ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2025;10(2):1-10

REVIEW ARTICLE

Analytical Review of Deep Learning Architectures in Financial Frameworks for Fraud Identification of Credit Cards

Prithviraj Singh Rathore*

Department of Computer Sciences and Applications, Mandsaur University, Mandsaur, Madhya Pradesh, India

Received on: 12-03-2025; Revised on: 10-04-2025; Accepted on: 02-05-2025

ABSTRACT

The finance sector has made cybersecurity a crucial focus due to the exponential rise in cyberattacks and digital financial crimes. One of the most significant issues is credit card fraud, which has grown in frequency alongside the proliferation of both online and physical shopping. When faced with increasingly complex fraud strategies, traditional rule-based and anomaly detection systems might be resource-intensive and fail to detect them. The purpose of this research is to examine state-of-the-art deep learning (DL) methods for efficient and precise detection of credit card fraud. Its main focus is on deep neural architectures, including long short-term memory, convolutional neural networks, autoencoders, and hybrid ensemble models. These methods demonstrate superior performance in capturing non-linear relationships and temporal dependencies within transactional data. The use of data preprocessing methods such as principal component analysis and the synthetic minority oversampling technique helps with class imbalance and dimensionality reduction. Experimental results validate the effectiveness of DL approaches in enhancing detection accuracy and robustness, thereby contributing to more resilient financial security systems.

Key words: Anomaly detection, autoencoder, convolutional neural network, credit card fraud, deep learning, fraud detection, GRU, long short-term memory, real-time analytics, xgboost

INTRODUCTION

Internet banking is rapidly expanding, and financial institutions increasingly provide the public with actual business facilities. Electronic payment systems have grown vital in today's competitive financial market due to the convenience they provide when purchasing goods and services. The introduction of cashless transactions and the associated insurance against lost, damaged, or stolen items has revolutionized consumer convenience.[1,2] Credit and debit cards have further expanded this insurance. By requesting confirmation from consumers before making a purchase using their credit cards, an extra layer of protection is incorporated. Credit card fraud, however, is an ongoing issue that hinders both customer and bank profits. Internet fraudsters are always coming up with new techniques, making it harder for financial institutions and other organizations to detect and prevent their crimes.

Address for correspondence:
Prithviraj Singh Rathore
E-mail: prathviraj.rathore@meu.edu.in

A credit card allows its holder to purchase goods and services or withdraw cash within a specified credit limit, offering the advantage of deferred payments to the next billing cycle.[3,4] However, this convenience also presents an opportunity for fraudulent activities. Fraudsters can exploit vulnerabilities to perform unauthorized transactions, often bypassing existing security mechanisms and causing substantial financial losses in a short span without the cardholder's knowledge.

The crime of fraud is committed when one party uses deceit to obtain money or property unfairly or unlawfully, even if the other party does not face immediate legal repercussions for their actions.[5-7] To mitigate such risks, financial systems employ two primary countermeasures: Fraud prevention and fraud detection mechanisms. Fraud prevention refers to proactive techniques aimed at eliminating fraud before it occurs, whereas fraud detection systems focus on identifying fraudulent transactions that have already bypassed preventive controls. These detection systems must evaluate every transaction, regardless of previous filters, to promptly recognize anomalies and prevent further loss.

The proliferation of digital technologies, such as telephone banking, automated teller machines (ATMs), and online credit systems, has intensified the risk and impact of fraud, making manual verification of each transaction infeasible due to cost and scalability constraints. In this context, machine learning (ML) and, more recently, deep learning (DL) have emerged as powerful tools to identify fraudulent behavior through automated classification techniques.[8,9] By learning from historical patterns of fraud, these systems can classify and detect new fraudulent instances with higher accuracy.

DL is an approach to ML that uses multilayered, deep artificial neural networks (ANNs) to simulate brain function. These networks consist of multiple hidden layers capable of learning complex, non-linear representations of input data.[10] Particularly well-suited to binary classification challenges such as fraud detection is their capacity to model high-level abstractions. With the rise of sophisticated fraud strategies and the limitations of traditional rule-based methods, DL provides a flexible and scalable answer. It uses massive amounts of transaction data to identify unique and ever-changing instances of fraud.

Structure of the Paper

This paper is organized in the following way: Section II explains the fundamentals of identifying fraudulent charges on credit cards. In Section III, it goes over the DL process and the preprocessing approaches. Section IV delves into various DL architectures that are used for fraud detection. A thorough literature review is presented in Section V, and the study is concluded with important findings and directions for future research in Section VI.

FUNDAMENTALS OF CREDIT CARD FRAUD DETECTION

The crime of credit card fraud is when someone else makes transactions using another person's card without their authorization. It encompasses all forms of bank card fraud, including those involving debit and credit cards. Even though most of the transactions happen online, it can still use the physical card if it is lost or has it is stolen.[11] Fraudsters use a variety of techniques to get their hands on cardholder data. One is phishing, in which the criminal pretends to be a financial official in order to trick the user into giving over sensitive information. Skimming is another kind of card fraud where the criminal uses an interface to enter a system that scans cards directly at points of sale or ATMs. Protecting customers' money and personal information requires detecting credit card fraud. Automated systems and human investigation are the two primary methods for identifying fraudulent actions.

Types and Characteristics of Credit Card Fraud

Credit card fraud is complex; therefore, it is important to know what it is. Examples of common types are:

Card-not-present (CNP) fraud

One distinguishing feature of CNP fraud is that it is both a hybrid and an output crime. Frauds can be perpetrated in either the real world or online, which is why considers them a hybrid cybercrime.[12,13] Since con artists can get victims' credit card details by physically scanning and skimming their cards, CNP fraud might be considered a hybrid cybercrime. Furthermore, criminals may employ social engineering techniques to send unwanted emails in an effort to trick people into divulging their credit card information.

Lost or stolen card fraud

Crucially, fraudulent transactions represent the minority class of primary interest. However, their rarity often hampers the classifier's learning process, resulting in suboptimal model performance.[14] When added together, these two groups accounted for 68% of all instances of card fraud in South Africa during 2007 and 2008.

Counterfeit card fraud

Once a criminal has a legitimate card number, they might use it to make a counterfeit card. The data can thereafter be written onto the magnetic stripe of a new, blank card or entered by hand onto the surface of a counterfeit plastic card.[15] A criminal can find all the information they need to make fake cards with just a few clicks on the Internet. Credit

card counterfeiting equipment, including custom embossing machines, tipping machines, decoding software, and programs for encoding credit card magnetic stripes, may be found on numerous online marketplaces.

Application fraud

Applicants commit credit card application fraud when they supply false information. Finding a fraud system that can detect suspicious applications is the solution to the issue of application fraud. In the first case, known as duplicate applications, numerous applicants provide the same or nearly identical information; in the second, known as identity fraud, numerous applicants utilize the same or nearly identical information to submit their applications.

Behavioral fraud

Conducting sales on a "cardholder present" basis after fraudulently obtaining the details of valid cards is behavioral fraud. This category includes sales conducted over the phone or online, where the only information needed is the card details. For behavioral fraud, a fraud scorecard that forecasts which clients would default is a useful tool.[16,17] Some of the reasons why traditional credit scorecards fail to identify consumers who are likely to default include fraud. How it works: Applying scoring to the prevention of fraud is identical to applying it to any other use case, including profit, default, or collection. Figure 1 depicts the many forms of credit card fraud; the score is calculated by averaging previous occurrences. One of two outcomes is possible: a real or fake consumer.

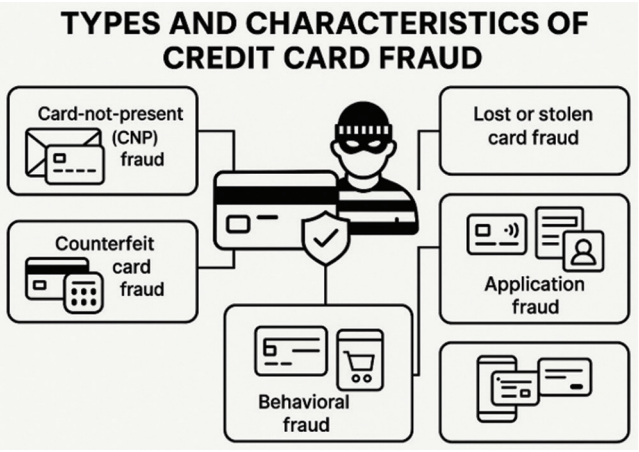

Figure 1: Types of credit card fraud

Challenges in Fraud Detection

There are some challenges of fraud:

- Massive imbalance in the data: Since the number of valid transactions (around 0.2 percent) much outweighs the number of fraudulent ones. Crucially, fraudulent transactions represent the minority class of primary interest. However, their rarity often hampers the classifier's learning process, resulting in suboptimal model performance.
- Unavailability of data sets: Since card companies are unable to divulge these to the general public or academics for reasons related to privacy, secrecy, confidentiality, and the law. The vast number of ML algorithms and the tremendous interest in this field are not enough to propel research forward; real data are essential. The substitution of synthetic data and the lack of or difficulty gaining access to research and its results were also mentioned.
- Limited published work: The characteristics of the data or the parameters utilized by classifiers are typically not divulged by researchers. Funding institution constraints may be to blame. It is challenging to exchange ideas in fraud detection because of security and privacy issues, which, according to, greatly hinders the development of innovative approaches for detecting credit card fraud.
- Adaptive and innovative fraudulent behavior: Constant relearning of the new patterns is necessary due to the frequent and ongoing evolution of fraud and normal profiles. Furthermore, the computer could learn the wrong details about fraudulent transactions in the past and treat them as real. It just takes one slip-up for new frauds to emerge that look like regular transactions.

Traditional Detection Techniques

One of the first approaches brought in was a rule-based system for detecting credit card fraud. Such systems are based on a pre-worked-out body of logical rules developed by domain experts to mark anomalous transactions. They all have different attributes, such as the amount of transactions, time, location, or frequency, that they target. An example here is of a transaction that is exceeding a

specific amount in a foreign place may be marked as suspicious.[18] Although rule-based systems are simple, obvious, and easy to execute, they are ineffective and cannot keep up with the changes in the nature of fraud. They have a tendency to give out high false-positive outcomes and cannot be useful in representing complex or subtle fraud patterns. The limitations of rule-based systems in learning and development make them an incomplete solution to the credit card fraud detection problem when applying DL. They are, therefore, becoming augmented and even superseded by even more data-driven methods, more importantly DL models, which can learn on its own to detect non-linear relationships and shifting fraudulent patterns. Despite its shortcomings, the rule-based systems are also useful in hybrid frameworks of fraud detection, where they help perform the initial screening before performing a deeper-level inspection.

ML approaches

ML is a technique that may be applied to many different issues, particularly in fields that deal with data analysis and processing. The imbalanced dataset can be resolved with the help of ML, which can be categorized as supervised, unsupervised, or reinforcement ML. The ability to automatically recognize patterns across massive amounts of data is what makes ML approaches so useful for detecting and preventing fraud. Differentiating between genuine and fraudulent activities becomes easier with the right ML models in place. Eventually, these smart systems might figure out how to cheat previously unknown frauds. Figure 2 displays various ML methods.

- Supervised learning: Supervised learning trains ML systems using labeled or modifiable data sets with known variable goals. Classification, inference, and regression are all instances of supervised learning. Most ML approaches rely on supervised models trained on massive datasets of correctly tagged transactions. There is a valid and a fraudulent category for every single transaction.
- Unsupervised learning: One way to train ML algorithms is through unsupervised learning, which involves using datasets with potentially unclear target variables.[19] Finding the most important patterns in the data is the model's goal. Cluster segmentation and dimensionality reduction are examples of unsupervised learning approaches.
- Semi-supervised learning: Models can be trained using unlabeled data by semi-supervised learning, a type of learning that combines supervised and unsupervised techniques. In this approach, the best way to represent data is determined by the unsupervised learning attribute, and then the relationships within that representation are analyzed by the directed learning attribute, giving rise to predictions.

OVERVIEW OF DL IN FRAUD DETECTION

Figure 3 shows that DL, a subset of ML, makes use of neural networks to either generate predictions or convert incoming data into new representations. Among the many architectures used in DL are deep reinforcement learning, convolutional neural networks (CNNs), RNNs, transformers, and deep neural networks (DNNs). When applied to tasks such as picture recognition, Natural Language Processing (NLP), Computer Vision (CV), and speech recognition, these DL architectures have achieved results that are competitive with, and even better than, those of human specialists. At the same time, RNNs are shining brightest when it comes to sequential data modeling, which includes things such as credit card transactions.[11] To address the vanishing gradients

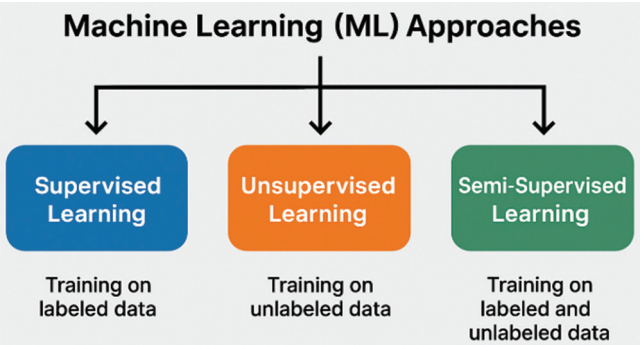

Figure 2: Machine learning

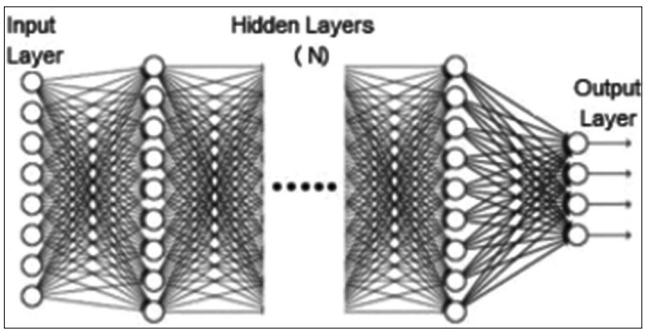

Figure 3: Deep neural network

problem, the long short-term memory (LSTM) was developed.[20] While RNNs perform well as models for sequence data, their training becomes challenging when gradients explode or disappear. The Gated Recurrent Unit (GRU) can maintain data and perform LSTM-like tasks without an additional memory unit, despite its development in. To improve the accuracy of their state forecasting algorithms, bidirectional versions of these networks use data from both the past and the future.

General DL Workflow for Fraud Detection

The typical workflow for implementing DL in fraud detection involves several key stages:

Data collection and integration

The fraud detection system is built upon the records of financial institutions' transactions. The input transactional data are retrieved from the transaction database to execute the fraud detection process.[21] The following will be displayed if the database has n bits of transactional data, which it will refer to as K:

$$K = \{H_1, H_2 \ldots\ldots H_n\}: 1 \leq l \leq n \quad (1)$$

Database (K), transaction data (H), and the total number of records relevant to transactions are shown in the first equation. The preprocessing step takes the input data H_1, selected from the database, to move on with processing, the detection method.

Data preprocessing

The data that H_1 collected from the database are to be preprocessed by the preprocessing module. Data cleaning, normalization, and encoding should precede training.

Model selection and training

Prioritize CNNs, LSTMs, or hybrid models as your DL architectures of choice. Train them with transaction data from the past.

Validation and testing

Evaluate model performance using labeled test data to assess generalizability.

Data Preprocessing Techniques

Below are some techniques of data preprocessing:

SMOTE

The SMOTE strategy employs an oversampling procedure with the main objective of increasing the minority class's case count, leading to the formation of a new synthetic sample.[22] A new synthetic sample can be generated from any point along the line that starts with the minority class samples' nearest neighbors. The experiment employs the SMOTE class of the imbalanced-learn package to perform the over-sampling. The total number of occurrences of the minority class after resampling divided by the total number of occurrences of the majority class yields the sampling ratio.

Principal component analysis (PCA)

Data scaling commonly employs principal component analysis. A new set of uncorrelated variables, or PCs, is formed that sequentially maximizes variance to reduce the number of correlated variables from n to m. The newly introduced variables are linear combinations of their older, less important counterparts. The goal is to account for as much variation in the original data as can be feasibly explained using the first principal component.

DL Models for Fraud Detection

There are some models of DL for fraud detection discussed below:

Recurrent neural networks (RNNs) and LSTM

The fraud detection sector has adopted RNN-based DL techniques because these algorithms are often considered to be among the most accurate for sequence analysis tasks.[23] Rapid neural networks (RNNs) can assess the changing temporal behavior of various bank accounts by mimicking the sequential reliance between subsequent credit card transactions.

LSTM artificial RNN [Figure 4]. To forecast a transaction label from a sequence of prior transactions, LSTM neural networks use feedback connections between hidden units linked with discrete time steps and, unlike traditional feedforward networks, learn sequence dependencies over time.[24] To address the problem of regular RNNs training with vanishing and exploding gradients, the LSTM neural network

was created. A promising use of LSTM networks is the detection of fraudulent credit card transactions.

Autoencoders

An autoencoder is an unsupervised learning model that attempts to reconstruct its input, denoted as x, through a compressed representation. The output xˆis a reconstruction of the original input x. Autoencoders learn by encoding the input into a lower-dimensional latent space and then decoding it back to its original form. The encoder maps the input to the hidden layer (latent representation), and the decoder reconstructs the input from this representation. Using low-dimensional, nonlinear hidden layers, the autoencoder captures essential features of the input data. However, due to the bottleneck structure which limits the information throughput the model must learn efficient compression of the input. The structure of the autoencoder, including the hidden layer, is illustrated in Figure 5.

DNNs/Multilayer Perceptrons (MLPs)

The unique architecture of DNNs enables them to learn and adapt, ultimately leading to the best possible solution for any given problem. Its building blocks are neurons arranged in a hierarchical fashion. A DNN is an ANN that uses a network of linked neurons to simulate the way the human brain works. A multitude of mathematical computations are performed by these neurons using data supplied from the activation function and the input layer. With the help of a feedforward multilayer perceptron, a specific kind of three-layer neural network, the researchers were able to organize the data in this specific case. This network only processes input in one way. For mathematical computations in the hidden layer and output layer, a differentiable sigmoid activation function is utilized. It tackles non-linearly separable problems using the sigmoid activation function.[26] To train itself, the network makes use of the backpropagation learning method, a supervised learning technique. The network was trained using an online financial dataset.

MLP, as depicted in Figure 6, consists of four nodes that take in a vector of four inputs (x_1,x_2,x_3,x_4). Divide all transactions into two groups: suspicious (S) and non-suspicious (-S). It is from the MLP's output that it determines if a transaction is suspicious (S) or not (-S).

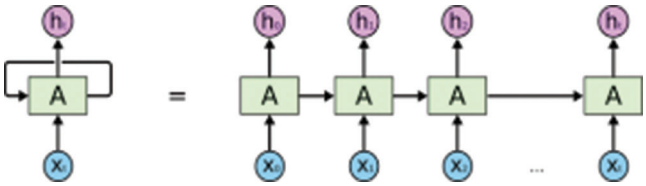

Figure 4: Long short-term memory

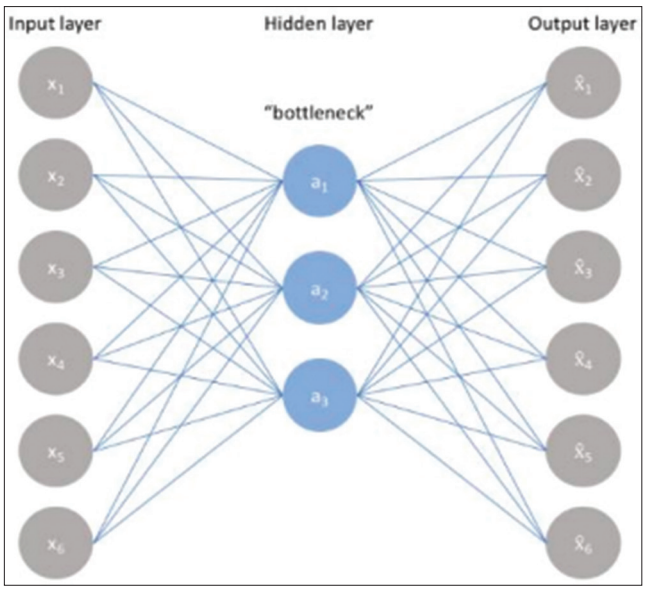

Figure 5: Autoencoder with hidden layers

Hybrid and Ensemble Deep Models

A hybrid ensemble model that combines the capabilities of CNNs, LSTMs, and transformers, and is built on the XGBoost meta-learner. Incorporating the supplementary features of the two models helps strengthen and improve credit card fraud detection systems.[27] To understand the spatial patterns and localized characteristics in the transactional data, CNNs are utilized as base

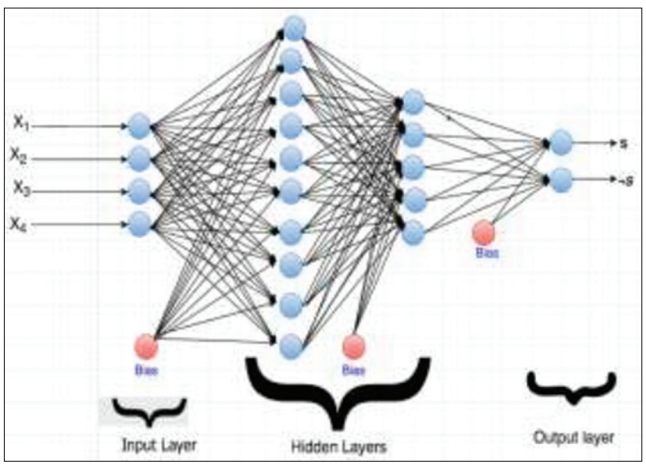

Figure 6: Multilayer perceptron

learners. As a foundational learning mechanism, LSTMs are used to grasp the sequential patterns and temporal dependencies included in transaction sequences. LSTMs can detect suspicious patterns of transactions that would not be obvious from a single transaction. On the other hand, transformers are used as foundational learners to record intricate interdependencies and interactions in transaction sequences.

The suggested hybrid ensemble model makes use of XGBoost as its meta-learner feature. XGBoost is an effective gradient-boosting technique that captures intricate patterns and works wonders with tabular data. A hybrid ensemble model uses a stacking technique to aggregate predictions from the CNN, LSTM, and transformer base learners, with XGBoost serving as the meta-learner. Pictured in Figure 7 are the output vectors P_{CNN}, P_{LSTM}, and $P_{Transformer}$, which are the results of each base model's prediction on the validation set following its independent training on the training set. The XGBoost meta-learner trains on the ensemble of predictions from each base learner and uses these outputs as input features to make the final classification decision.

LITERATURE REVIEW

Credit card fraud detection research on four DL architectures, ANN, CNN, autoencoder, and sequential models, is compiled here. Class imbalance, sparse features, and real-time detection are some of the main issues that are tackled. A comparative summary of recent approaches, performance metrics, and future directions is provided in Table 1 for a concise overview.

Yadlapalli *et al*., the major focus of this study is to build an ANN model and compare it with other famous ML models that can detect credit card theft and help users stay secure. The reliability and the resilience of the ANN model were ensured by fine-tuning it to handle class imbalance and sparseness of fraud cases. Their ANN model beats all other models in the credit card fraud detection arena in terms of accuracy and durability, with a record of 99.99%.[28]

Elmangoush *et al*. investigate the matter and create a dependable model to detect cases of credit card fraud. A synthetic minority oversampling approach has been implemented to tackle the issue of class imbalance. Developing a model for credit card identification using sequential DL methods was the subsequent stage. By enhancing feature extraction and representation using data supplied by SMOTE, this approach tackles the issue of insufficient features. They compared the proposed model to existing literature in the field and looked at its accuracy, detection rate, and f-measure. The outcomes demonstrate that the proposed model surpasses the most advanced models in this domain.[29]

Mohammad and Logeshwaran proposed a learning strategy for real-time credit card fraud detection. Their framework leverages deep learning (DL) techniques to enable fast and accurate identification of fraudulent transactions. By utilizing advanced DL algorithms, the system analyses real-time transactional data to detect anomalies indicative of fraud. Trained through a data-driven approach, the DL-based model can dynamically adapt to emerging fraud patterns, enhancing its detection capabilities over time. This adaptability allows it to maintain high accuracy in identifying fraudulent behaviour. Moreover, the framework supports real-time analytics on large volumes of data, making it well-suited for financial institutions that process high transaction volumes. Notably, the architecture offers significantly higher throughput for a given latency compared to traditional methods, potentially reducing response time and minimizing financial losses due to fraudulent activities..[30]

Satti *et al*., the investigation's objective is to establish a connection between these frauds. The ML literature mentions a number of credit card recognition methods, including XG Boost,

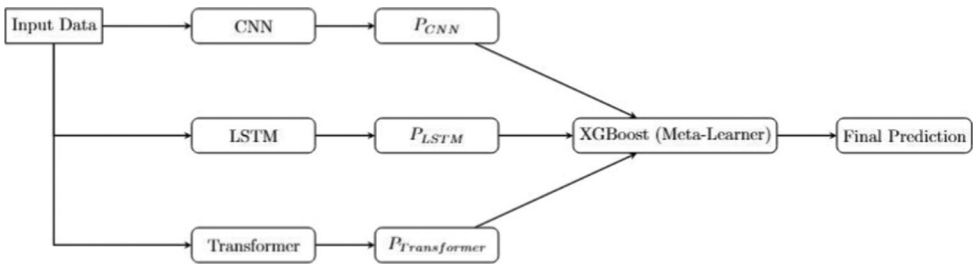

Figure 7: Proposed stacking ensemble approach

Table 1: Literature review based on deep learning architectures for credit card fraud in financial systems

Reference	Study on	Approach	Key findings	Challenges	Future direction
Yadlapalli *et al*. (2025)	ANN vs. ML models	ANN optimized for class imbalance	Achieved 99.99% accuracy; outperformed traditional ML models	Sparse fraud patterns; imbalanced data	Extend to hybrid DL models for further improvement
Elmangoush *et al*. (2024)	Sequential DL with SMOTE	SMOTE + Sequential DL for better feature extraction	0.99924 Accuracy and 0.75976 F-measure; superior to existing models	Class imbalance and feature insufficiency	Explore advanced feature engineering and real-time detection
Mohammad and Logeshwaran (2024)	Detecting digital fraud in real-time	DL with real-time analytics	High throughput and adaptability to new frauds	Latency vs. accuracy trade-offs	Incorporate edge computing for ultra-low latency detection
Satti *et al*. (2024)	Comparative analysis of ML/DL	Compared DL models with XGBoost, SVM, RF, etc.	AUC of up to 98.1%, F1-score of 85.71, and accuracy of 99.9%	DL models still lag in generalization	Combine ensemble and DL for robust detection
Bharath *et al*. (2023)	Autoencoder-based DL	ILSDFD using autoencoder and feature selection	Adapts to new fraud patterns with high performance	Evolving fraud patterns and feature drift	Employ continuous learning and adaptive training
Chaudhari *et al*. (2023)	DL + Face detection	Two-step verification using face + DL	Enhanced verification mechanism with DL integration	Privacy and hardware dependency	Improve facial verification robustness with biometric fusion
Gambo *et al*. (2022)	CNN + ADASYN	CNN with ADASYN Sampling	Achieved 0.9982 accuracy, 0.9965 precision, 0.9999 recall	Class imbalance and CNN overfitting	Optimize CNN architecture and use explainable AI for transparency

ANN: Artificial neural network, ML: Machine learning, DL: Deep learning, CNN: Convolutional neural network, AUC: Area under the curve, AI: Artificial intelligence, ADASYN: Adaptive synthetic

Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), Logistic Regression (LR), and extreme learning method. Ultramodern deep literacy algorithms are still needed toward lower fraud losses due to their low delicacy. Exercising the most recent developments in deep literacy algorithms has been primarily ideal in order to achieve this. Toward achieving effective results, a relative analysis of machine literacy and deep literacy ways was conducted.[31]

Bharath *et al*., the proliferation of online shopping and payment systems has been linked to an increase in financial fraud, particularly the fraudulent use of credit cards. As a result, instantly implementing systems that can detect credit card theft is essential. People all across the world are increasingly making purchases using stolen credit cards, and this situation needs to be addressed immediately. Limiting this kind of behavior is good for consumers because the system's main purpose is to stop users from being charged for services and goods they did not authorize. Extreme caution is required when selecting fraudulent transaction attributes for use in ML-based credit card fraud detection.[32]

Chaudhari *et al*. explored various machine learning (ML) techniques for classifying fraudulent credit card transactions. These approaches are based on the assumption that patterns in historical transaction data can help identify suspicious activity. However, the dynamic nature of consumer behavior and the evolving tactics of fraudsters pose significant challenges to traditional ML models. To address these limitations, the authors proposed a deep learning (DL)-based framework capable of analyzing both historical and real-time transactional data to detect anomalies. DL models demonstrated superior performance compared to conventional ML methods due to their ability to extract complex features and adapt to new fraud patterns. Their proposed solution includes a two-stage verification system that combines DL techniques with facial recognition technology to enhance the accuracy and robustness of credit card fraud detection.[33]

Gambo *et al*. investigate the skyrocketing growth of online purchases made through e-commerce platforms, highlighting the pervasiveness of credit card payments. Consumers and banks lose billions of dollars annually because of CCF strategies that are always evolving to match the speed of industry transformation. It is critical to successfully distinguish fraudulent transactions from the many lawful ones. To address the imbalance in the dataset, this study suggests a CNN model for credit card fraud detection that is based on the adaptive synthetic sampling technique.[34]

The literature review is summarized in Table 1, which highlights the emphasis, methodology,

important findings, obstacles, and suggested future paths of each study.

CONCLUSION AND FUTURE WORK

The growing number of online transactions and the ever-changing methods used by cybercriminals have made the detection of credit card fraud an increasingly pressing issue. There have been several applications of DL approaches because of their efficacy and reliability. Credit card fraud employing DL models has recently been discovered to be significantly more common. To find credit card scams more effectively than traditional rule-based and classical ML methods, this study shows that DL methods such as LSTM, CNN, Autoencoders, and hybrid ensemble models are the best. These models greatly improve the accuracy of detection and cut down on false positives by learning complicated, non-linear patterns and temporal relationships from transactional data. Due to the dynamic nature of financial fraud tactics, DL frameworks provide a scalable and adaptable means of preventing real-time fraud in online banking systems.

The main goal of future work will be to create real-time scam detection systems that use federated learning to make sure that institutions can train models in a way that respects privacy. Furthermore, by integrating explainable artificial intelligence, model transparency will be enhanced, which will help human analysts comprehend and have faith in automated fraud choices. Expanding datasets to include multi-channel transaction data and applying graph neural networks to uncover relational fraud patterns are also promising directions for advancing fraud detection capabilities.

REFERENCES

1. Unogwu OJ, Filali Y. Fraud detection and identification in credit card based on machine learning techniques. Wasit J Comput Math Sci 2023;2:16-22.
2. Wawge SJ. Evaluating machine learning and deep learning models for housing price prediction: A review. Int J Adv Res Sci Commun Technol 2025;5:367-77.
3. Dornadula VN, Geetha S. Credit card fraud detection using machine learning algorithms. Procedia Comput Sci 2019;165:631-41.
4. Majumder RQ. A review of anomaly identification in finance frauds using machine learning systems. Int J Adv Res Sci Commun Technol 2025;5:101-10.
5. Sahin Y, Duman E. Detecting credit card fraud by decision trees and support vector machines. In: IMECS 2011 - International Multi Conference of Engineers and Computer Scientists. Vol. 1. Berlin: Springer; 2011. p. 442-7.
6. Wawge SJ. A survey on the identification of credit card fraud using machine learning with precision, performance, and challenges. Int J Innov Sci Res Technol 2025;10:3345-52
7. Mantha G. Transforming the insurance industry with sales force: Enhancing customer engagement and operational efficiency. North Am J Eng Res 2024;5:3-4.
8. Singh V. Predicting loan default risk in P2P lending platforms: A study of lending club borrowers. Int J Sci Res 2023;12:2255-60.
9. Chaudhari B, Verma SC. Synergizing generative AI and machine learning for financial credit risk forecasting and code auditing. Int J Sci Res Comput Sci Eng Inf Technol 2025;11:2882-93.
10. Abakarim Y, Lahby M, Attioui A. An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning. In: Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications. New York, NY, USA: ACM; 2018. p. 1-7.
11. Mienye ID, Jere N. Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. IEEE Access 2024;12:96893-910.
12. Akdemir N, Yenal S. Card-not-present fraud victimization: A routine activities approach to understand the risk factors. Güvenlik Bilim Derg 2020;9:243-68.
13. Chaudhari B, Verma SC. Achieving high-speed data consistency in financial microservices platforms using NoSQL using Nosql (Mongodb, Redis) technologies. Int J Adv Res Sci Commun Technol 2024;4:750-9.
14. Mishra A. Ai-powered cybersecurity framework for secure data transmission in Iot network. Int J Adv Eng Manag 2025;7:5-13.
15. Burns P, Stanley A. Fraud Management in the Credit Card Industry. Philadelphia, PA: Ten Independence Mall; 2002. p. 1-16.
16. Ramanujam B. Statistical in sights in to anti-money laundering : Analyzing large-scale financial transactions. Int J Eng Res Technol 2025;14:1-6.
17. Chatterjee P, Das A. Adaptive financial recommendation systems using generative ai and multimodal data. J Knowl Learn Sci Technol 2025;4:112-20.
18. Pillai V. System and method for intelligent detection and notification of anomalies in financial and insurance data using machine learning. Pat Off J 2025.
19. Kali H. Optimizing credit card fraud transactions identification and classification in banking industry using machine learning algorithms. Int J Recent Technol Sci Manag 2024;9:85-96.
20. Garg S. AI, blockchain and financial services: Unlocking new possibilities. Int J Innov Res Creat Technol 2022;8:1-4.
21. Kolli CS, Tatavarthi UD. Fraud detection in bank transaction with wrapper model and Harris water optimization-based deep recurrent neural network. Kybernetes 2021;50:1731-50.
22. Karthika J, Senthilselvi A. Smart credit card fraud

detection system based on dilated convolutional neural network with sampling technique. Multimed Tools Appl 2023;82:31691-708.
23. Benchaji I, Douzi S, El Ouahidi B. Credit card fraud detection model based on LSTM recurrent neural networks. J Adv Inf Technol 2021;12:113-8.
24. Janumpally BK. Architecting serverless payment gateways: A systematic analysis of scale, security, and performance trade-offs. Int J Res Comput Appl Inf Technol 2025;8:1186-201.
25. Al-Shabi MA. Credit card fraud detection using autoencoder model in unbalanced datasets. J Adv Math Comput Sci 2019;33:1-16.
26. Mbunge E, Makuyana R, Chirara N, Chingosho A. Fraud detection in E-transactions using deep neural networks-a case of financial institutions in Zimbabwe. Int J Sci Res 2015;6:2319-7064.
27. Chatterjee P. Proactive infrastructure reliability: AI-powered predictive maintenance for financial ecosystem resilience. J Artif Intell Gen Sci 2024;7:291-303.
28. Yadlapalli P, Srivatsal P, Polimera N, Srinivas M. Credit Card Fraud Detection using Machine Learning Algorithms and Artificial Neural Network. In: 2025 International Conference on Artificial Intelligence and Data Engineering (AIDE). United States: IEEE; 2025. p. 539-42.
29. Elmangoush AM, Hassan HO, Fadhl AA, Alshrif MA. Credit Card Fraud Detection Using Synthetic Minority Oversampling Technique and Deep Learning Technique. In: 2024 IEEE 7th International Conference on Advanced Technologies, Signal and Image Processing (ATSIP); 2024. p. 455-8.
30. Mohammad R, Logeshwaran J. Real-Time Credit Card Fraud Detection using Deep Learning Based Framework. In: 2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT); 2024. p. 496-500.
31. Satti P, Tamilkodi R, Maduri N, Ratalu S, Saritha K, Santharaju N. Credit Card Fraud Detection Using Machine Learning and Amp Deep Learning Algorithms. In: 2024 2nd International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES). United States: IEEE; 2024. p. 1-5.
32. Bharath AP, Rajendran N, Devi SD, Saravanakumar S. Experimental Evaluation of Smart Credit Card Fraud Detection System using Intelligent Learning Scheme. In: 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES); 2023. p. 1-6.
33. Chaudhari A, Sontakke A, Tendulkar S, Zambare S, Yewale M. Detecting Credit Card Frauds Using Deep Learning and Face Detection. In: 2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA); 2023. p. 1-6.
34. Gambo ML, Zainal A, Kassim MN. A Convolutional Neural Network Model for Credit Card Fraud Detection. In: 2022 International Conference on Data Science and Its Applications (ICoDSA); 2022. p. 198-202.