias; ($w^T x_i + b$) are the input features; y_i are the labels. SVM uses the kernel trick to map the data into an advanced dimension, from which it can pick out these complex fraud patterns. Sahin and Duman[19] showed how SVMs apply to credit card fraud detection, showing that SVMs are very good at separating fraudulent transactions. Second, Bhattacharyya et al.[25] applied SVMs to credit card fraud detection, founded on the advantages of SVMs in dealing with imbalanced data and noticing complex patterns present in the transaction data.

K-nearest Neighbors (KNN)

KNN is a simple instance-based learning algorithm that classifies a sample by a majority vote of its kk nearest neighbors in the feature space.[26] The distance between points is typically calculated using metrics such as Euclidean distance:

$$d\left(x_i, x_j\right) = \sqrt{\sum_{k=1}^{n} \left(x_{ik} - x_{jk}\right)^2} \tag{5}$$

Where $d(x_i, x_j)$ refers to the Euclidean distance between two points. x_{ik}: k^{th} feature of point x_i . x_{jk}: k^{th} feature of point x_j . n: Total number of features. $\sum_{k=1}^{n}$: Summation over all features from 1 to n.

Saeed and Abdulazeez[27] have compared KNN, Random Forest, and Logistic Regression in credit card fraud detection, and it has been found that KNN is more effective in identifying fraudulent transactions. Rzayeva and Malekzadeh[28] proposed a hybrid approach that uses a combination of deep neural networks and KNN, which is very accurate in detecting fraudulent activities. It is a simple, instance-based learning algorithm that categorizes a sample with the common of a sample's kk nearest neighbors in the feature space.

Gradient Boosting

Gradient boosting is an ensemble method that constructs models sequentially, and each of these models tries to improve the error of the previous model. It iteratively builds up the weak learners (normally Decision Trees) until a loss function is minimized.[29] The general formula for the model is:

$$F_m(x) = F_{m-1}(x) + \eta \, . \, h_m(x) \tag{6}$$

Where $F_m(x)$ is the updated model; $F_{m-1}(x)$ is the previous model; η is the learning rate; $h_m(x)$ is the new weak learner. In the problem of credit card fraud detection, Ding et al.,[30] suggested an AutoEncoder-enhanced LightGBM method, in which DL is combined with gradient boosting, which is more accurate than the state-of-the-art. For instance, Xu et al. [31] combined the neural networks and gradient boosting to recover representation learning and interpretability and named their approach Deep Boosting Decision Trees to detect fraud. XGBoost and LightGBM, popular implementations of Gradient Boosting, offer scalability and efficiency, making them ideal for large-scale fraud detection tasks.[32]

ML techniques for banking fraud detection vary in complexity, interpretability, and computational efficiency. Logistic Regression is simple and fast but struggles with non-linear data. Decision Trees and Random Forests handle non-linearity well, though trees overfit easily, while forests are more robust but computationally expensive. Support Vector Machines (SVMs) are effective in high-dimensional spaces but require careful tuning and are resource-intensive. K-Nearest Neighbors (KNN) is easy to implement but inefficient for large datasets. Gradient Boosting methods (e.g., XGBoost, LightGBM) achieve high accuracy and handle imbalanced data well but require careful hyperparameter tuning. Each method has trade-offs, making model selection crucial based on dataset size, complexity, and real-time processing needs.

Applications of ML in Various Banking Fraud Scenarios

ML techniques have been successful applications in fraud detection scenarios across banking. Simple and fast: Logistic regression and decision trees are often used for real-time transaction monitoring. Random Forest and Gradient Boosting are used to detect credit card fraud (the last column is a feature indicating whether the transaction is fraudulent) and loan fraud

DOI: https://doi.org/10.70389/PJAI.100014 | Premier Journal of Artificial Intelligence 2025;3:100014

Table 1 | Comparison of ML techniques in fraud detection

Technique	Key Features	Strengths	Limitations	Typical Applications	References
Logistic Regression	The probabilistic model assumes a linear relationship between features and output.	Simple, interpretable, fast to train and deploy.	Assumes linear separability; limited performance on complex, non-linear data.	Real-time transaction monitoring.	13–16
Decision Trees	Tree-like structure; uses metrics like Gini or Information Gain for splits.	Easy to interpret; handles non-linear data; no need for feature scaling.	Prone to overfitting; sensitive to noisy data.	Fraud pattern detection, small datasets.	18–20
Random Forest	Ensemble of decision trees; aggregate predictions via voting or averaging.	Robust to overfitting; handles high-dimensional data; good generalization.	Computationally expensive; less interpretable than single Decision Trees.	Credit card fraud, loan fraud detection.	21–23
Support Vector Machines (SVM)	Finds optimal hyperplane for classification; uses kernel functions for non-linearity.	Effective for high-dimensional spaces; robust to overfitting with proper kernel selection.	Computationally intensive for large data sets; requires careful tuning of hyperparameters.	Identity theft detection, anomaly detection.	19,24,25
K-Nearest Neighbors (KNN)	Instance-based: classifies based on a majority vote of nearest neighbors.	Simple to implement; works well for small datasets.	Computationally expensive for large datasets, performance degrades with high-dimensional data.	Fraud detection in small datasets.	26–28
Gradient Boosting (e.g., XGBoost, LightGBM)	The sequential ensemble method minimizes loss function iteratively.	High accuracy; handles imbalanced datasets; scalable and efficient implementations available.	Sensitive to hyperparameter tuning; risk of overfitting without proper regularization.	Large-scale fraud detection, real-time analysis.	29–32

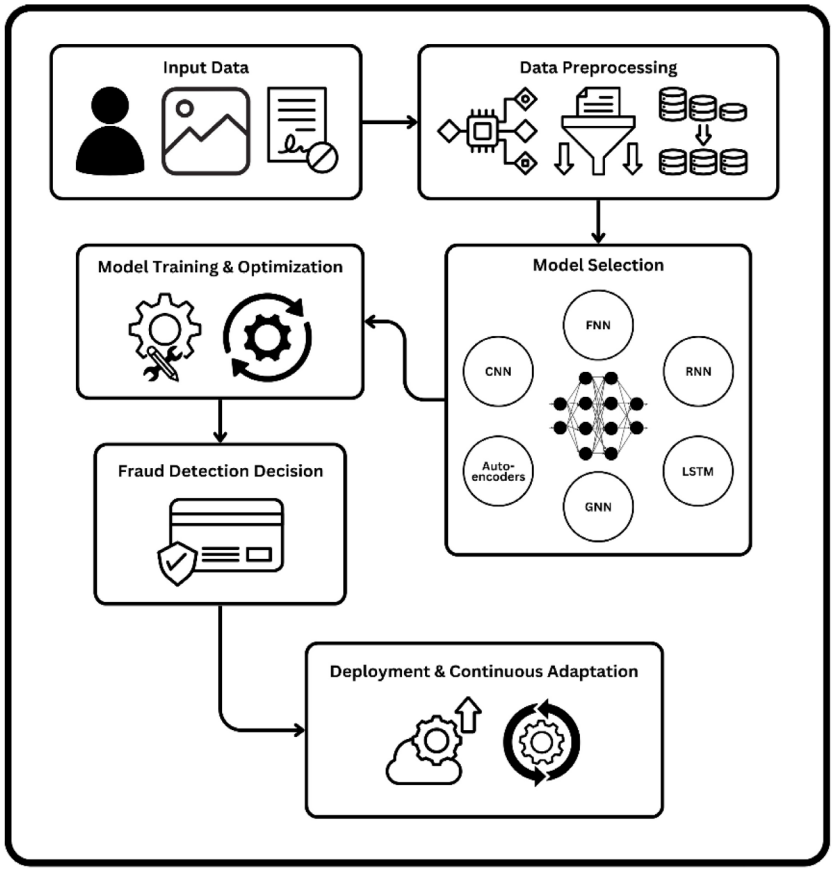

Fig 3 | General architecture of DL techniques in credit fraud detection

(features are ratios of the size of the loan to the business's credit limit, area of business, etc.) based on patterns in historical data.[12] Identity theft detection is applied using SVM and KNN, which consists of recognizing the anomalies in customer behavior.[33] The ability of these ML techniques to accurately adapt and address the multitude of ever-changing banking frauds makes these techniques extremely valuable in the round in contradiction of banking fraud.

DL Techniques for Fraud Detection

DL has become a powerful tool for fraud detection in banking, offering the capability to detonate complex patterns in vast and high-dimensional datasets, as shown in Table 2. Unlike traditional ML models, DL architectures such as FNN, CNN, RNN, LSTM networks, Autoencoders, and Graph Neural Networks (GNN) can more effectively process sequential, unstructured, and graph-based data. These models enhance fraud detection by identifying intricate transaction relationships, reducing false positives, and adapting to evolving fraud tactics. The general process of DL techniques implementation in credit fraud detection is exposed in Figure 3.

Introduction to DL and Its Relevance to Fraud Detection

ML, in particular a subset called DL, uses artificial neural networks (with multiple layers, hence "deep") to study complex patterns from data. Fraud detection is a typical use case for these models since they can contract with large-scale, high-dimensional data and capture complicated relationships in data.[34] Traditional ML models, which are based on feature engineering, cannot pick up sophisticated fraud patterns like DL algorithms, which can automatically extract relevant features from raw data. As the volume and complexity of financial transactions grow, DL provides a powerful means to enhance the accuracy and efficiency of fraud detection systems by providing real-time monitoring and dynamic fraud tactic adaptation.[32]

Feedforward Neural Networks (FNN)

The simplest and most commonly used styles of DL are FNN. FNNs are where data runs only in one way from an input to an output without any cycles or loops. It has an input layer, one or multiple hidden layer(s), and an output layer.[35] Applying the activation function like the sigmoid or ReLU function to the weighted sum of inputs determines its output. Moreover, Jameel and George[36] used an FNN to detect phishing emails based

on features extracted from the email headers and HTML bodies. The results show that FNNs are a good approach for detecting fraudulent communications, with a high accuracy rate of 98.72%. The general equation for an FNN is:

$$y = f\left(\sum_{i=1}^{n} w_i x_i + b\right) \tag{7}$$

Where x_i are the input features; w_i are the consistent weights; b is the bias term; f is the activation function. In the application of fraud detection, FNNs are used to categorize transactions as either legitimate or fraudulent based on patterns learned. It is very effective if the relations between features are complex but not sequential. Quah and Sriganesh[37] trained a neural network system on a large database of labeled credit card transactions to tell legitimate from fraudulent credit card activities. The results of these studies indicate the capability of FNNs to capture complex connections between features for fraud detection.

Convolutional Neural Networks (CNN) for Image-Based Fraud Detection

Primarily used for image processing, CNN can also be used on fraud detection tasks where data can be represented as a grid. Convolutional layers are used to learn spatial hierarchies of features automatically in CNNs.[38] It applies filters to the input data, which enables it to detect local patterns like edges, textures, and shapes. The equation for a convolution operation is:

$$y(i,j) = (x * w)(i,j) = \sum_{m}\sum_{n} x(m,n)\, w(i-m, j-n) \tag{8}$$

Where x is the input; w is the filter (or kernel); y is the output feature map. In particular, CNNs are well suited for image-based tasks for fraud detection, such as counterfeit documents, forged signatures, and fraudulent checks. Furthermore, transaction patterns can be analyzed as time series images or matrices using the CNNs. For example, Fu et al.,[39] presented a framework based on CNNs for credit card fraud detection that exploits inherent features to elevate sophisticated fraudulent transaction detection. Zhang et al.,[40] designed a CNN-based model to detect online transaction fraud and showed that the model can capture complex patterns typical for fraudulent activities. The versatility of CNNs in working with structured data representations to perform fraud detection is highlighted in these studies.

Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) for Sequential Data

RNNs are designed to handle sequential data that is suitable for fraud detection as both the transaction histories and the fraud detection itself are time-dependent. RNNs keep a hidden state that retains info from previous time steps to model temporal dependencies. However, traditional RNNs suffer from vanishing gradient problems, making it hard to learn over long sequences.[41] This problem is addressed by LSTM networks, which introduce memory cells that store information over longer periods. The equation for an LSTM cell is:

$$f_t = \sigma\left(W_f[h_{t-1}, x_t] + b_f\right) \tag{9}$$

$$i_t = \sigma\left(W_i\ [h_{t-1}, x_t] + b_i\right) \tag{10}$$

$$\hat{C}_t = \tanh\left(W_C\left[h_{t-1}, x_t\right] + b_C\right) \tag{11}$$

$$C_t = f_t * C_{t-1} + i_t * \hat{C}_t \tag{12}$$

$$o_t = \sigma\left(W_o\left[h_{t-1}, x_t\right] + b_o\right) \tag{13}$$

$$h_t = o_t * \tanh\left(C_t\right) \tag{14}$$

Where f_t, i_t, and o_t are the forget, input, and output gates, respectively; C_t is the cell state; h_t is the hidden state. It covers the usage of LSTMs for fraud detection in sequential data, such as time series of transaction sequences or detection of unusual patterns in customer behavior over time. Benchaji and Douzi[42] presented a credit card fraud detection system using LSTM networks as sequence learners to instantiate transaction sequences to capture the historical obtaining behavior of credit card holders and improve fraud detection accuracy. A similar work was proposed by Jurgovsky et al.,[43] that used LSTM networks to model long-term dependencies within a transaction sequence, which can help detect fraudulent activity by considering the temporal dynamics of user behavior.

Autoencoders for Anomaly Detection

In an unsupervised neural network, autoencoders learn to compress data into a lower dimensional representation (encoding) and recreate it to the original data (decoding) for anomaly detection.[44] The network is trained to minimize the reconstruction error, and outliers are detected by their high reconstruction error. When labeled data is scarce, Autoencoders are particularly successful in fraud detection. An anomalous transaction refers to those transactions that deviate significantly from the normal transaction patterns, a common characteristic of fraudulent activities, and can be used to identify such transactions.[45] The general objective of an autoencoder is to minimize the loss function:

$$L(x, \hat{x}) = \| \vee x - \hat{x} \|^{\| \vee \|^2} \tag{15}$$

Where x is the input; $\hat{x}$ is the reconstructed output. For example, Pumsirirat and Yan[46] used an autoencoder and a Restricted Boltzmann Machine to detect credit card fraud, proving the model effectively detects unusual transactions. Moreover, Yılmaz Çakır and Şirin[47] also proposed an enhanced autoencoder-based fraud detection method that uses noise factor encoding and

DOI: https://doi.org/10.70389/PJAI.100014 | Premier Journal of Artificial Intelligence 2025;3:100014

Synthetic Minority Over-sampling Technique (SMOTE) to further improve the detection performance.

Graph Neural Networks (GNN) for Transaction Network Analysis

Graph neural networks (GNN) are DL models for graph-structured data where nodes correspond to entities (e.g., customers, accounts) and edges indicate relations between different entities (e.g., transactions, interactions).[34] In these scenarios where fraudsters act together across multiple accounts or transactions and form a dense web of fraudulent activities, GNNs are good at fraud detection. The graph convolution operation in a GNN is defined as:

$$h_v^{(k+1)} = \sigma\left(W^{(k)} \cdot \sum_{u \in N(v)} h_n^{(k)} + b^{(k)} \right) \quad (16)$$

Where $h_v^{(k+1)}$ is the updated node feature; $W^{(k)}$ is the weight matrix at layer k; $u \in N(v)$ represents the neighbors of node v. Dou et al.[48] introduced a GNN-based model, which enhances fraud detection by leveraging label information inside the graph structure and helps predict fraud nodes more accurately. Furthermore, Lou et al.[6] developed a GNN solution that leverages context encoding and adaptive aggregation while detecting fraudulent activities regarding the overall transactional context. The result is that these studies show that GNNs are effective for modeling complex relational data for fraud detection. GNNs excel in fraud detection, where the problem is capturing fraudulent transaction patterns across multiple entities, e.g., money laundering schemes or coordinated fraud rings.[49]

DL techniques offer powerful solutions for fraud detection but come with computational challenges. FNNs effectively model complex non-linear relationships but are limited to non-sequential data. CNNs excel in image-based fraud detection but require large datasets and high computational resources. RNNs and long short-term memory (LSTMs) capture temporal dependencies, making them ideal for transaction sequence analysis, though they demand careful tuning. Autoencoders are effective for anomaly detection in unsupervised settings but require precise reconstruction error thresholds. Graph neural networks (GNNs) leverage network structures to detect complex fraud patterns, such as money laundering but are computationally intensive. Model selection depends on data structure, computational constraints, and fraud detection objectives.

Preprocessing Techniques

The quality and quantity of data are very important for ML and DL models on fraud detection. Whether the datasets are relevant and the preprocessing applied to them is available or not greatly influences the efficiency of fraud detection systems.[5] For this, we explore common data preprocessing issues that manifest and their mitigation, data privacy, and the development of appropriate ethical considerations.

Data Preprocessing Challenges and Solutions

Data preprocessing plays a huge part in the fraud detection pipeline. The raw data usually needs massive cleaning and transformation before it can go into model training. Fraud detection involves some common preprocessing challenges like imbalanced dataset handling, feature engineering & selection, and missing and noisy data handling, as shown in Table 3.[10]

Zahra et al. [50] studied preprocessing techniques on a credit card fraud dataset using four collective classifiers, pointing out that feature extraction and data sampling are essential for improving detection performance. Moreover, Zainab et al.,[51] mentioned data preprocessing steps like cleaning, integration, feature selection, and data transformation, which are important to dealing with imbalanced datasets for fraud detection.

Handling Imbalanced Datasets

A problem with fraud detection datasets is that they are typically highly imbalanced: fraudulent transactions are a small percentage of the total. Because legitimate transactions dominate it during training, this imbalance can result in biased models that tend to predict all transactions are legitimate. To deal with this,

Table 2 | Comparison of DL techniques in fraud detection

Technique	Key Features	Strengths	Limitations	Typical Applications	References
Feedforward Neural Networks (FNN)	Simple architecture, fully connected layers, no temporal dependencies.	Easy to implement; effective for complex non-linear relationships.	Limited to non-sequential data; may struggle with large datasets or intricate patterns.	Transaction classification; general fraud detection.	35–37
Convolutional Neural Networks (CNN)	It uses convolutional layers to detect spatial patterns, primarily for image data.	Excellent for image-based tasks; automated feature extraction.	Computationally intensive; requires large datasets.	Image-based fraud detection (e.g., forged documents).	38–40
Recurrent Neural Networks (RNN) and Long Short-term Memory (LSTM)	Designed for sequential data, LSTMs handle long-term dependencies.	Effective for time-series and sequential data; captures temporal dependencies.	Computationally expensive, LSTMs require careful tuning.	Time-series fraud detection; transaction sequence analysis.	41–43
Autoencoders	Unsupervised learning: learns data compression and reconstruction.	Effective for anomaly detection; works well with unsupervised data.	High reconstruction error threshold tuning is required but limited to complex fraud patterns.	Anomaly detection in transaction data.	44–47
Graph Neural Networks (GNN)	Processes graph-structured data; learns from nodes and edges.	Ideal for fraud detection in networks; captures complex relationships between entities.	It requires graph-structured data and is computationally intensive for large graphs.	Network-based fraud detection; Money laundering.	6,34,48,49

resampling techniques are used; for example, sample the majority class (e.g., legitimate transactions) or oversample the minority class (e.g., fraudulent transactions). SMOTE is a good example of oversampling by creating synthetic examples of the minority class to balance a dataset.[52]

A second method of addressing this issue is cost-sensitive learning, wherein different costs for the misclassification of classes are given, along with heavier penalties for the model attempting to label legitimate transactions as fraudulent. Further, since activities are usually considered anomalies for fraud, anomaly detection techniques are also employed.[53] To overcome the class imbalance in datasets, Chawla et al.,[54] introduced a technique called SMOTE, which creates synthetic minority class examples. Their method is currently seen in many fraud detection applications to improve model performance in imbalanced data. Furthermore, Baloch et al.,[55] propose the Focused Anchors Loss, a cost-sensitive learning approach to enhance the discriminative power of classifiers in imbalanced settings with applications to fraud detection.

Feature Engineering and Selection

Feature engineering is where you generate new features or transform existing ones to make a model that can better spot fraud. Interactions between features are created, data is normalized and scaled, and categorical variables are encoded.[1] In credit card fraud detection, these features indicate fraudulent activity, such as transaction frequency, average transaction amount, and time of day. Feature collection is a significant step in this process, and it eliminates irrelevant or redundant features to decrease dataset dimensionality and improve model performance.

Recursive feature elimination (RFE) and random forest feature importance are popular feature selection techniques,[21] allowing to spot the key features the model can focus on to pick out the most significant fraud indicators. In this direction, Bahnsen et al.,[56] provide credit card fraud detection feature engineering strategies, focusing on manually creating features that represent the behavior of fraudulent transactions. Their study showed that the performance of fraud detection models can be enhanced through engineered features. In the credit card fraud detection problem, Lucas et al.,[57] introduced an automated feature engineering approach through multi-perspective hidden Markov models (HMMs). Their method views sequences of transactions from multiple angles and provides more features that increase the potential of classification tasks in fraud detection.

Dealing with Missing and Noisy Data

Learning from real-world financial transaction datasets and missing and noisy data are common challenges. Data may be missing because of incomplete records or errors in data collection. One of the most used techniques for this issue is imputing missing data, where missing values are substituted by estimated values based on the observed data. Some simple methods are to fill the missing values with the mean, median, or mode of the feature, and more elaborate approaches like the k nearest neighbors (KNN) imputation predict values based on the similarities of the neighboring points.[33] Erroneous or outlier data points that generally do not reflect underlying patterns are called noisy data.[18] Unaddressed anomalies, including fraudulent data, can lead to model training on such data, which renders the model incapable of effectively detecting fraud.

Moreover, using outlier detection methods, such as the Z-score method or isolation forest, will help to detect and reduce the effect of such anomalies, ensuring that models are trained on spotlessly clean and dependable data.[58] However, Lukui et al.,[59] examine how missing value imputation impacts fraud detection models and find that appropriate imputation methods can positively impact model performance. Furthermore, Kulatilleke and Samarakoon[60] performed an empirical study on ML classifier evaluation metrics in the setting of massively imbalanced and noisy data, concluding how to deal with noisy data in fraud detection problems.

Importance of Data Privacy and Ethical Considerations

Data privacy and ethical considerations are paramount in the growth and deployment of fraud detection systems, especially in the banking and financial sectors. Typically, fraud detection models rely on sensitive customer data, such as transaction history, personal information, and financial behavior.[61] Therefore, it is important to guarantee that the data used for training and evaluation complies with privacy regulations such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States.[62] To maintain data privacy, data anonymization, and encryption are commonly used. Anonymization includes removing personally identifiable information (PII) from the dataset, while encryption ensures that sensitive data is protected during transmission and storage.[63]

Furthermore, ethical considerations should be considered when designing fraud detection systems, particularly in avoiding biases that could lead to unfair treatment of certain customers. A key requirement is to ensure the models do not leak discrimination against specific demographics or cause unintended harm. Pombal et al.[64] research proves the significance of understanding and combating unfairness in fraud detection models. They caution that biased models can restrict whole groups from accessing financial services. They argue for developing fair machine learning (Fair ML) principles to examine, quantify, and reduce unfairness in algorithmic predictions. Additionally, a study suggested by Kamalaruban et al.,[65] of evaluating fairness within transaction fraud models highlights the need to develop fairness because of the likely harms and legal repercussions of unfair decision-making. The research characterizes unique challenges in fraud detection, including fairness metrics that account for the imbalance of fraud data and the tradeoff between

DOI: https://doi.org/10.70389/PJAI.100014 | Premier Journal of Artificial Intelligence 2025;3:100014

Table 3 | Overview of preprocessing challenges in fraud detection

Preprocessing Challenge	Solution	Advantages	Limitations	References
Imbalanced Datasets	Resampling (SMOTE, under-sampling), cost-sensitive learning	Balances class distribution, improves model performance on the minority class	This can lead to overfitting, especially with oversampling	52–55
Feature Engineering and Selection	Recursive feature elimination (RFE), Random forest feature importance	Improves model accuracy by focusing on relevant features	Requires domain knowledge and time-consuming	1,21,56,57
Missing Data	Imputation (mean, median, KNN)	Fills in missing values, prevents data loss	Imputation can introduce bias if not done carefully	33,59
Noisy Data	Outlier detection (Z-score, Isolation Forest)	Removes erroneous data points, improves model accuracy	May remove valid but rare transactions as outliers	18,58,60
Data Privacy and Ethics	Data anonymization, encryption	Protects sensitive customer information, ensures compliance with regulations	It can complicate data processing and model training	61–65

providing fraud protection and maintaining service quality.

Effective preprocessing is crucial for fraud detection but comes with trade-offs. Imbalanced datasets are addressed with resampling and cost-sensitive learning, improving minority class performance but risking overfitting. Feature engineering and selection enhance model accuracy but require domain expertise and time. Missing data is handled through imputation, though improper methods can introduce bias. Noisy data is mitigated with outlier detection, but rare yet valid transactions may be mistakenly removed. Data privacy and ethics are ensured via anonymization and encryption, though these methods can complicate model training. Balancing these solutions is key to optimizing fraud detection systems.

Challenges and Limitations

These methods of fraud detection in banking using ML and DL have abundant challenges and limitations, as shown in Table 4. These pose challenges of computational and resource demands, interpretability of the model, real-time fraud detection as a necessity, and vulnerability of fraud detection systems to adversarial attacks.[66] These challenges are further discussed in more detail in this section, and their implications for the effectiveness and deployment of fraud detection systems are also described.

Computational and Resource Challenges

ML and DL techniques for fraud detection pose a serious challenge of high computational and resource requirements. For instance, DL fraud detection models are computationally intensive and memory-intensive models. Processing such a huge volume of transactional data is time-consuming and resource-expensive for training DL models.[32] For instance, in the case of special DL architecture like RNNs or LSTM networks, we have to train them faster, which requires special hardware, such as Graphics Processing Units (GPUs).[44] This can be a barrier for organizations with limited access to high-performance computing resources.

Additionally, DL models are complex, which, in turn, increases the storage and memory requirement. If the models get bigger, the parameters and intermediate computation need to be stored in memory, eventually leading to inefficiencies and slowing down real-time processing environments.[67] Furthermore, cloud-based solutions can also help to reduce some of those resource problems, but there come other problems like data privacy concerns and latency in getting data from remote servers.

Interpretability of ML/DL Models

Understanding how a model operates is a big challenge for both ML and DL models, particularly regarding high-stakes fields such as banking fraud detection. ML models such as decision trees and random forests can usually be explained more due to a transparent decision-making process; however, DL models, especially neural networks, are often considered a 'black box.'[68] The lack of interpretability of the two systems bears a problem in fraud detection systems, where stakeholders (e.g., bank employees and regulators) need to understand why a model decides to flag a transaction as fraudulent.

Trust in the system requires the system to be interpretable, i.e., the decisions made by the fraud detection system cannot be arbitrary or biased. In certain cases, regulators may ask for explanations as to why a specific transaction was deemed fraudulent, e.g., when the complaint was raised to a specific transaction that turned out to be legitimate. LIME (Local Interpretable Model-agnostic Explanations) and SHAP (Shapley Additive Explanations) are being developed to enable us to understand which features led to a model's prediction in the case of complex models.[69] Nevertheless, these methods are still being refined, and their application to huge-scale fraud detection systems is still being researched.

Real-Time Fraud Detection Requirements

Banking fraud detection systems have to work in real time to prevent any financial losses. Meeting this requirement poses a significant challenge as fraud detection models must be able to process large volumes of transactions in real time without creating latency on approval or customer experience.[1] RNNs and LSTMs, which are both very useful DL models for sequential data, can be very slow to process and might not satisfy the strict latency requirements necessary for real-time fraud detection.[70]

Besides model latency, fraud detection systems need to take care of high throughput data streams from different sources like transaction logs, customer behavior, and external fraud indicators. Efficient data pipelines and parallel processing frameworks are necessary for ingesting large volumes of high-velocity data streams.[2] Some of these issues can be mitigated with edge computing and streaming analytics, which process data closer to the source and thus shorten the time to detect and respond to fraudulent activities.

Adversarial Attacks on Fraud Detection Systems

Fraud detection systems are increasingly under threat from adversarial attacks. So, they're attacks that

Table 4 | Overview of challenges in implementing ML and DL techniques in fraud detection

Challenge/ Limitations	Impact on Fraud Detection	Solutions/ Approaches	Limitations
Computational and Resource Challenges	High resource and computational demands for training models	Use of GPUs, cloud computing, and parallel processing	Expensive hardware requirements, latency in cloud solutions
Interpretability of ML/DL Models	Difficulty in understanding model decisions, especially for DL models	Use of LIME, SHAP, and model simplification techniques	Limited application for large-scale fraud detection systems
Real-time Fraud Detection	Latency in processing large volumes of transactions	Stream processing, edge computing, and real-time data pipelines	May not meet real-time requirements for large-scale systems
Adversarial Attacks	Vulnerability to subtle attacks that deceive the model	Adversarial training, defensive distillation, and robust models	It may require continuous monitoring and adaptation to new attack methods

manipulate the input data in such a way that causes an ML or DL model to predict incorrectly. Adversarial attacks in the context of fraud detection could be performed by changing transaction details or customer data to mislead the model to detect legitimate transactions as fraudulent or fraudulent transactions as legitimate, respectively.[71] Banking especially worries about adversarial attacks since they could be associated with significant financial loss when fraud is not detected.

Particularly, DL models are vulnerable to adversarial attacks because of their inherent complexity and high dimensional feature space. Unlike the more obvious money laundering attacks, these can be subtle and hard to catch by traditional fraud detection systems.[72] Researchers have been exploring techniques to defend against adversarial attacks, including adversarial training (training on adversarial examples to progress the robustness of the model) and defensive distillation (simplifying the model so that small changes in input data have less effect on the model).

Future Trends and Directions

The future of banks' anti-fraud systems is evolving rapidly as emerging technologies and methodologies shape the banking fraud detection landscape.[10] With the sophistication of the fraud techniques phishing to an increasing level, financial institutions have to adopt innovative approaches like Explainable AI (XAI), real-time and edge computing solutions, blockchain integration, utilization of Synthetic data, and collaboration between academic and industrial to build more effective and secure fraud detection system.[69] This section delves into these future trends and their potential impact on fraud prevention.

Explainable AI (XAI) for Fraud Detection

One of the most challenging aspects of deploying ML and DL models for fraud detection is the Lack of Transparency and Interpretability. With fraud detection systems growing more complex, explainable AI (XAI) is becoming more necessary. In high-stakes environments like banking, the idea behind XAI is to help humans recognize the decision-making process of the AI model and make it more transparent.[69]

Financial organizations can use explainable AI techniques to understand why a transaction was flagged as fraudulent, helping to take action appropriately and allow for an audit trail for regulatory compliance. For ML and DL models, one can use LIME (Local Interpretable Model-agnostic Explanations) and SHAP (Shapley additive explanations) to understand features that affected the model's decision.[4] These particular techniques are useful to improve trust and confidence in the AI system and provide the stakeholders with a clear explanation of the behavior of the model. With the further evolution of XAI, it will probably become key to beating the interpretability problems of sophisticated fraud detection models.

Real-Time and Edge Ccomputing Solutions

To prevent financial losses, banking institution requirements include the necessity for real-time fraud detection. The challenges of large volumes of transactions and the need for rapid decision-making make traditional fraud detection systems ineffective for real-time processing. Through real-time and edge computing solutions, this is being addressed.

Edge computing refers to processing data at the edge of a network, close to the source of the data (where it's generated), instead of sending it to a central server. This cuts latency and allows for faster fraud detection systems decisions.[66] For example, edge devices can process real-time transactional data and flag potentially fraudulent activities before they are done. Streaming analytics can also be leveraged by real-time fraud detection systems to detect fraud patterns with data streamed in real-time. Real-time processing with edge computing is set to drastically increase speed and efficacy in fraud detection systems, so banks can now react to fraud attempts in almost real-time.

Integration of Blockchain with ML/DL for Fraud Prevention

As known for its ability to offer secure, transparent, and immutable records, blockchain technology pairs with ML and DL models to improve fraud prevention. So, blockchain is perfect for ensuring the openness and security of financial processes because it is decentralized, which makes it tamper-proof. [73]

Using blockchain and ML/DL, financial institutions could bring a much safer and more efficient fraud detection system to the market. The blockchain could store this data, creating an organized transaction history and a secure ledger for transaction data. ML/dl methods could be run on this data to identify fraud. Blockchain can be used to trace the origin and flow of funds, and ML/DL models can be used to classify unusual patterns or actions that indicate potential fraud.[74] However, it is now possible to integrate these technologies to provide a more robust and trustworthy system for detecting and preventing fraudulent transactions, ensuring the integrity of financial transactions worldwide.

DOI: https://doi.org/10.70389/PJAI.100014 | Premier Journal of Artificial Intelligence 2025;3:100014

Use of Synthetic Data and Generative Models for Training

It is hard to collect labeled data for fraud detection. The number of fraudulent transactions is very small, which is related to the number of legitimate transactions, resulting in imbalanced datasets that can hurt the presentation of the fraud detection model. However, the use of synthetic data and generative models is becoming a promising approach to solving this problem.[75]

Generative models such as GANs can generate realistic synthetic data that follow the distribution of real fraudulent transaction data. These synthetic data can supplement the training datasets to help compensate for the data and improve the fraud detection model training performance.[70] Training models on a more diverse data set, including legitimate and fraudulent transactions, allows models to learn better to detect fraud. Furthermore, synthetic data can replicate rare fraud situations absent in the historical data, which allows fraud detection systems to address new and emerging fraud methods.[32]

Collaboration Between Academia and Industry for Better Models

The field of fraud detection is evolving, and research collaboration between academia and industry is more important than ever. Industry practitioners contribute their practical insights into the challenges of financial institutions in the real-world environment, and academic researchers add their theoretical knowledge and bring innovative ideas.[76] Similar to any other problem, academia, and industry can work together and build more robust fraud detection models that use the latest technologies, including ML and DL.

Collaborative efforts can also fill the gap between research and application to see if the bleeding edge techniques work and one hopes in practice. For example, academia will develop novel algorithms and frameworks for fraud detection, and industry will provide access to large-scale datasets and operational expertise.[61] These are synergies that potentially allow us to build more resilient, more scalable fraud detection systems that can deal with the kind of complexity that modern financial fraud has become.

Conclusion

This review highlighted the growing complexity of fraud detection in banking and the evolving role of ML and DL in addressing these challenges. Traditional ML techniques such as logistic regression, decision trees, random forests, and support vector machines have been widely used for fraud classification, offering scalability and interpretability. However, their ability to handle high-dimensional and complex fraud patterns remains limited. Conversely, DL techniques, including FNNs, CNNs, and RNNs, demonstrate superior performance in capturing intricate patterns and temporal dependencies. Despite their effectiveness, these models introduce challenges related to complexity, interpretability, and large-scale deployment.

This study underscores the importance of data preprocessing, including handling imbalanced datasets, feature engineering, and addressing missing or noisy data, as these steps significantly impact model performance. Furthermore, emerging trends such as explainable AI, real-time and edge computing, blockchain integration, and synthetic data generation are poised to shape the future of fraud detection. The next generation of fraud detection systems will likely leverage these advancements to enhance speed, accuracy, and security. Overall, this review emphasizes the need for continuous research, industry collaboration, and the adoption of advanced AI-driven approaches to strengthen fraud prevention mechanisms in banking.

While fraud detection has come a long way, many challenges still do not seem to go away. Continued research and development are required to address the computationally and resource-intensive nature of DL models, the necessity for real-time decision-making, and the vulnerability of fraud detection systems to adversarial attacks. Furthermore, fraud detection systems of the future must be interpretable, given the complexity of many modern models, and tackle issues of an ethical nature, such as data privacy.

Integrating ML and DL techniques into fraud detection systems is a huge step forward in helping to fight financial fraud. However, more work is needed on model transparency, real-time processing, and collaboration between research and industry to fully take advantage of these technologies. With the solution of these challenges, the effectiveness of financial institutions' fraud detection systems can be improved, thereby ensuring the safety and security of these institutions' operations and fostering the trust of their customers.

References

1 Mytnyk B, Tkachyk O, Shakhovska N, Fedushko S, Syerov Y. Application of artificial intelligence for fraudulent banking operations recognition. Big Data Cogn Comput. 2023;7(2). http://doi.org/10.3390/bdcc7020093

2 Kotagiri A, Yada A. Improving fraud detection in banking systems: RPA and advanced analytics strategies. Int J Mach Learn Sustain Dev. 2024;6(1):1–20.

3 Sharma B, Singh S. An investigation of challenges faced in detecting frauds. Int J Mech Prod Eng Res Dev. 2020;10(3):11813–22. http://doi.org/10.24247/ijmperdjun20201129

4 Bhasin ML. The fight against bank frauds: Current scenario and future challenges. Cienc e Tec Vitivinic 2016;31(2):56.

5 Alarfaj FK, Malik I, Khan HU, Almusallam N, Ramzan M, Ahmed M. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access. 2022;10:39700–15. http://doi.org/10.1109/ACCESS.2022.3166891

6 Lou C. Graph Neural Network for Fraud Detection via Context Encoding and Adaptive Aggregation (Vol. 261). Elsevier. 2025.

7 Mahmud F. Transforming banking security: The role of deep learning in fraud detection systems. Am J Eng Technol. 2024;6:20–32.

8 Violetta K, Volodymyr K, Roman G. Financial fraud in the banking sphere: Essence, types and current state. Polit Sci Secur Stud J. 2022;3(2):11–9. ISSN 2719-6410. http://doi.org/10.5281/zenodo.6801599

9 Sanusi ZM, Rameli MNF, Isa YM. Fraud schemes in the banking institutions: Prevention measures to avoid severe financial loss. Procedia Econ. Financ. 2015;28:107–13. http://doi.org/10.1016/s2212-5671(15)01088-6

10 Abu-Shanab E, Matalqa S. Security and fraud issues of E-banking. Int J Comput Netw Appl. 2015;2(4):179–87.

11 Btoush E, Zhou X, Gururajan R, Chan KC. Achieving excellence in cyber fraud detection: A hybrid ML + DL ensemble approach for credit cards. Appl Sci. 2025;15(3):1081.
12 Minastireanu EA, Mesnita G. An analysis of the most used machine learning algorithms for online fraud detection. Inform Econ. 2019;23(1):5–16. http://doi.org/10.12948/issn14531305/23.1.2019.01
13 Sahin Y, Duman E. Detecting credit card fraud by ANN and logistic regression. In 2011 International Symposium on Innovations in Intelligent Systems and Applications 2011;(pp. 315–9). IEEE. http://doi.org/10.1109/INISTA.2011.5946108
14 Mishra KN, Pandey SC. Fraud prediction in smart societies using logistic regression and k-fold machine learning techniques. Wirel Pers Commun. 2021;119(2):1341–67. http://doi.org/10.1007/s11277-021-08283-9
15 Hmidy Y, Ben Mabrouk M. Reliable logistic regression for credit card fraud detection. Int J Adv Comput Sci Appl. 2024;15(11).
16 Mohammed NH, Maram SCR. Fraud detection of credit card using logistic regression. SSRN Electron J. 2022. http://doi.org/10.2139/ssrn.4135514
17 Prins TJ. UCLA UCLA Electronic Theses and Dissertations Title. 2019.
18 Save P, Tiwarekar P, Jain KN, Mahyavanshi N. A novel idea for credit card fraud detection using decision tree. Int J Comput Appl. 2017;161(13):6–9. http://doi.org/10.5120/ijca2017913413
19 Sahin Y, Duman E. Detecting credit card fraud by decision trees and support vector machines. In IMECS 2011—International Multiconference of Engineers and Computer Scientists 2011;(Vol. 1, pp. 442–7IM).
20 Martins L, Bravo J, Gomes AS, Soares C, Bizarro P. RIFF: Inducing rules for fraud detection from decision trees. Lect Notes Comput Sci (including Subser. Lect Notes Artif Intell Lect Notes Bioinformatics). 2024;15183:50–8. http://doi.org/10.1007/978-3-031-72407-7_5
21 Boyko N, Mokryk Y. Detecting fraud in banking transactions with random forest models. In 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T) 2021;(pp. 535–40). http://doi.org/10.1109/PICST54195.2021.9772209
22 Xuan S, Liu G, Li Z, Zheng L, Wang S, Jiang C. Random forest for credit card fraud detection. In 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC) 2018;(pp. 1–6). http://doi.org/10.1109/ICNSC.2018.8361343
23 Liu C, Chan Y, Alam Kazmi SH, Fu H. Financial fraud detection model: Based on random forest. Int J Econ Financ. 2015;7(7):178–88. http://doi.org/10.5539/ijef.v7n7p178
24 Gyamfi NK, Abdulai JD. Bank fraud detection using support vector machine. In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference IEMCON 2018 2018;(pp. 37–41). IEEE. http://doi.org/10.1109/IEMCON.2018.8614994
25 Bhattacharyya S, Jha S, Tharakunnel K, Westland JC. Data mining for credit card fraud: A comparative study. Decis Supp Syst. 2011;50(3):602–13. http://doi.org/10.1016/j.dss.2010.08.008
26 Khodabakhshi M. Archive of SID fraud detection in banking using KNN (K-nearest neighbor). Algorithm Archive of SID. Int Conf Res Sci Technol. 2016:26–34.
27 Saeed VA, Abdulazeez AM Credit card fraud detection using KNN, random forest and logistic regression algorithms: A comparative analysis. Indonesian J Comput Sci. 2024;13(1):218–27. http://doi.org/10.33022/ijcs.v13i1.3707
28 Rzayeva D, Malekzadeh S. A Combination of Deep Neural Networks and K-Nearest Neighbors for Credit Card Fraud Detection. arXiv Prepr. arXiv2205.15300. 2022. p. 1–6.
29 Taha A, Malebary SJ. An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE Access. 2020;8:25579–87. http://doi.org/10.1109/ACCESS.2020.2971354
30 Ding L, Liu L, Wang Y, Shi P, Yu J. An AutoEncoder enhanced light gradient boosting machine method for credit card fraud detection. Peer J Comput Sci. 2024;10:e2323. http://doi.org/10.7717/peerj-cs.2323
31 Xu B, Wang Y, Liao X, Wang K. Efficient fraud detection using deep boosting decision trees. Decis Support Syst. 2023;175(28). http://doi.org/10.1016/j.dss.2023.114037
32 Hashemi SK, Mirtaheri SL, Greco S. Fraud detection in banking data by machine learning techniques. IEEE Access. 2022;11:3034–43. http://doi.org/10.1109/ACCESS.2022.3232287
33 Moreira MÂL, de Souza Rocha C Jr, de Lima Silva DF, de Castro MAP Jr, de Araújo Costa IP, Gomes CFS, et al. Exploratory analysis and implementation of machine learning techniques for predictive assessment of fraud in banking systems. Procedia Comput Sci. 2022;214(C):117–24. http://doi.org/10.1016/j.procs.2022.11.156
34 Sambrow VD, Iqbal K. Integrating artificial intelligence in banking fraud prevention: A focus on deep learning and data analytics. Eigenpub Rev Sci Technol. 2022;6(1):17–33.
35 Yan N, Au OTS. Online learning behavior analysis based on machine learning. Asian Assoc Open Univ J. 2019;14(2):97–106. http://doi.org/10.1108/AAOUJ-08-2019-0029
36 Ghazi N, Jameel M, George LE. Detection of phishing emails using feed forward neural network. Int J Comput Appl. 2013;77(7):10–15. http://doi.org/10.5120/13405-1057
37 Quah JTS, Sriganesh M. Real-time credit card fraud detection using computational intelligence. Expert Syst Appl. 2008;35(4):1721–32. http://doi.org/10.1016/j.eswa.2007.08.093
38 Mendoza-Bernal J, González-Vidal A, Skarmeta AF. A convolutional neural network approach for image-based anomaly detection in smart agriculture. Expert Syst Appl. 2024;247:123210. http://doi.org/10.1016/j.eswa.2024.123210
39 Fu K, Cheng D, Tu Y, Zhang L. Credit card fraud detection using convolutional neural networks. In Neural Information Processing: 23rd International Conference, ICONIP 2016, Kyoto, Japan, October 16–21, 2016, Proceedings, Part III 23 2016;(pp. 483–90). http://doi.org/10.1007/978-3-319-46675-0
40 Zhang Z, Zhou X, Zhang X, Wang L, Wang P. A model based on convolutional neural network for online transaction fraud detection. Secur Commun Netw. 2018;2018. http://doi.org/10.1155/2018/5680264
41 김김김, Kim E. Supervised Deep Learning-based Anomaly Detection Models and Their Applications in Finance, Manufacturing, and Media. 서울대학교 대학원. 2019.
42 Douzi BS, El Ouahidi B. Credit card fraud detection model based on LSTM recurrent neural networks. J Adv Inf Technol. 2021;12(2):113–8. http://doi.org/10.12720/jait.12.2.113-118
43 Jurgovsky J, Granitzer M, Ziegler K, Calabretto S, Portier P-E, He-Guelton L, et al. Sequence classification for credit-card fraud detection. Expert Syst Appl. 2018;100:234–45. http://doi.org/10.1016/j.eswa.2018.01.037
44 Shrestha, Mahmood A. Review of deep learning algorithms and architectures. IEEE Access. 2019;7:53040–65. http://doi.org/10.1109/ACCESS.2019.2912200
45 Wei R, Garcia C, El-sayed A, Peterson V, Mahmood A. Variations in variational autoencoders—A comparative evaluation. IEEE Access. 2020;8:153651–70. http://doi.org/10.1109/ACCESS.2020.3018151
46 Yousefi N, Alaghband M, Garibay I. A comprehensive survey on machine learning techniques and user authentication approaches for credit card fraud detection. Comput Sci Mach Learn. 2019;9(1):18–25.
47 Çakır MY. Enhanced Autoencoder-Based Fraud Detection: A Novel Approach with Noise Factor Encoding and SMOTE (Vol. 66). Springer. 2023. p. 635–52.
48 Dou Y, Liu Z, Sun L, Deng Y, Peng H, Yu PS. Enhancing graph neural network-based fraud detectors against camouflaged fraudsters. Int Conf Inf Knowl Manag Proc. 2020:315–24. http://doi.org/10.1145/3340531.3411903
49 Kipf TN, Welling M. Semi-supervised classification with graph convolutional networks. ICLR. 2017:1–11.
50 Salekshahrezaee Z, Leevy JL, Khoshgoftaar TM. The effect of feature extraction and data sampling on credit card fraud detection. J Big Data. 2023;10(1). http://doi.org/10.1186/s40537-023-00684-w
51 Rubaidi ZS, Ben Ammar B, Ben Aouicha M. Fraud detection using large-scale imbalance dataset. Int J Artif Intell Tools. 2022;31(8). http://doi.org/10.1142/S0218213022500373
52 Meng C, Zhou L, Liu B. A case study in credit fraud detection with SMOTE and XGboost. J Phys Conf Ser. 2020;1601(5). http://doi.org/10.1088/1742-6596/1601/5/052016
53 Ileberi E, Sun Y, Wang Z. Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. IEEE Access. 2021;9:165286–94. http://doi.org/10.1109/ACCESS.2021.3134330
54 Peranginangin R, Harianja EJG, Jaya IK, Rumahorbo B. Synthetic minority over-sampling technique. Methomika J Manaj Inform dan Komputerisasi Akunt. 2020;4(1):67–72. http://doi.org/10.46880/jmika.vol4no1.pp67-72

55 Baloch BK, Kumar S, Haresh S, Rehman A, Syed T. Focused anchors loss: Cost-sensitive learning of discriminative features for imbalanced classification. Proc Mach Learn Res. 2019;101(2009):822–35.

56 Correa Bahnsen D, Stojanovic AA, Ottersten B. Feature engineering strategies for credit card fraud detection. Expert Syst Appl. 2016;51:134–42. http://doi.org/10.1016/j.eswa.2015.12.030

57 Lucas Y, Portier P-E, Laporte L, He-Guelton L, Caelen O, Granitzer M, et al. Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. Futur Gener Comput Syst. 2020;102:393–402. http://doi.org/10.1016/j.future.2019.08.029

58 Oberreuter G, L'Huillier G, Ríos SA, Velásquez JD. Approaches for intrinsic and external plagiarism detection notebook for PAN at CLEF 2011. In CEUR Workshop Proc. 2011;(Vol. 1177, pp. 1–10).

59 Huang L, Abrahams A, Ractham P. Enhanced financial fraud detection using cost-sensitive cascade forest with missing value imputation. Intell Syst Account Financ Manag. 2022;29(3):133–55. http://doi.org/10.1002/isaf.1517

60 Kulatilleke GK, Samarakoon S. Empirical Study of Machine Learning Classifier Evaluation Metrics Behavior in Massively Imbalanced and Noisy Data. arXiv:2208.11904. 2022.

61 Shoetan PO, Oyewole AT, Okoye CC, Ofodile OC. Reviewing the role of big data analytics in financial fraud detection. Financ Account Res J. 2024;6(3):384–94. http://doi.org/10.51594/farj.v6i3.899

62 Alexander CB. The general data protection regulation and California consumer privacy act: The economic impact and future of data privacy regulations. Loyola Consum Law Rev. 2020;32(2):199–245.

63 Del Rosal V. Personal identifiable information (PII) detection and identification for Fintech with AI and text analytics. Int J Adv Comput Sci Appl. 2021;12(9):1–9.

64 Pombal J, Cruz AF, Bravo J, Saleiro P, Figueiredo MAT, Bizarro P. Understanding Unfairness in Fraud Detection through Model and Data Bias Interactions; 2022.

65 Kamalaruban P, Pi Y, Burrell S, Drage E, Skalski P, Wong J, et al. Evaluating fairness in transaction fraud models: Fairness metrics, bias audits, and challenges. In ICAIF 2024—Proceedings of the 5th ACM International Conference on AI in Finance 2024 2024;(pp. 555–63). http://doi.org/10.1145/3677052.3698666

66 Alzubaidi L, Zhang J, Humaidi AJ, Al-Dujaili A, Duan Y, Al-Shamma O, et al. Review of Deep Learning: Concepts, CNN Architectures, Challenges, Applications, Future Directions (Vol. 8, no. 1). Springer International Publishing. 2021. http://doi.org/10.1186/s40537-021-00444-8

67 Bommasani R, Wu J, Child R, Luan D, Amodei D, Sutskever I, et al. Language Models are Unsupervised Multitask Learners; 2021.

68 Wang W, Kiik M, Peek N, Curcin V, Marshall IJ, Rudd AG, et al. A systematic review of machine learning models for predicting outcomes of stroke with structured data. PLoS One. 2020;15(6):1–16, http://doi.org/10.1371/journal.pone.0234722

69 Ji Y. Explainable AI Methods for Credit Card Fraud Detection: Evaluation of LIME and SHAP Through a User Study. DiVA. 2021. p. 49.

70 Shiri FM, Perumal T, Mustapha N, Mohamed R. A Comprehensive Overview and Comparative Analysis on Deep Learning Models: CNN, RNN, LSTM, GRU. arXiv:2305.17473. 2023.

71 Fursov I, Morozov M, Kaploukhaya N, Kovtun E, Rivera-Castro R, Gusev G, et al. Adversarial attacks on deep models for financial transaction records. In Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining 2021;(pp. 2868–78). http://doi.org/10.1145/3447548.3467145

72 Carminati M, Santini L, Polino M, Zanero S. Evasion attacks against banking fraud detection systems. In 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID) 2020;(pp. 285–300).

73 Obeng S, Iyelolu TV, Akinsulire AA, Idemudia C. Utilizing machine learning algorithms to prevent financial fraud and ensure transaction security. World J Adv Res Rev. 2024;23(1):1972–80

74 Dhanawat V. Anomaly detection in financial transactions using machine learning and blockchain technology. Int J Bus Manag Vis. 2022;5(1):34–41. ISSN 3006-2705.

75 Werhahn M, Xie Y, Chu M, Thuerey N. A multi-pass GaN for fluid flow super-resolution. Proc ACM Comput Graph Interact Tech. 2019;2(2). http://doi.org/10.1145/3340251

76 Chang Y, Wang X, Wang J, Wu Y, Yang L, Zhu K, Chen H, et al. A survey on evaluation of large language models. ACM Trans Intell Syst Technol. 2024;15(3). http://doi.org/10.1145/3641289