Cureus Journal of Computer Science

Open Access Review Article

# The Role of Deep Learning in Credit Card Fraud Detection: A State-of-the-Art Review

Pranita N. Sangit [1] , Savita Sangam [1]

1. Information Technology, Shah and Anchor Kutchhi Engineering College, Mumbai, IND

**Corresponding authors:** Pranita N. Sangit, pranita.18606@sakec.ac.in, Savita Sangam, savita.sangam@gmail.com

**Received** 03/29/2025
**Review began** 04/20/2025
**Review ended** 09/04/2025
**Published** 09/10/2025



**DOI:**
https://doi.org/10.7759/s44389-025-04298-6

## Abstract

Credit card fraud detection is a critical challenge in the financial sector, as fraudulent activities continue to evolve in complexity with the rapid growth of digital transactions. Traditional fraud detection methods, including rule-based systems, and classical machine learning approaches like decision tree, support vector machines, and random forest have shown limited effectiveness in handling the dynamic and sophisticated nature of modern fraud schemes. These methods often struggle with high false-positive rates, data imbalance, and adaptability to new fraud patterns. In contrast, deep learning techniques have demonstrated remarkable potential in enhancing fraud detection by learning intricate transaction patterns, reducing manual feature engineering, and improving classification accuracy. These techniques have emerged as a powerful tool to enhance fraud detection by capturing complex transaction patterns and improving detection accuracy. This review provides analysis of state-of-the-art deep learning techniques applied to credit card fraud detection, exploring their architectures, methodologies, and performance in real-world scenarios. This study examines various deep learning models, including artificial neural networks, convolutional neural networks, recurrent neural networks, long short-term memory networks, generative adversarial networks, autoencoders, and hybrid deep learning architectures in previous research studies. These models leverage powerful feature extraction and representation learning capabilities, allowing them to detect fraudulent transactions more effectively than traditional approaches. One of the primary challenges in fraud detection is the highly imbalanced nature of transaction datasets, where fraudulent transactions constitute only a small fraction of the total data. This paper explores synthetic data generation using generative adversarial networks. Finally, this study highlights key challenges and future research directions in deep learning-based credit card fraud detection.

**Categories:** AI applications, Application Security, Artificial Intelligence and Machine Learning in the Cloud
**Keywords:** credit card frauds, deep learning, machine learning, ann, cnn, rnn

## Introduction And Background

Today, both online and offline, credit cards are among the most widely used payment options. Credit card usage is to pay for something in a store. The consumer pays with a physical card that they carry with them at all times. An unauthorized entity has to obtain the card to engage in fraud during this transaction. Financial losses will occur if the user is not aware that their card has been lost. Each credit card user is given a special code that includes details about the purchase, the amount spent, and the date of the most recent transaction. Fraud is thought to be anything that does not follow this pattern. Fraud is the use of deceit to gain financial security. Since more people are using credit cards to make purchases online due to consumers' increased internet usage, the use of a credit card is more likely to result in effective and targeted fraud.

Credit card information and other personal data are frequently misappropriated to conduct unauthorized transactions and withdraw cash [1]. The most common scam technique is this one. Online shopping and other online activities, such as online banking and credit cards, are becoming increasingly popular. Only when the fraud has already taken place does the cardholder realize it. Credit card larceny poses a threat to users, cardholders, and corporate assets alike. The quantity of money lost due to fraud increased in recent years, according to cardholders, retailers, and ATM card acquirers transactions at ATMs. Various types of fraud can occur during card swipes at retail outlets, such as skimming, claiming overpayment, cloning during ATM withdrawals, and hacking card or account information during online transfers.

The number of transactions that do not require a physical credit card has increased as e-commerce has become more prevalent. Because there is no physical proof, such as a PIN or a signature, these activities are the most likely to be faked. Unauthorized individuals have a higher propensity for adapting to change and are not afraid to change their behavior to lessen the chance of being detected. Adaptability is also required of anti-fraud systems. A two-step process is used to find people who commit credit card fraud: first, suspect management practices are identified, and then an inquiry is made to see if fraud has actually taken place. It is possible for a computer program to handle the first part, but the rest needs to be done manually.

The number of credit cards like VISA and MasterCard issued is increasing globally [2]. The rapid expansion of digital transactions has led to a rise in fraudulent activities, causing significant financial losses. Traditional fraud detection methods rely on manually designed rules and classical machine learning techniques, which often fail to adapt to new fraud patterns. Deep learning, with its ability to learn hierarchical representations, has gained attention for its potential to improve fraud detection accuracy.

## Search strategy

In this study, for a comprehensive review, we referred to popular and credible scientific databases such as IEEE Xplore, Scopus, Springer Link, ScienceDirect, ACM Digital Library, and Google Scholar, as well as selected websites and newsletters. The majority of the studies considered were published between 2020 and 2024. The PRISMA process used to select research papers for addressing the research questions is outlined below.

Step 1: Records identified through database searching.

Step 2: Records screened, excluded based on the criteria that if not in English language and repeated work, and included if studies are using deep learning techniques to identify credit card frauds and have mentioned about credit card dataset used.

Step 3: Full articles assessed for eligibility (n = 50).

Step 4: Articles assessed for considerations for review purpose (n = 20).

## Inclusion and exclusion criteria for research study

This study includes articles presenting experimental results, frameworks, or comparative analyses of machine learning and deep learning methods. It considers peer-reviewed conference papers, journal articles, and reputable proceedings. This study includes research paper references that consider evaluation metrics like accuracy. Each technique is reviewed using multiple references and mentioned accordingly.

This study excludes articles that provide insufficient technical details. Duplicate publications or extended versions without new contributions have also been excluded. Non-English papers, editorials, theses, blogs, or grey literature are not referred to while performing the research study.

# Review

Credit card fraud detection is a critical task that requires real-time identification and classification of suspected fraud instances before the approval or rejection of the transaction. For the identification and categorization of data related to credit card fraud, many researchers have proposed various methodologies. This study reviews several classification and fraud detection algorithms for credit card fraud detection.

Various machine learning algorithms have been implemented for the identification of fraudulent transactions, such as logistic regression, decision tree, support vector machine (SVM) [3], and random forest [4,5]. In developing systems for credit card fraud detection, a major challenge faced is handling data imbalance. Data imbalance refers to a significant difference in the number of samples in different classes. The credit card dataset available on Kaggle, used by most research studies, is highly imbalanced, meaning the number of fraudulent samples is comparatively far less than legitimate transactions. Rtayli [6] presents a detailed study of the classification of unbalanced datasets. Mostly, unbalanced datasets are common in medical diagnosis, fraud detection applications, and spam filtering. In a study by Akinwamide et al. [7], different sampling techniques like undersampling and oversampling [8], synthetic minority over-sampling technique (SMOTE) [9], SMOTETomek [10,11], hybrid undersampling and oversampling [12], and other similar techniques have been reviewed along with machine learning classifiers. Various bagging and boosting algorithms like XGBoost [13,14], AdaBoost [15], catBoost [16], and boosting mechanisms with spiral oversampling techniques [17] have been used. Das [18] built a support vector data description machine learning model to improve performance. Brezočnik et al. [19] used an adversary-based oversampling technique to deal with data imbalance. A study by Ileberi et al. [20] provides a comparison of various machine learning techniques. In credit card fraud detection systems, feature selection and dimensionality reduction are major steps. Various techniques like principal component analysis [21], swarm intelligence [22], and genetic algorithm have been used for this. Some of the studies that have been presented are explained in the following section.

Patil et al. [23] provide a comprehensive analysis of various machine learning algorithms for identifying fraudulent credit card transactions. It compares different machine learning techniques for detecting credit card fraud, aiming to identify which models provide the best performance, especially considering the challenge of class imbalance. The study uses a real-world, highly imbalanced dataset where fraudulent transactions are significantly fewer than legitimate ones. Machine learning techniques evaluated include Logistic Regression, Naive Bayes, Decision Tree, Random Forest, SVM, K-Nearest Neighbors, and neural networks. Results have shown that random forest and neural networks delivered the best performance overall, particularly in detecting frauds while minimizing false positives. SVM and K-Nearest Neighbors struggled with computation time and scalability on large datasets. Logistic Regression and Naive Bayes were faster but less accurate on imbalanced data.

Pradhan et al. [24] propose a risk control algorithm for integrated learning, combining SMOTE and principal component analysis for data processing, a single-layer decision tree, and an improved Adaboost algorithm. A trained risk control system is applied to individual data for fraud identification. After testing a commercial bank data sample, the simulation results showed an accuracy rate of 96.50% and an F-Measure value of 97.3%. The principal component analysis determines initial weights by analyzing the dataset and the principal components based on the dataset. The coefficient corresponding to each index is used as the initial weight of the iterated classifier.

Mizher and Nassif [25] integrate machine learning algorithms (XGBoost, KMeans, random forest, and decision tree classifier) with blockchain technology to classify transactions as legitimate or fraudulent. Transactions are analyzed using a Bitcoin transaction dataset, with the assumption that patterns are transferable to Ethereum due to similarities in cryptocurrency transaction behaviors. This innovative approach leverages the strengths of blockchain's decentralization and machine learning's pattern recognition to address fraud in digital finance. The authors suggest enhancing the model with deep learning for greater precision, improving resilience against Sybil attacks, and scaling it for larger datasets.

Femila Roseline et al. [26] contribute to the field by demonstrating the efficacy of artificial neural networks (ANNs) over traditional and other machine learning methods like random forest for credit card fraud detection. ANNs, inspired by biological neurons, and random forest, an ensemble method using multiple decision trees, are highlighted in this study. The system processes transaction data through a verification module to classify it as fraud or non-fraud. ANNs are trained using supervised learning (with known answers) or unsupervised learning (for pattern discovery). Random forest uses bagging and feature randomness to enhance prediction accuracy. Performance is evaluated using metrics such as accuracy, precision, and recall. Among the tested algorithms, ANNs outperformed others, achieving the highest accuracy in classifying transactions. Random forest, while effective, was less accurate and more computationally complex, particularly for real-time applications.

Almarshad et al. [27] demonstrate that the HOBA framework, paired with deep learning, considers the heterogeneity of transaction types (e.g., cash withdrawals vs. purchases) and includes location as a behavioral measure. It analyzes homogeneous groups of transactions based on specific characteristics (e.g., transaction type, time, location) using two strategies: transaction aggregation (quantifying recency, frequency, monetary value, and location) and rule-based (categorical variables based on domain knowledge). Three deep learning architectures are employed: Deep Belief Networks, convolutional neural networks (CNN), and recurrent neural networks (RNN). These models leverage hierarchical feature learning to process the extensive feature set generated by HOBA without manual feature selection, improving adaptability and performance. The future scope of this study requires exploring computational efficiency for real-time systems and investigating hybrid machine learning approaches.

San Miguel Carrasco et al. [28] successfully demonstrate that the long short-term memory (LSTM)-RNN model, supported by preprocessing and resampling, provides a highly effective solution for credit card fraud detection. It surpasses traditional methods (Naive Bayes, SVM, ANN) in accuracy and robustness, offering a promising approach for handling big data and evolving fraud patterns in the financial sector. The study introduces an LSTM-RNN-based fraud detection system tailored for sequential credit card transaction data, addressing limitations of traditional RNNs. The LSTM-RNN achieves perfect scores, significantly outperforming Naive Bayes (e.g., 71.6% precision, 69.53% accuracy), SVM (68.8% precision, 86.56% accuracy), and ANN (92.6% precision, 91.84% accuracy). However, the paper does not discuss computational costs or real-time implementation challenges. The perfect 100% performance metrics raise questions about overfitting or dataset-specific biases that are not addressed.

Tingfei et al. [29] propose a novel unsupervised learning approach to detect anomalies (specifically fraud) in highly imbalanced datasets without using class labels during training. The core idea is to iteratively clean the training dataset to enhance detection accuracy. The method uses an autoencoder as the base learner. Training occurs in iterations. In each iteration, the model is trained on the current dataset. Instances with high reconstruction error (beyond 2 standard deviations from the mean, $\lambda_2$SD) are removed. A new model is then trained on this cleaned dataset. The assumption is that instances with high reconstruction errors are likely to be anomalies. The autoencoder architecture uses an encoder with two layers (100, then 50 neurons, ReLU), a decoder with two layers (50, then 100 neurons, Tanh), and an output with ReLU activation. The model is evaluated using area under the curve and true positive rate. The proposed method significantly outperforms both the baseline autoencoder and isolation forest. The current approach uses the two standard deviation ($\lambda_2$SD) rule. Future work could explore adaptive thresholds based on percentiles or clustering methods, and use learnable thresholds tuned via reinforcement or meta-learning. The study uses only one type of model, the autoencoder, for anomaly detection. The results may not generalize well to other unsupervised learners without testing.

Zhang et al. [30] introduce credit card fraud detection model based on generative adversarial networks (GANs), a novel unsupervised fraud detection model using GANs, designed to detect credit card fraud without requiring fraudulent samples for training. It is composed of an encoder that maps transactions to latent space.

Generator that reconstructs normal transaction data and discriminator that distinguishes between real and fake (generated or penalized) data. It addresses challenges like scarcity of labeled fraud data; complex, unpredictable fraud patterns; spatio-temporal dependencies in transaction data; and GANs generating unrealistic or misleading data.

Though this model is suitable for offline detection, the model does not support real-time fraud detection or online learning, which is critical in production fraud systems. While it uses Extreme Value Theory for thresholding, thresholds still need careful tuning, and performance may vary based on the distributional assumptions Extreme Value Theory makes.

## Deep learning techniques

*Artificial Neural Networks*

The simplest form is ANNs, which are made up of input layer, hidden layers of interconnected nodes (neurons) that take in input data and produces output. Input nodes in first layer represents exploratory variables . These node values along with specific weights are passed on to hidden layers. In hidden layers these values are summed up with some bias value . Output is produced by applying activation function to the value obtained in hidden layers.

In a study by Asha and Suresh Kumar [31], 15 hidden layers along with RELU activation function is used in Credit card fraud detection model .Advantage of using these networks for fraud detection is that they have flexibility in learning non- linear patterns and have capability of handling large datasets and complex features. Since they can be prone to overfitting if not properly tuned, especially with imbalanced datasets and requires significant computational resources.

*Convolutional Neural Networks*

CNNs are primarily used in image recognition tasks but have been adapted for fraud detection by treating transaction data as a spatial or temporal grid. These networks have six distinct layers: input layer, convolutional layer, pooling layer, fully connected layer, softmax layer, and output layer. The input layer loads the CSV data. The convolutional layer performs the task of feature extraction. The spatial capacity of the input text after convolution is decreased. Max pooling must be used to reduce the spatial volume of the input text. The fully connected layer is used to classify data between dissimilar categories by training. These categories can be dropout and flattening. The softmax or logistic layer performs binary classification and forms the final layer of the network. The output layer holds the label, which is in the procedure of one-hot encoding.

Alarfaj et al. [32] found that a CNN with 20 layers, and the baseline model, was highly effective in detecting credit card fraud. To increase performance, numerous sampling techniques are used. The performance is observed to decrease significantly on unseen data. These networks can automatically learn spatial hierarchies of features, which makes them powerful for detecting fraud in time-series or sequential transaction data. They can extract features automatically, reducing the need for manual feature engineering. They have high accuracy for detecting complex patterns in transaction data. However, they require large datasets with labeled data to train their models.

*Recurrent Neural Networks*

RNNs are designed to handle sequential data, making them ideal for time-series analysis. In fraud detection, RNNs can learn patterns from transaction sequences and detect anomalous behavior over time. These networks can be effective for detecting fraud in sequential transaction patterns (e.g., detecting unusual spending behavior). They can capture temporal dependencies in data. They suffer from vanishing gradient issues, though techniques like LSTM networks mitigate this problem. They require extensive training data for effective learning.

Hsu et al. [33], in order to take advantage of the time dependencies present in these dynamic features, suggest learning an RNN feature extractor with gated recurrent unit on credit card payment data. This feature extractor first preprocesses the input sequences. An upgraded RNN model (RNN-RF) is then trained using the retrieved dynamic features and static characteristics to forecast credit card client defaults. Comparing the enhanced RNN predictor to the other benchmark models, numerical experiments verified that it performs best in terms of lift index (0.659) and area under the curve (0.782). With the help of the suggested model, we can efficiently integrate static and dynamic variables to deliver better financial data prediction performance.

*LSTM Networks*

LSTMs are a special type of RNN designed to learn long-range dependencies in sequential data. LSTMs are highly effective in fraud detection tasks that involve identifying fraudulent sequences of transactions over time. They are capable of handling long-term dependencies in time-series data. These networks are less prone to vanishing gradient issues, making them more reliable in complex sequence modeling. However, these networks are computationally expensive and can struggle with very large and complex datasets without proper tuning.

The research study presented BY Forough and Momtazi [34] states that LSTM is the best technique for fraud detection tasks. One of the major issues with RNNs is vanishing or exploding gradients. LSTM networks solve this issue with their architecture. LSTMs are memory-based, more efficient networks in which memory retains its state. To control the data flow to and from the memory cell, filtering devices are used. In addition, it consists of an input gate, output gate, and forget gate.

*Autoencoders*

Both encoders and decoders are employed in the training process of autoencoders. However, only encoders are used when applied to new data for dimension reduction. AE uses backpropagation for training and operates in layers of neurons, much like any other deep learning architecture. The layers are separated into distinct layers for encoders and decoders. The first encoder layer is linked to the input. Until we reach the final encoded layer, which contains the fewest neurons and represents the bottleneck features, the number of neurons in each succeeding encoder layer decreases. Inputs are transformed until this layer represents the reduced dimension of the data that can reflect the maximum signals. Following this layer are the decoder layers, where each layer's neuron count increases until the output layer has the same number of neurons as the input.

Autoencoders [35] are unsupervised neural networks used for anomaly detection. They learn to encode and then decode transaction data, and any significant deviation in the reconstruction error can be flagged as potential fraud. These networks are well-suited for detecting new, unseen fraud patterns since they do not rely on labeled data. However, they are effective in anomaly detection scenarios where fraud patterns are not fully known. They require careful tuning to avoid overfitting and might not perform well if the fraud data distribution is very different from normal transaction data.

*Generative Adversarial Networks*

Fiore et al. [36] introduce a framework where a GAN is trained on the minority class (fraudulent transactions) to generate synthetic but realistic fraud examples. These synthetic samples are then added to the training data to balance the dataset. A classifier is then trained on this augmented dataset.

The following steps describe how the GAN framework works:

1. Train classifier $C_0$ on original dataset.

2. Extract minority class examples (frauds) from training set.

3. Train a GAN using these fraud examples.

4. Generator G produces synthetic fraud samples from random noise.

5. Discriminator D distinguishes between real and synthetic frauds.

6. Generate synthetic frauds F′ using trained G.

7. Augment training set with F′.

8. Train a new classifier $C_a$ on the augmented data and compare with $C_0$.

Metrics used include Sensitivity (Recall), Specificity, Precision, F-measure, and Accuracy. The results show an increase in sensitivity (recall) when training on augmented data, with a slight drop in specificity due to more false positives. The best performance was observed when synthetic fraud samples were approximately twice the number of real fraud cases. The proposed method outperformed SMOTE, a widely used synthetic oversampling technique.

These networks are effective for generating realistic fraudulent transaction data in cases of imbalanced datasets. That can augment training datasets, improving the model's ability to detect rare fraudulent patterns. However training GANs can be challenging due to their adversarial nature. The quality of synthetic data generated depends heavily on the architecture and training process. There are several types of GAN architectures that can used to generate synthetic data like conditional GANs (cGANs),Wasserstein GANs (wGANs), and Hybrid GANs (hGANs).

## Legal and ethical dimensions of deploying deep learning models in finance domain

Deploying deep learning models in finance offers significant benefits, such as enhanced risk assessment, fraud detection, and personalized financial services. However, it also raises critical legal and ethical considerations.

*Legal Considerations*

Data privacy and protection: Deep learning models often require vast amounts of personal and financial data. Ensuring compliance with data protection regulations like the General Data Protection Regulation is essential to safeguard user privacy and maintain trust.

Transparency and explainability: The "black box" nature of some deep learning models can make it challenging to understand how decisions are made, which is problematic in regulated financial environments where explainability is crucial for accountability and compliance.

Regulatory compliance: Financial institutions must navigate a complex landscape of regulations that may not have kept pace with AI advancements. Ensuring that deep learning applications adhere to existing financial laws and anticipating future regulatory changes is vital.

*Ethical Considerations*

Bias and fairness: Deep learning models trained on historical data may inadvertently perpetuate existing biases, leading to unfair treatment of certain groups in lending, insurance, or investment decisions. It is crucial to implement measures that detect and mitigate such biases.

Accountability: Determining responsibility for decisions made by autonomous deep learning systems can be complex. Establishing clear accountability frameworks ensures that ethical standards are upheld and that there is recourse in cases of harm or error [37].

Impact on employment: The automation of financial services through deep learning can lead to job displacement. Ethically deploying these technologies involves considering their impact on employment and implementing strategies to mitigate negative effects on the workforce.

Addressing these legal and ethical dimensions is crucial for the responsible integration of deep learning in finance, ensuring that technological advancements do not compromise fairness, transparency, or societal well-being.

## Results and discussion

Table *1* summarizes different neural networks for the purpose of credit card fraud detection.

| Neural Network | Features | Advantages | Limitations | Findings |
|---|---|---|---|---|
| Artificial Neural Network (ANN) [31] | Fully connected layers; static data input. Latency: Low to Moderate – fast inference due to simple architecture. Interpretability: limited explainability. Scalability (Handling Large Data): Easily scaled with more neurons/layers | i) Flexible in learning non-linear patterns. ii) Capable of handling large datasets and complex features | Struggles with imbalanced data; limited for temporal patterns | ANN achieved higher accuracy (93.7%) compared to the existing Random Forest model (90.1%) |
| Convolutional Neural Network (CNN) [32] | Local feature extraction (adapted for tabular or transformed data). Latency (Real-Time Suitability): Designed for spatial data, so less optimal for tabular fraud data. Interpretability: Harder to interpret convolutional layers. Scalability (Handling Large Data): Scales well with GPU support | Captures feature correlations; adaptable to structured data | i) Automatic feature extraction, reducing the need for manual feature engineering. ii) High accuracy for detecting complex patterns in transaction data | Accuracy for EPOCH size 35 is 0.999, Precision 0.932, Recall 0.775, AUC 0.929 |
| Recurrent Neural Network (RNN) [33] | Sequential processing; temporal dependencies. Latency (Real-Time Suitability): Sequential computation causes slower inference. Interpretability: Temporal dependencies are hard to interpret. Scalability (Handling Large Data) is moderate | Captures time-series patterns; detects unusual sequences | Vanishing gradient issues; computationally intensive for long sequences | AUC score is 0.782, Accuracy score is 0.802, Lift index is 0.659 |
| Long Short-Term Memory (LSTM) [34] | Gated RNN; overcomes vanishing gradients. Latency (Real-Time Suitability): slower than RNN due to gating mechanisms. Interpretability: Some interpretability via memory cell analysis. Scalability (Handling Large Data): Needs careful tuning to scale | Handles long-term dependencies; suitable for temporal data | High computational cost; sensitive to hyperparameter tuning | Precision is 0.8575, Recall is 0.7408, F1-score is 0.786, AUC-ROC is 0.8702, AUC–PR is 0.6292 |
| Autoencoders [35] | Encoder-decoder architecture; unsupervised anomaly detection. Latency (Real-Time Suitability): Simple encoder-decoder structure enables efficient anomaly detection. Interpretability: Difficult to understand latent feature space. Scalability (Handling Large Data): works well on large tabular datasets | Detects anomalies via reconstruction error; learns compressed representations | False positives if thresholds are not set correctly | Using the holdout method, Recall is 0.727, Precision is 0.5714, and AUC-ROC is 0.746. Using 5-fold cross-validation, Recall is 0.57, Precision is 0.686, and AUC-ROC is 0.729 |
| Generative Adversarial Network (GAN) [36] | Generator-discriminator pair; unsupervised or semi-supervised learning. Latency (Real-Time Suitability): Training is complex; inference faster but not ideal for real-time. Interpretability: both generator and discriminator are opaque. Scalability (Handling Large Data): Requires careful balancing, harder to train on large imbalanced data | Generates synthetic fraud data; improves dataset balance | Training GANs can be challenging due to their adversarial nature. | Sensitivity is 0.702, Specificity is 0.999, Precision is 0.958, F-measure is 0.810, and Accuracy is 0.999 |

### TABLE 1: Summary of Deep Learning Techniques Used in Credit Card Fraud Detection

AUC–PR, Area Under the Precision–Recall Curve; AUC-ROC, Area Under the Receiver Operating Characteristic Curve; GPU, Graphics Processing Unit

## Conclusions

Deep learning neural networks offer significant advantages over traditional machine learning models in fraud detection, particularly in scenarios involving complex patterns, large-scale data, or dynamic behaviors. Deep learning models automatically extract and learn hierarchical features from raw data, eliminating the need for extensive manual feature engineering required by traditional machine learning models. Neural networks are adept at identifying subtle, nonlinear, and high-dimensional relationships within data, which are common in fraudulent activities. Deep learning models perform better with large and diverse datasets, leveraging their ability to learn complex representations. Traditional models, such as logistic regression or decision trees, often plateau in performance with increasing data size. Fraud patterns continuously evolve. Deep learning architectures like LSTMs and Graph Neural Networks can adapt to temporal changes and relational dynamics in transaction data, providing an edge in identifying new fraud strategies. Techniques like autoencoders, GANs, and hybrid deep learning models can handle imbalanced datasets more effectively by learning representations of normal transactions and detecting deviations. Some promising future research paths in credit card fraud detection, focusing on emerging trends like Explainable AI, Graph Neural Networks, and Federated Learning, include integrating Explainable AI with real-time fraud detection systems, credit card transactions forming natural graphs (user-merchant relations, shared IPs, geolocation clusters), which are not fully exploited by standard deep learning, designing privacy-preserving fraud detection models that aggregate knowledge across institutions.

# Additional Information

## Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

**Concept and design:** Pranita N. Sangit, Savita Sangam

**Acquisition, analysis, or interpretation of data:** Pranita N. Sangit, Savita Sangam

**Drafting of the manuscript:** Pranita N. Sangit, Savita Sangam

**Critical review of the manuscript for important intellectual content:** Pranita N. Sangit, Savita Sangam

**Supervision:** Savita Sangam

## Disclosures

**Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

## Acknowledgements

We would like to express our gratitude to Shah and Anchor Kutchhi Engineering College, Chembur, Mumbai, for providing the necessary resources and support for this study. We also extend our appreciation to our Principal, Dr. Bhavesh Patel, for his valuable insights and guidance throughout the research process. Additionally, we acknowledge the contributions of Dr. Pramod Bhavarthe for his support in facilitating this work. Lastly, we thank the open-source community and researchers whose work has laid the foundation for advancements in Deep Learning techniques used in Credit Card Fraud Detection.

# References

1. Sarker A, Yasmin M, Rahman M, Rashid M, Roy B: Credit card fraud detection using machine learning techniques. Journal of Computer and Communications. 2024, 12:1-11. 10.4236/jcc.2024.126001
2. Bin Sulaiman R, Schetinin V, Sant P: Review of machine learning approach on credit card fraud detection. Human-Centric Intelligent Systems. 2022, 2:55-68. 10.1007/s44230-022-00004-0
3. Sumanth CH, Kalyan PP, Ravi B, Balasubramani S: Analysis of credit card fraud detection using machine learning techniques. 7th International Conference on Communication and Electronics Systems, ICCES Coimbatore, India. 2022, 1140-1144. 10.1109/ICCES54183.2022.9835751
4. Penumala S, Santhi Sree K: A comparative study of sampling techniques for imbalanced credit card fraud detection. International Journal for Research in Applied Science & Engineering Technology (IJRASET). 2024, 12:789-800.
5. Shamsudin H, Yusof UK, Jayalakshmi A, Akmal Khalid MN: Combining oversampling and undersampling techniques for imbalanced classification: A comparative study using credit card fraudulent transaction dataset. 2020 IEEE 16th International Conference on Control & Automation (ICCA). 2020, 803-808. 10.1109/ICCA51439.2020.9264517
6. Rtayli N: An efficient deep learning classification model for predicting credit card fraud on skewed data. Journal of Information Security and Cybercrimes Research. 2022, 5:57-71.
7. Akinwamide SO, Taiwo F, Ibitayo FB: Prediction of fraudulent or genuine transactions on credit card fraud detection dataset using machine learning techniques. International Journal for Research in Applied Science & Engineering Technology (IJRASET). 2022, 10:5061-5071. 10.22214/ijraset.2022.44962
8. Alamri M, Ykhlef M: Hybrid undersampling and oversampling for handling imbalanced credit card data. IEEE Access. 2024, 12:14050-14060. 10.1109/access.2024.3357091
9. Ahirwar N, Singh D, Maheshwar K: Efficient credit card fraud detection based on multiple ML algorithms. 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Pune, India. 2024, 1-7. 10.1109/I2CT61223.2024.10544195
10. Ahmed AN, Saini R: Detection of credit card fraudulent transactions utilizing machine learning algorithms. 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India. 2023, 1-5. 10.1109/INOCON57975.2023.10101137

11. Ning W, Chen S, Lei S, Liao X: AMWSPLAdaboost credit card fraud detection method based on enhanced base classifier diversity. IEEE Access. 2023, 11:66488-66496. 10.1109/access.2023.3290957
12. Nguyen N, Duong T, Chau T, Nguyen VH, Trinh T, Tran D: A proposed model for card fraud detection based on CatBoost and deep neural network. IEEE Access. 2022, 10:96852-96861. 10.1109/access.2022.3205416
13. Almhaithawi D, Jafar A, Aljnidi M: Example-dependent cost-sensitive credit cards fraud detection using SMOTE and Bayes minimum risk. SN Applied Sciences. 2020, 2:1574. 10.1007/s42452-020-03375-w
14. Mniai A, Tarik M, Jebari K: A novel framework for credit card fraud detection. IEEE Access. 2023, 11:112776-112786. 10.1109/access.2023.3323842
15. Lunghi D, Paldino GM, Caelen O, Bontempi G: An adversary model of fraudsters' behavior to improve oversampling in credit card fraud detection. IEEE Access. 2023, 11:136666-136679. 10.1109/access.2023.3337635
16. Kalid SN, Khor K-C, Ng K-H, Tong G-K: Detecting frauds and payment defaults on credit card data inherited with imbalanced class distribution and overlapping class problems: a systematic review. IEEE Access. 2024, 12:23636-23652. 10.1109/access.2024.3362831
17. Salekshahrezaee Z, Leevy JL, Khoshgoftaar TM: The effect of feature extraction and data sampling on credit card fraud detection. Journal of Big Data. 2023, 10:6. 10.1186/s40537-023-00684-w
18. Das S: PCA-based anomaly detection in credit card transactions: a machine learning approach. 2024, 10.6084/m9.figshare.26300503.v1
19. Brezočnik L, Fister I, Podgorelec V: Swarm intelligence algorithms for feature selection: a review. Applied Sciences. 2018, 8:1521. 10.3390/app8091521
20. Ileberi E, Sun Y, Wang Z: A machine learning based credit card fraud detection using the GA algorithm for feature selection. Journal of Big Data. 2022, 9:24. 10.1186/s40537-022-00573-8
21. Trivedi NK, Simaiya S, Lilhore UK, Sharma SK: An efficient credit card fraud detection model based on machine learning methods. International Journal of Advanced Science and Technology. 2020, 29: 3414-3424.
22. Zhou H, Wei L, Chen G, Lin P, Lin Y: Credit card fraud identification based on principal component analysis and improved Adaboost algorithm. 2019 International Conference on Intelligent Computing, Automation and Systems (ICICAS), Chongqing, China. 2019, 507-510. 10.1109/ICICAS48597.2019.00111
23. Patil S, Godse A, Gawade P, Halkare P, Dhamankar A: Credit card fraud detection using machine learning and blockchain. International Journal for Research in Applied Science and Engineering Technology. 2023, 11:2745-2751. 10.22214/ijraset.2023.52214
24. Pradhan SK, Krishna Rao NV, Deepika NM, Harish P, Kumar MP, Kumar PS: Credit card fraud detection using artificial neural networks and random forest algorithms. 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India. 2021, 1471-1476. 10.1109/ICECA52323.2021.9676142
25. Mizher MZ, Nassif AB: Deep CNN approach for unbalanced credit card fraud detection data. 2023 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates. 2023, 1-7. 10.1109/ASET56582.2023.10180615
26. Femila Roseline J, Naidu GBSR, Samuthira Pandi V, Alamelu S alias Rajasree, Mageswari N: Autonomous credit card fraud detection using machine learning approach. Computers & Electrical Engineering. 2022, 102:108132. 10.1016/j.compeleceng.2022.108132
27. Almarshad FA, Gashgari GA, Alzahrani AIA: Generative adversarial networks-based novel approach for fraud detection for the European cardholders 2013 dataset. IEEE Access. 2023, 11:107348-107368. 10.1109/access.2023.3320072
28. San Miguel Carrasco R, Sicilia-Urbán M-Á: Evaluation of deep neural networks for reduction of credit card fraud alerts. IEEE Access. 2020, 8:186421-186432. 10.1109/access.2020.3026222
29. Tingfei H, Guangquan C, Kuihua H: Using variational auto encoding in credit card fraud detection. IEEE Access. 2020, 8:149841-149853. 10.1109/access.2020.3015600
30. Zhang W, Zhang S, Chen J, Huang H: CCFD-GAN: credit card fraud detection based on generative adversarial networks enhanced by penalty mechanism. 2023 International Joint Conference on Neural Networks (IJCNN), Gold Coast, Australia. 2023, 1-8. 10.1109/ijcnn54540.2023.10191810
31. Asha RB, Suresh Kumar KR: Credit card fraud detection using artificial neural network. Global Transitions Proceedings. 2021, 2:35-41. 10.1016/j.gltp.2021.01.006
32. 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, 10:39700-39715. 10.1109/access.2022.3166891
33. Hsu T-C, Liou S-T, Wang Y-P, Huang Y-S, Che-Lin: Enhanced recurrent neural network for combining static and dynamic features for credit card default prediction. ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK. 2019, 1572-1576. 10.1109/ICASSP.2019.8682212
34. Forough J, Momtazi S: Ensemble of deep sequential models for credit card fraud detection. Applied Soft Computing. 2021, 99:106883. 10.1016/j.asoc.2020.106883
35. Fanai H, Abbasimehr H: A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection. Expert Systems with Applications. 2023, 217:119562. 10.1016/j.eswa.2023.119562
36. Fiore U, De Santis A, Perla F, Zanetti P, Palmieri F: Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences. 2019, 479:448-455. 10.1016/j.ins.2017.12.030
37. Mehrabi N, Morstatter F, Saxena N, Lerman K, Galstyan A: A survey on bias and fairness in machine learning. ACM Computing Surveys. 2021, 54:1-35. 10.1145/3457607