Pertanika J. Sci. & Technol. 33 (6): 2641 - 2663 (2025)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Review Article

Credit Card Fraud Detection Using Machine Learning and Deep Learning Techniques: A Review

Shuchita Sheokand and Sunita Beniwal*

Department of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology, Hisar, Haryana 125001, India

ABSTRACT

Credit cards are becoming increasingly common worldwide due to the growing demand for online payments and shopping, resulting in a rise in credit card usage. Consequently, several opportunities may arise for fraudsters to cause scams. A credit card fraud detection (CCFD) system needs to be established, which alerts banking organizations when fraudulent activities occur. Many machine learning (ML) and deep learning (DL) models have been proposed by researchers to detect credit card fraud. In this survey, work done on CCFD has been reviewed. Analyzing the papers provides insight into the challenges associated with CCFD, such as class imbalance and the performance of various ML and DL techniques in detecting fraud. The techniques most used are clustering, DL, ensemble, ML, optimization, synthetic minority oversampling technique (SMOTE), and transfer learning. The analysis was done on datasets, evaluation metrics, tools, publication year, and techniques commonly used for CCFD. The papers studied have utilized Python, MATLAB, and Apache on datasets for credit card fraud taken from various sources, including Kaggle, e-commerce transactions, insurance fraud, and real-world credit card transaction datasets. A comparison between various techniques is conducted using different metrics, including accuracy, precision, recall, and *F*-measure.

Keywords: Clustering, credit card fraud detection, deep learning, machine learning, optimization

ARTICLE INFO

Article history:
Received: 09 December 2024
Accepted: 29 May 2025
Published: 08 October 2025

DOI: https://doi.org/10.47836/pjst.33.6.11

E-mail addresses:
shuchita.sheokand@gmail.com (Shuchita Sheokand)
sunitabeniwalcse@gmail.com (Sunita Beniwal)
* Corresponding author

INTRODUCTION

CCFD is a significant concern in the financial industry, garnering the attention of ML and statistical intelligence groups (Afriyie et al., 2023; Mienye & Sun, 2023), which has resulted in numerous methods being proposed to address this issue (Ahmad et al., 2023; Mahmoudi & Duman, 2015). Given

e-ISSN: 2231-8526

the problem of class imbalance, where the number of unaffected transactions greatly exceeds the number of scams, and concept drift (Alhashmi et al., 2023), where transactions may alter their numerical assets over time, this really seems to be most challenging from a learning viewpoint. Although these are not the only challenges fraud detection systems face when approaching learning (Bahnsen et al., 2015; Jain et al., 2019). Frauds in credit cards can be carried out offline as well as online. E-commerce organizations extensively conduct data mining on their users' logs. This type of log files contains both authentic and fraudulent transactions (Benchaji et al., 2021; Kim et al., 2019). Credit card fraud arises when a fraudster uses an extra card without the approval of a credit card user by locating crucial information like personal identification number (PIN) and password (Carcillo, Le Borgne, et al., 2018; Carcillo et al., 2021; Karthik et al., 2022). As the world is moving towards a cashless society, there is an increasing dependence on online transactions. Modern fraud does not need criminals to be present physically during the fraud, and they employ many approaches to hide their identity (Dal Pozzolo, Caelen, et al., 2014; Dal Pozzolo, Johnson, et al., 2014; Langevin et al., 2022).

Multi-factor authentication (MFA) methods and advanced encryption techniques, such as biometric tools, have been utilized to prevent fraudulent actions and protect credit card holders and issuers, thereby reducing financial losses for users. Conversely, impostors persistently seek out a vulnerability to exploit (Darwish, 2020; Prabhakaran & Nedunchelian, 2023). There is a problem of class imbalance, i.e., distribution among the classes is not even, and the performance of ML algorithms is affected because of this. Various approaches and procedures have been implemented to reduce the disparity between the two classes, addressing the problem. One of the methods used is oversampling to raise the number of transactions in the minority class by arbitrarily imitating the illustrations (Fiore et al., 2019), whereas under-sampling is a method that is utilized to decrease the number of transactions in the majority class (Forough & Momtazi, 2022; Padhi et al., 2022). Ebiaredoh-Mienye et al. (2020, 2022) used a cost-sensitive adaptive boosting (AdaBoost) weighting technique to solve class imbalance by assigning higher weights to the minority class than the majority class, thus increasing accuracy in chronic kidney disease prediction. Obaido et al. (2022) stated that accuracy can be misleading for imbalanced data while using it for disease prediction, so they used balanced accuracy for imbalanced data, which is the arithmetic mean of specificity and sensitivity.

Fraud detection and prevention are the primary methods for reducing credit card scams. To avoid scams, a set of processes, norms, and guidelines is in place. Protecting payment access, intrusion detection schemes, and firewalls are mostly employed approaches to prevent scams (Gama et al., 2014; Zhu et al., 2020). Approaches like data mining, predictive analytics, and clustering methods can be employed for anomaly detection, which you have already employed for disease detection.

Moreover, none of these methods can be used without ML, whether it is unsupervised or supervised, which is valuable for organizing credit card fraud. However, to detect all fraudulent activities, these ML systems must overcome numerous challenges (Ghosh et al., 2022; Habibpour et al., 2023). The primary objective of this study is to analyze different techniques employed in the detection of credit card fraud. The present approaches can be classified into many categories, such as clustering, ML, optimization, SMOTE, transfer learning (TL), ensemble, and DL. The analysis is also conducted by considering various tools, evaluation metrics, and datasets used (Halvaiee & Akbari, 2014).

RELATED WORK

This section provides an analysis of different methods used for detecting credit card fraud. CCFD methods encompass various methodologies, including clustering, ML, optimization, SMOTE, TL, ensemble methods, and DL, among others.

Categorization of Various CCFD Techniques

The categorization of various CCFD methods is: clustering, ML, optimization, SMOTE, TL, ensemble, and DL. Figure 1 shows the categorization of various CCFD methods. The application of these techniques for CCFD and their performance are explained in the ongoing section.

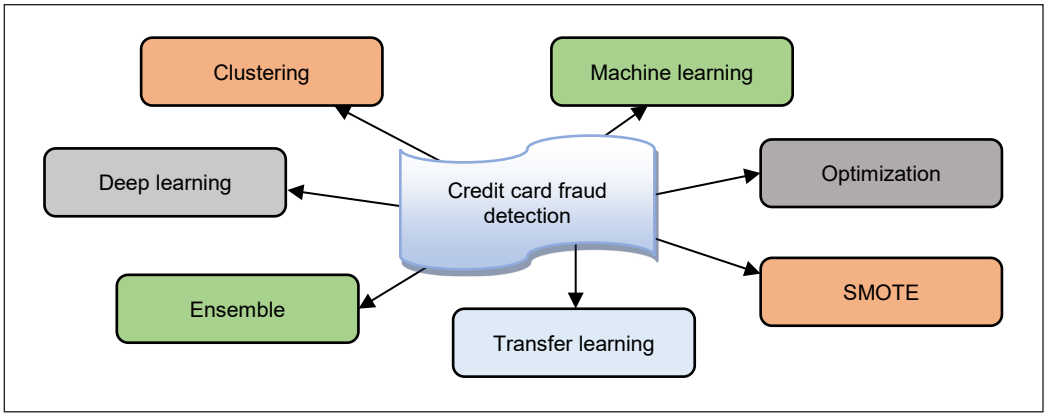

Figure 1. Classification of credit card fraud detection techniques
Note. SMOTE = Synthetic minority oversampling technique

Clustering-Based Methods

Carneiro et al. (2022) introduced a value clustering for categorical attributes (VCCA) method in which the cost is decreased by reducing the training period and by permitting the presence of high-cardinality (HC) features. In this method, ML classifiers like

Support Vector Machines (SVMs) and Random Forests are explored. This approach delivered the programmed design, which was further refined and revised by fraud agents in a transformation board. Kültür and Çağlayan (2017) developed a Cardholder Behavior Model (CBM) and concentrated on real-world issues of CCFD by suggesting an innovative method. The CBM introduced in this paper has a real-world influence and can suggest an extra fraud detection implementation that will work together with the existing rule-based capabilities.

Ahmad et al. (2023) devised an approach of Similarity-based Selection (SBS) to resolve the issue of an imbalanced class by utilizing Fuzzy C-means. To highlight the effectiveness of SBS methodology and validate its advantage, research performance was related to further methods and to address the issue of random under-sampling (RUS), SBS confirms the resemblance and honesty of the features. The determination of discovering the finest under-sampling method is free from RUS issues and gives a better outcome.

DL-Based Methods

The text2IMG conversion method developed by Alharbi et al. (2022) was designed to provide effective outcomes for CCFD. By using computer vision, this technique enhanced the detection of credit card fraud. This method also addresses future approaches for converting various types of text data into images and organizing the information in distinct forms. To discover new differentiating characteristics for CCFD, several feature engineering techniques were used, and this model also offers new features to enhance the performance. Forough and Momtazi (2022) introduced deep neural networks (DNNs) and probabilistic graphical models (PGMs) for analyzing credit fraud detection. This technique was analyzed with the baseline method by utilizing two practical databases and then observed how taking the concealed consecutive relations among businesses and anticipated labels may enhance the outcomes, and this model accomplished the capable outcomes in under-sampling and oversampling.

Li et al. (2020) developed a deep representation learning method for detecting credit card scams, which offered the benefit of achieving better and consistent performance. This method comprises the particularly enhanced loss function, FCL, and DNN. To expand the intra-class density and interclass departure, full center loss (FCL) was capable of managing the deep representation learning technique from a selection of approaches. Competitive swarm optimization-Deep convolutional neural network (CSO-DCNN) was devised by Karthikeyan et al. (2023) to make a DCNN for identifying the abnormalities by using the proposed CSO. In case of fraud situations, supervised learning on previous records was unable to detect a specific accent. They suggested CSO-DCNN, known as an unsupervised learning technique, and customized ReLu by connecting the contributions and productions.

Ensemble-Based Methods

Karthik et al. (2022) established a Hybrid ensemble model of boosting and bagging group classifiers, and the model also used the prominent features of both approaches. Since the issue of data imbalance was addressed by a hybrid method, experiments using Brazilian bank data and University of California, San Diego-Fair Isaac Corporation (UCSD-FICO) data displayed durability. Xie et al. (2021) introduced a heterogeneous ensemble learning model based on data distribution (HELMDD) to resolve the issue of extremely imbalanced information circulation in CCFD. In this method, the resampling method based on majority class data distribution (RMDD) was developed in terms of the majority class, where it was classified into ordinary samples and boundary samples. It produced numerous balanced subgroups in terms of clustering, in which many base classifiers were trained. Thus, this method achieved a high recall rate for the majority class.

The champion-challenger framework was formulated by Kim et al. (2019) for the advancement procedure. It has significant class and rate imbalances, thus necessitating the use of accurate calculation measures. Additionally, these models were utilized in a practical fraud detection system to assess their effectiveness over a one-month period. Alhashmi et al. (2023) used a bank account fraud (BAF) dataset on which an ensemble method was employed, and performance was compared with other classifiers, namely Voting Classifier, Random Forest, Gradient Boosting, Logistic Regression, and Neural Networks, on different metrics such as accuracy, precision, recall, and F1-score. The suggested ensemble model performed better than other classifiers with an accuracy of 98%. The importance of precision-recall trade-offs in fraud detection was also showcased.

ML-Based Approaches

The learning algorithm was developed by Dal Pozzolo et al. (2017), which was essential for providing opinions throughout the learning problem and accepting precise statements. The suggested learning technique involves individually training a classifier on feedback and a classifier on delayed supervised samples, then relating to detecting warnings, which obviously places major importance on feedback. Afriyie et al. (2023) employed Logistic Regression, Decision Tree, and Random Forest approaches to categorize online credit card transactions as either fraudulent or legitimate. The dataset was balanced before creating the models using the under-sampling strategy to guarantee that the model did not only favor the majority class and prevent over-fitting the techniques to the data.

Alfaiz and Fati (2022) demonstrated a method called AllKNN-CatBoost, which pays on stratified K-fold cross-validation together with a real-life dataset of European cardholders for detecting credit card fraud. To find fraudulent transactions, the ML approaches were taken to the test in the first stage, and then they were chosen to be applied once more in the second stage. AdaBoost and Light Gradient Boosting Machine (LightGBM) are established by Malik

et al. (2022), in which several hybrid ML models were generated and inspected based on the combination of supervised ML approaches. It was exposed that the hybridization of some methods produced an important benefit over the most progressive methods.

Ghosh et al. (2022) revealed a Neural Aggregate Generator (NAG) method to extract the features based on neural networks that acquire feature aggregates. The NAG's network scheme thoroughly resembles the configuration of feature aggregates, in contrast to other programmed feature extraction methods. Furthermore, the NAG improved learnable aggregates over predictable ones by easy feature value matching and relative weights. The generative adversarial networks (GAN) technique was developed by Langevin et al. (2022), in which the influence of artificial information on the performance is reliant on basic customer distributions and the source of information. In order to increase training sets for fraud detection, it has the potential to increase model performance by accumulating small quantities of GAN-generated synthetic data.

Carcillo et al. (2021) devised supervised and unsupervised approaches for the application of a hybrid strategy that uses unsupervised outlier scores to increase a fraud detection classifier's feature set. Beyond its applicability, the datasets of credit card transactions and the effect of the invention lie in the execution and assessment of several granularity levels for the purpose of an outlier score. Attention mechanism and long short-term memory (LSTM) deep model were introduced by Benchaji et al. (2021) to relate the assets of several ML approaches, like a swarm intelligence-based approach, which was utilized to select the best division of relevant features. The uniform manifold approximation and projection (UMAP) approach was used to decrease dataset dimensionality, and SMOTE was employed to address the problem of imbalanced data. To overcome the issue of imbalanced data, the prediction efficacy during the identification of fraudulent transactions was enhanced.

Lin and Jiang (2021) developed an autoencoder-probabilistic random forest (AE-PRF) to reduce the data dimensionality and to remove data features. Additionally, it used RF with a probabilistic arrangement to make data appear fraudulent and offer a probability to that label. When the related probability influences a certain threshold, the AE-PRF reports the final classification as fraudulent. Data resampling approaches, such as SMOTE, were utilized to balance the quantities of legitimate and fraudulent transactions. Strelcenia and Prakoonwit (2023) introduced a method of K CGAN, which was used to compare and assess the performance of classifiers in characteristics between criminal and permitted transactions. It is also used to test the categorization outputs and to distinguish between fraudulent and legitimate transactions. For accessibility, recall, F1 score, recall, and accuracy precision are engaged.

Seera et al. (2021) produced an ML approach to improve the learning approaches. A Malaysian financial institution utilized the definite payment card database. In order to accurately assess the effectiveness of the recognized tactic, fraud detection was identified in other parts of the world, which would be useful to collect more real-world data from other

countries. Hidden Markov models (HMMs) were established by Lucas et al. (2020) for producing features based on HMMs that permit the incorporation of sequential knowledge in transactions as features. These HMM-based characteristics allow the Random Forest classifier to categorize the information using sequential data. HMMs agree to take in a wide range of sequential data due to their numerous perspective assets.

Fiore et al. (2019) devised a GAN to tackle the class imbalance issue while using supervised classification to find credit card fraud. A training set is utilized to create an augmented set, which has more instances of the minority class than the training set. A tailored GAN is used to create synthetic instances. The advised method was fundamentally reliant on labeled examples of fraudulent transactions. Alshutayri (2023) employed logistic regression for fraud transaction detection on movie ticket transactions done using credit cards on data collected from European cardholders. The dataset consisted of 284,807 transactions, with 492 fraud transactions. The accuracy of the suggested technique was reported as 99.88%.

A parenclitic network was demonstrated by Zanin et al. (2018) to show how data mining and complex networks are combined as corresponding tools in a synergistic manner to improve the classification rates obtained by classical data mining algorithms. To advance data mining methods, fraud instances were identified in credit card transactions. Carcillo, Dal Pozzolo, et al. (2018) revealed the SCAlable Real-time Fraud Finder (SCARFF) method to identify fraud in a short period of time mechanically. The scheme, progress, and testing of an open-source big data solution for actual fraud detection were done using a comfortable real-life data set, which establishes the framework's novel contribution. In order to give emphasis to the approach, it has been entirely open source and replicable using a synthetic dataset and Docker9 container.

Carcillo, Le Borgne, et al. (2018) developed an active learning system to analyze the accuracy of CCFD. Various approaches, including semi-supervised learning, exploratory active learning, combining functions, and traditional active learning, are applied to a real-life dataset. The two-dimensional cognitive therapy of complications, such as non-separability, the issue in fraud detection, is delivered through various tactics, and it is similar to visualization. Artificial Immune Recognition System (AIRS) algorithm within artificial immune system (AIS) was devised by Halvaiee and Akbari (2014) to identify credit card fraud, and a new technique called AIS-based Fraud Detection Model (AFDM) was established for this purpose. The AIRS method has established many advancements in the technique by improving accuracy while lowering system training time and costs. An exclusive method in AFDM was utilized to regulate the antigens' empathy for one another.

Zhang et al. (2022) established a one-class support vector machine (OCSVM) and AdaBoost, in which SMOTE has resolved the imbalanced class problem with excessive performance, and their categorization capability needs to be developed in various practical circumstances. To precisely identify fraudulent activities, it utilized anomaly detection

on imbalanced data and IForest with kernel principal component analysis. OCSVM and AdaBoost approaches were active in sensing outliers, which significantly improved detection effectiveness and accuracy. Alshawi (2023) proposed an approach for detecting fraud that could deal with tiny, unbalanced datasets. He trained Logistic regression, Decision Trees, Naïve Bayes, AdaBoost, Random Forest, and XGBoost on synthetic data generated using GAN. He reported that, except for naïve Bayes, all other models had an accuracy of 95% or more.

LSTM and gated recurrent unit (GRU) were demonstrated by Mienye and Sun (2023), which serve as the source learners for a robust deep-learning policy, which also included a multilayer perceptron (MLP) functioning as the meta-learner. To balance the stability of the class distribution in the dataset, the hybrid synthetic minority oversampling model-edited nearest neighbor (SMOTE-ENN) technique is used. Du et al. (2023) introduced an autoencoder and decision tree-based classifier with Light Gradient Boosting (AED-LGB) approach, and bank credit card fraud was addressed using the AED-LGB. This method first customizes an auto-encoder to remove the features from the input, after which it feeds them into the LightGBM approach for calculation and organization. The algorithm then recognizes information that goes beyond the threshold as fake information. AED-LGB approach performance was estimated by using an anonymized database from a bank.

Hafez et al. (2025) offered a systematic review of AI-enhanced techniques used in CCFD, focusing on recent advancements in ML, DL, and hybrid models, critically evaluating over 50 studies by comparing methodologies, feature engineering techniques, and performance outcomes across different datasets. Farabi et al. (2024) also conducted a comprehensive study focused on evaluating multiple ML algorithms for CCFD, aiming to identify models that offer optimal performance in terms of accuracy and fraud mitigation. After analysis of algorithms like decision trees, random forest, SVM, logistic regression, and neural networks on benchmark datasets, the authors concluded that ensemble models, particularly random forest and gradient boosting, demonstrated superior detection capabilities.

Optimization-Based Approaches

Prabhakaran and Nedunchelian (2023) formulated the technique, oppositional cat swarm optimization-based feature selection model with a deep learning model for CCFD (OCSODL-CCFD), to identify and categorize credit card fraud. The OCSODL-CCFD method includes a variety of developments, such as oppositional cat swarm optimization (OCSO)-based feature selection, preprocessing, chaotic Krill Herd algorithm (CKHA)-based hyper-parameter optimizer, and bidirectional gated recurrent unit (BiGRU) classifier. The OCSO models' design aids in decreasing computing complexity and improving classification outcomes. Group Search Firefly Algorithm was presented by Jovanovic et al. (2022) to tackle the problem of CCFD, and it recommends a hybrid ML and swarm meta-heuristic method.

Extreme learning machines, SVMs, and extreme gradient-boosting ML methods were adjusted using the newly upgraded firefly technique called the group search firefly approach.

Padhi et al. (2022) employed the Rock Hyrax Swarm Optimization Feature Selection (RHSOFS) method to progress credit card fraud transaction documentation methods. The feature selection (FS) method in terms of a metaheuristic approach called RHSOFS, which was stimulated by the normal behavior of rock hyrax swarms. From a high-dimensional dataset, a subgroup of the best applicable features is preferred using this method. Singh and Jain (2020) presented a cost-sensitive learning flower pollination metaheuristic algorithm (CSFPA) with the benefit of the correlation-based feature selection (CFS) model and flower pollination algorithm (FPA). The other method of cost-sensitive metaheuristic technique and cost-sensitive classifier was offered to ease the misclassification cost of credit card transactions from class imbalance data.

Hyper-Heuristic Evolutionary Algorithm (HHEA), an exclusive Bayesian network classifier (BNC) approach, was established by Sánchez et al. (2009) to address a practical issue of CCFD. A HHEA method, which advances unique solutions for categorizing datasets, originally produced the FraudBNC method, and this algorithm is common enough to resolve further classification problems.

SMOTE-Based Methods

SMOTE and Easy Ensemble were introduced by Dal Pozzolo et al. (2017) to address the fraud detection issue and recommend suitable performance measures for fraud detection tasks like average precision (AP), area under curve (AUC), and precision rank. In relation to the overall number of transactions, fraud is quite occasional. Additionally, the purpose of detection is to provide the investigators with the transactions that pose the most significant risk of fraud. Therefore, rating transactions according to their chance of fraud is more important. Rtayli and Enneya (2020) developed a hyperparameter optimization (HPO) approach using SMOTE to generate a hybrid algorithm for CCFD. The advised method has a great capability to distinguish fraudulent transactions. More precisely, the Recursive Feature Elimination (RFE) was utilized for indicating the most valuable predictive features, and the Grid Search cross-validation (CV) for SMOTE and HPO are used to resolve the imbalanced data problem, and are united to produce robustness.

TL-Based Methods

Fraud detection system (FDS) was introduced by Lebichot et al. (2021) to investigate the presentation of TL methods in transaction-based fraud detection systems. It is very reasonable from a business standpoint, and the improvement of techniques to relate detection models learned in combined markets to fresh ones was still a primary goal for transactional organizations.

Other Methods

Habibpour et al. (2023) employed an uncertainty quantification (UQ) approach in which the grade of uncertainty associated with generating the predictions was measured using three deep UQ methods, which resulted in a responsible categorization. In order to advance fraud prevention, decision-makers might get supplementary insights by enumerating the uncertainty of predictable fraudulent transactions. To evaluate the prediction uncertainty estimations, various performance measures and the UQ confusion matrix are also engaged. Information utilization method (INUM) was devised by Han et al. (2021) to support four newly developed MMEAs to do a better job of handling multimodal multi-objective issues. Its inventive technique is to arbitrarily choose multiple D-vectors from all D-vectors in the choice space, to categorize them, to select the top and bottom D-vectors, to make a data vector by deducting the top from the bottom D-vectors, and finally to produce offspring by accumulating data for all solutions to produce the best results.

Prusti et al. (2021) demonstrated a graph database model in response to the graph database pattern, and a fraud detection system was offered. Some transaction database features are united with graph features that are recovered using the Neo4j tool. To precisely recognize fraudulent transactions, five supervised and two unsupervised ML approaches are applied. For detecting fraudulent transactions, the categorization methods are also utilized to calculate the features. Tingfei et al. (2020) developed a variational automatic coding (VAE) to address the issue, a VAE-based oversampling technique that syndicates traditional DL methods. In an unbalanced dataset, the VAE approach is used to generate a large number of diverse instances from minority groups, which are subsequently used to train the classification network. Additionally, it outperforms existing oversampling systems based on GAN methods.

Gianini et al. (2020) established a Game Theory-based methodology that assigns a normalized score to every individual rule, evaluating the rule's contribution to the pool's overall performance. By using the Shapley value (SV), a power index produced under Coalitional Game Theory, it was to extend the efficacy of association. This score has two major uses: to maintain or eliminate a rule from the pool during the periodic rule evaluation process and to select the best k rules. Weighted extreme learning machine (WELM) was developed by Zhu et al. (2020) to equate the performance of many intelligent optimization practices on an unbalanced classification problem while enhancing the WELM. The WELM with a probability-based mutation-enabled dandelion approach performs WELM with a bat algorithm, a dandelion algorithm, particle swarm optimization, and a genetic algorithm. The advised method is also used to detect credit card fraud and has excellent detection performance.

Darwish (2020) produced a two-level CCFD method to increase classification accuracy and accelerate detection convergence. A two-level artificial bee colony algorithm (ABC)

and k-means approaches were utilized to recognize credit card fraud from extremely unbalanced datasets. To deal with the k-means classifier's inability and to identify the precise cluster, cluster ABC was used.

Ebiaredoh-Mienye et al. (2021) presented a stacked sparse autoencoder approach integrated with an artificial neural network (ANN) to enhance the prediction accuracy of credit card fraud on high-dimensional and imbalanced data by employing feature learning techniques that automatically extract relevant patterns. Their proposed approach outperformed traditional neural networks and other ML classifiers in prediction performance while effectively reducing noise and dimensionality. Esenogho et al. (2022) integrated a neural network-based ensemble model and feature engineering techniques to improve the detection of credit card fraud, especially on imbalanced datasets. And they reported superior performance in fraud detection accuracy, F1-score, and false positive reduction compared to standalone models.

Table 1 presents a comparative analysis of various techniques reviewed in this paper on various parameters, like techniques employed, datasets used, and metrics used for evaluation.

A consumer incentive system was introduced by Wang et al. (2019) to end fraudulent credit card transactions. The two normally employed tactics are to take no preventative measures and to employ the ML detection method for all transactions. It also includes contribution motivations to customers and demanding inferior verification for every transaction, and the difficulties associated with fraudulent credit card transactions are captured by the required considerations. Somasundaram and Reddy (2019) developed a transaction window bagging (TWB) approach, which is based on incremental learning and challenges the proficient management of concept drifts caused by covariate drift

Table 1
Comparative analysis

Authors	Year	Proposed method	Dataset used	Evaluation metrics	Category
Carcillo et al.	2021	Supervised and unsupervised techniques	CCRD dataset	Precision, AUC-PR	ML
Benchaji et al.	2021	Attention mechanism and an LSTM deep model	Credit card fraud dataset	Accuracy, precision, recall	ML
Xie and Li	2021	HELMDD	Credit card transaction dataset	Recall, G-mean, AUC	Ensemble
Alharbi et al.	2022	Text2IMG conversion technique	Kaggle dataset	Accuracy, sensitivity, specificity, F1 score	DL
Alfaiz and Fati	2022	AllKNN-CatBoost	CCRD dataset	AUC, accuracy, recall, precision, F1 score	ML

Table 1 *(continue)*

Authors	Year	Proposed method	Dataset used	Evaluation metrics	Category
Malik et al.	2022	AdaBoost, LightGBM	IEEE-CIS fraud detection	ROC, TPR, precision, F-measure, TNR, Type-I error, Type-II error	ML
Jovanovic et al.	2022	Group Search Firefly Algorithm	CCRD	Accuracy, precision, recall, F1 score	Optimization
Forough and Momtazi	2022	DNN, PGM	CCRD	Precision, recall, F1 score, AUC-ROC, PR-AUC	DL
Carneiro et al.	2022	VCCA	Credit card transactions fraud detection dataset	F1 score, AUC, PRC	Clustering
Padhi et al.	2022	RHSOFS	Credit card fraud dataset	Accuracy, recall, precision, F1 score, MCC, specificity	Optimization
Zhang et al.	2022	OCSVM and AdaBoost	Credit card fraud dataset	Accuracy, precision, recall, F1 score	ML
Habibpour et al.	2023	UQ techniques	IEEE-CIS fraud detection	Accuracy, sensitivity, specificity, precision	Others
Mienye and Sun	2023	LSTM and GRU	Credit card fraud detection	Sensitivity, specificity, AUC	ML
Du et al.	2023	AED-LGB algorithm	Credit card transaction dataset	Accuracy, MCC, TPR, TN	ML
Prabhakaran and Nedunchelian	2023	OCSODL-CCFD	Credit card dataset	Accuracy, F1 score, MCC	Optimization
Karthikeyan et al.	2023	CSO-DCNN	Insurance fraud dataset	Accuracy, MAE, MSE	DL, optimization
Ebiaredoh-Mienye et al.	2021	Stacked sparse autoencoder + ANN	Credit card default dataset (likely a real-world/bank dataset)	Accuracy, precision, recall, F1 score	ML
Esenogho et al.	2022	Neural network-based ensemble model	CCRD dataset	Accuracy, F1 score, false positive rate	ML

Note. CCRD = Credit card fraud detection; ML = Machine learning; LSTM = Long short-term memory; HELMDD = Heterogeneous ensemble learning model based on data distribution; G-mean = Geometric mean; AUC = Area under curve; DL = Deep learning; AllKNN = All-k-nearest neighbors; LightGBM = Light Gradient Boosting Machine; IEEE-CIS = Institute of Electrical and Electronics Engineers – Computational Intelligence Society; ROC = Receiver operating characteristic; TPR = True positive rate; TNR = True negative rate; DNN = Deep neural network; PGM = Probabilistic graphical model; AUC-ROC = Area under the curve – Receiver operating characteristic; PR-AUC = Precision-recall area under the curve; VCCA = Value clustering for categorical attributes; PRC = Precision-recall curve; RHSOFS = Rock Hyrax Swarm Optimization Feature Selection; MCC = Matthews correlation coefficient; OCSVM = One-class support vector machine; UQ = Uncertainty quantification; GRU = Gated recurrent unit; AED-LGB = Autoencoder and decision tree-based classifier with Light Gradient Boosting; TN = True negative; OCSODL-CCFD = Oppositional cat swarm optimization deep learning for credit card fraud detection; CSO-DCNN = Competitive swarm optimization-Deep convolutional neural network; MAE = Mean absolute error; MSE = Mean squared error; ANN = Artificial neural network

and class drift. Their approach can also handle noisy and unbalanced data that creates extremely accurate predictions. To decrease the training period and offer predictions that are impervious to data imbalances, balanced data selection kept the lowest imbalance ratios.

Jiang et al. (2018) devised a fraud detection method to form a new behavioral profile of a cardholder that can be drawn on the forms of behavior from similar cardholders. To address the parameters' capacity and to respond quickly, cardholders' transactional behaviors are used. The efficiency and efficacy of the technique are confirmed by experimental findings. Advanced Transaction Exploration (APATE) was presented by Van Vlasselaer et al. (2015) for detecting fraudulent credit card transactions made at internet dealers. This method syndicated two types of features, namely intrinsic features and network-based features. The intrinsic features were a result of the characteristics of incoming transactions and customer history. Then, network-based features are derived by leveraging the network of credit card holders and merchants.

Seeja and Zareapoor (2014) developed Fraud Miner, a CCFD model designed to detect fraud in highly complex and unknown credit card transaction datasets, thereby identifying both lawful and fraudulent transaction configurations. Each client has frequent item set mining, which resolves the class imbalance problem. It was also utilized to determine if the configurations are fraudulent or legal and to make a judgment in line with the result.

RESEARCH GAPS AND ISSUES

The investigation difficulties encountered by clustering are as follows: The CBM method failed to focus on online transactions. Moreover, it was challenging to develop a new model and to create a distinct method for card-present and internet transactions. The SBS technique does not attain optimum and best outcomes, and thus, it was not easy to investigate in terms of improving the introduced approach.

The investigation challenges tackled by DL methods are revealed below: The goal of the text2IMG-based classification method is to increase the effectiveness of the method by the application of added portions. Moreover, it was stimulating to enhance prediction proficiency and to remove redundant data from transactions. The CSO-DCNN technique does not take any effort, and it was a challenge to incorporate further database, which covers statistically delicate features, and in executing ensemble attractive methods.

The experimentation problems conflicting with ML approaches are given below: The learning algorithm was unsuccessful in exchanging the linear accumulation of subsequent prospects, and it was difficult to improve the attentive precision by executing the learning-to-rank technique. AdaBoost and LightGBM techniques did not focus on the disadvantages of misplaced values. Furthermore, various approaches can be established through feature extraction and selection, allowing for the regulation of their influence on estimated accuracy.

The GAN approach was challenging to observe substitute variance in privacy explanations and allowances, which also includes perceiving the problem in privacy with the related information. Attention mechanism and LSTM deep method aim to train about CCFD approaches, in which it was difficult to process the series, which depends on transformers and attention without any recurrent networks. The AE-PRF model failed to advance its performance by utilizing the hyperparameters of the random forest (RF) and autoencoder (AE) approaches.

Moreover, there is a problem in applying the introduced technique to various requests for assessing its process. The devised model HMM did not synchronize the predictions of HMM features and LSTM, which is also a challenge to identify the scams in the face-to-face transaction. In the SCARFF technique, the challenge is to focus on analyzing the prevailing result for the business partner, assessing its effectiveness, and evaluating its robustness.

The analysis difficulties addressed by optimization are established as follows: The CSFPA did not demonstrate analysis on a larger number of datasets. Moreover, it was still a challenge to determine the time cost, and the performance of the devised technique also needs to be developed through subsequent features of unit tactics.

The difficulties encountered by the other techniques are also demonstrated below: the INUM approach aims to improve their performance by involving the challenge in contributing to real-life optimization issues. The recall rate is enhanced in the approach of VAE. It was also challenging to improve the metrics of F-score and precision, while maintaining the performance of recall equivalent to that of other techniques.

COMPARATIVE ANALYSIS

This section illuminates a discussion and analysis of CCFD based on various criteria. For this analysis, various research papers are compared on various approaches, such as characterized techniques, datasets, publication year, and performance metrics.

Analysis Based on Techniques

In this part, several CCFD techniques are compared. Figure 2 describes the distribution of various CCFD methods used in this survey. It is evident that the maximum papers surveyed used ML-based approaches, followed by optimization-related techniques. Other papers used

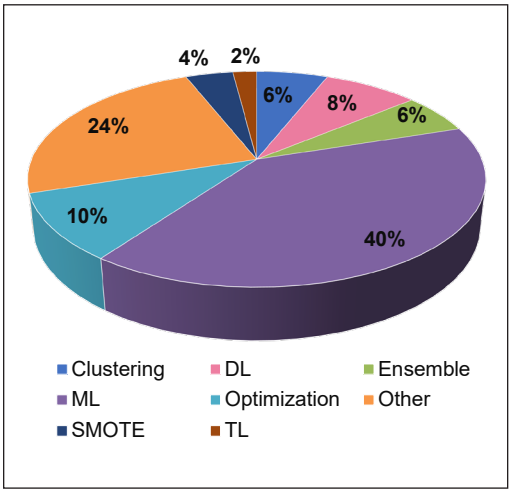

Figure 2. Category analysis based on various techniques
Note. DL = Deep learning; SMOTE = Synthetic minority oversampling technique; ML = Machine learning; TL = Transfer learning

clustering-based, DL, ensemble approaches, SMOTE techniques, and TL models for the detection of fraud.

Analysis Based on the Tools Used

In this section, the tools used by different researchers are compared. Table 2 shows the tools and software used for detecting credit card fraud. The implementation tools used by researchers are Apache, Python, Java, and MATLAB. Python and MATLAB were utilized by most of the researchers included in this survey. Apache and Java were utilized in one paper, respectively.

Table 2
Analysis based on tools

Tools	Apache	Python	Java	MATLAB
No. of publications	1	15	1	6

Analysis Based on Publication Year

Various CCFD methods were studied in this analysis. Table 3 illustrates the year of publication and the number of papers published. Most of the papers studied have been published in the years 2022 and 2023.

Table 3
Analysis based on the publication year

Year	2014	2015	2017	2018	2019	2020	2021	2022	2023
No. of publications	3	1	2	5	4	8	8	11	11

Analysis Based on the Dataset

In this section, the analysis is done on the datasets used by the papers included in the review. The datasets utilized in this analysis are BankSim dataset, Brazilian bank dataset, card-specific transaction datasets, credit card dataset, credit card fraud dataset, CCFD, credit card transaction data set, e-commerce transactions dataset, Institute of Electrical and Electronics Engineers-Computational Intelligence Society (IEEE-CIS) fraud detection, insurance fraud dataset, Kaggle dataset, PagSeguro dataset, real-world credit card transactions dataset, real-world dataset, Resilient Distributed Dataset (RDD), synthetic testing dataset, and UCSD-FICO dataset, to name a few. Figure 3 describes the datasets applied for the analysis. Here, the CCFD dataset is used in nine research papers, the credit card dataset is utilized in six papers, and a real-world dataset is used in five papers. Four papers used the credit card transactions dataset, and in three papers, the

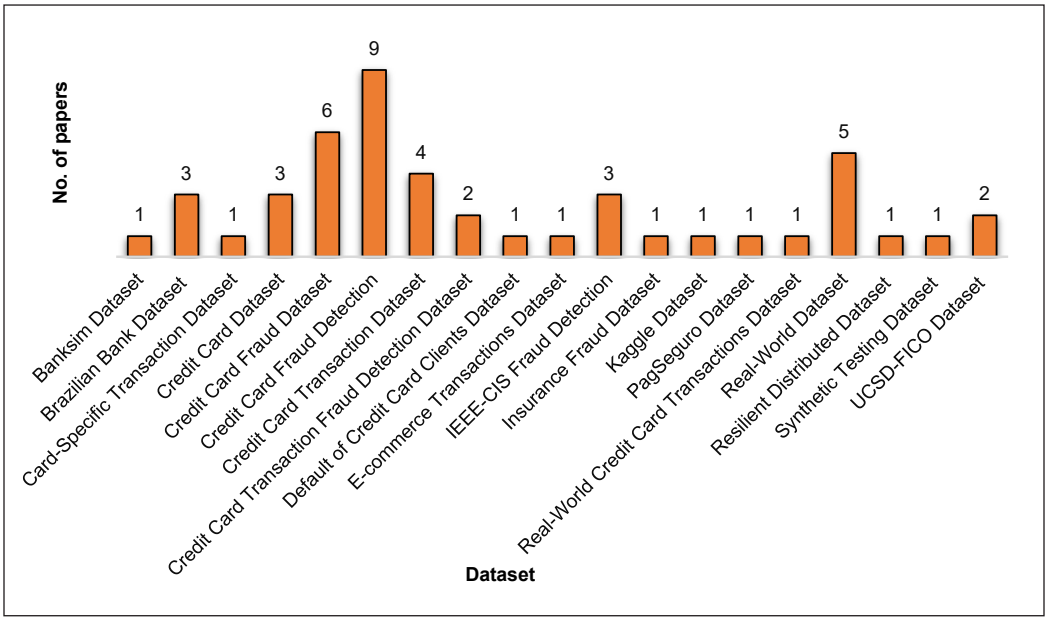

Figure 3. Analysis based on datasets
Note. IEEE-CIS = Institute of Electrical and Electronics Engineers-Computational Intelligence Society; UCSD-FICO = University of California, San Diego-Fair Isaac Corporation

Brazilian bank dataset, the credit card dataset, and the IEEE-CIS fraud detection dataset were engaged. The datasets UCSD-FICO and credit card transactions for fraud detection are used by two papers. One paper also utilizes datasets such as synthetic testing, RDD, real-world credit card transactions, PagSeguro, Kaggle, Insurance Fraud, e-commerce transactions, default of credit card clients, BankSim, and card-specific transaction datasets. The datasets used have many attributes; some are used in their original form, while others are used after feature extraction. Analysis done on these datasets can give us insight into what features generally distinguish fraud transactions from normal transactions. ML and DL algorithms were able to perform efficiently on real-world datasets as well as datasets available online. The research done on different datasets can be used by banking and credit card companies to identify fraudulent transactions and prevent fraud, leading to a decrease in losses due to fraud.

Analysis Based on Performance Metrics

In this analysis section, the evaluation metrics applied in the research papers are explained. The performance metrics utilized in this dataset are accuracy, precision, recall, F measure, specificity, AUC, sensitivity, Matthew's correlation coefficient (MCC), true positive rate (TPR), true negative rate (TNR), false positive rate (FPR), cost, Type II error, Type I error, receiver operating characteristic- area under curve (ROC-AUC score), receiver

operating characteristic (ROC), root mean quadratic error (RMQE), precision-recall curve (PRC), precision at k (Pk), negative predictive value (NPV), mean square error (MSE), misclassification rate, absolute mean error (AME), Kolmogorov–Smirnov (K-S statistics), hit rate, G-mean, Fraud detection rate, false negative rate (FNR), false alarm rate, fall-out, error rate, detection rate, process capability index (CPk), benefit-cost ratio (BCR), average cost, area under ROC curve (AUROC), area under the precision-recall (AUPR measure), area under the receiver operating characteristic (AUC-ROC), area under the curve of precision-recall (AUCPR), alert rate, and AP. Here, accuracy was used in 26 papers, precision in 25 papers, F-measure in 19 papers, recall in 21 papers, AUC in 11 papers, specificity in 12 papers, TPR and FPR in six papers, TNR in five papers, AUC-ROC, AUC-PR, BCR, and G-mean in two papers and finally, AP, alert rate, AUPR measure, AUROC, average cost, CPk, detection rate, error rate, fall-out, false alarm rate, FNR, fraud detection rate, hit rate, K-S statistics, MAE, misclassification rate, MSE, NPV, Pk, PRC, RMQE, ROC, ROC-AUC score, Type I and II errors are identified in only one paper, respectively.

Figure 4 illuminates the metrics-based analysis. As seen from the graph, accuracy is most frequently used, followed by precision, recall, and F-measure. Accuracy provides an overall evaluation of the method employed, including both fraudulent and normal transactions. Precision, on the other hand, emphasizes measuring the proportion of true positive predictions among all positive predictions. Recall measures the proportion of true positive predictions among all actual positive instances in the dataset. Recall is important in detecting fraud. High recall indicates fewer fraud transactions remain unidentified.

Analysis Based on Values of Accuracy

The range of accuracy and the number of research papers are given in Table 4, which indicates that accuracy ranges between the values of 0-80, 81-85, 86-99, and above 99%, respectively. Here, the accuracy between 0-80% lies in two papers. Next, between the values of 81-85%, two papers were selected. From 16 papers, the accuracy has a value between 86-99% and six research papers reached an accuracy range of above 99%.

Table 4
Analysis based on accuracy

Accuracy range (%)	Number of research papers
0-80	2
81-85	2
86-99	16
Above 99	6

CONCLUSION

This review aims to study past work in the field of CCFD. The survey focused on techniques employing clustering-, ML-, optimization-, SMOTE-, TL-, ensemble, and DL-based methods, respectively. Furthermore, the challenges in the literature are considered and identified from past research. Class imbalance is found in most of the CCFD datasets. Some

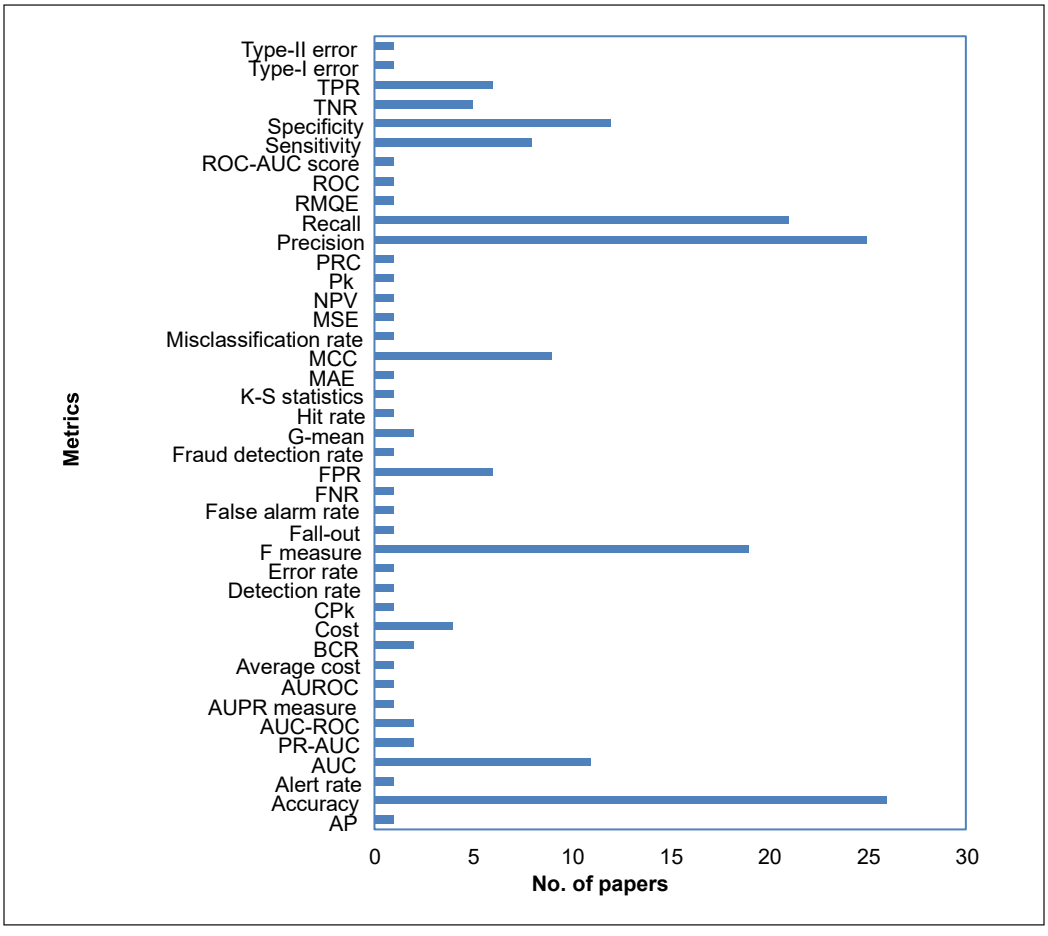

Figure 4. Analysis based on performance metrics

Note. TPR = True positive rate; TNR = True negative rate; ROC-AUC = Receiver operating characteristic-area under the curve; ROC = Receiver operating characteristic; RMQE = Root mean quadratic error; PRC = Precision-recall curve; Pk = Precision at k; NPV = Negative predictive value; MSE = Mean squared error; MCC = Matthews correlation coefficient; MAE = Mean absolute error; K-S statistics = Kolmogorov-Smirnov statistics; G-mean = Geometric mean ; FPR = False positive rate; FNR = False negative Rate; CPk = Process capability index; BCR = Balanced classification rate; AUROC = Area under the receiver operating characteristic curve; AUPR = Area under the precision-recall; AUC-ROC = Area under the curve–Receiver operating characteristic; PR-AUC = Precision-recall area under the curve; AUC = Area under curve; AP = Average precision

techniques that have been used for reducing the class imbalance problem are also discussed. Moreover, we have tried to identify the research gaps in the techniques analyzed. Different techniques are analyzed on various parameters. The analysis is conducted on the tools used for analysis, the datasets employed, the year of publication of papers, performance metrics, and other relevant factors. In this survey, it was discovered that Python was used more frequently by the researchers for analysis, followed by MATLAB. To assess performance,

accuracy was employed. The database used for this analysis was taken from online sources and some real-world datasets. In the future, research can be conducted to address the class imbalance problem present in CCFD datasets, and feature extraction techniques can be employed to reduce the processing time. The research should aim to enhance accuracy and speed in CCFD, enabling banks and other organizations to benefit from these techniques.

ACKNOWLEDGEMENTS

The authors would like to thank Guru Jambheshwar University of Science and Technology, Hisar, Haryana, India for their academic support throughout the completion of this research.

REFERENCES

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*, *6*, 100163. https://doi.org/10.1016/j.dajour.2023.100163

Ahmad, H., Kasasbeh, B., Aldabaybah, B., & Rawashdeh, E. (2023). Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS). *International Journal of Information Technology*, *15*, 325–333. https://doi.org/10.1007/s41870-022-00987-w

Alfaiz, N. S., & Fati, S. M. (2022). Enhanced credit card fraud detection model using machine learning. *Electronics*, *11*(4), 662. https://doi.org/10.3390/electronics11040662

Alharbi, A., Alshammari, M., Okon, O. D., Alabrah, A., Rauf, H. T., Alyami, H., & Meraj, T. (2022). A novel text2IMG mechanism of credit card fraud detection: A deep learning approach. *Electronics*, *11*(5), 756. https://doi.org/10.3390/electronics11050756

Alhashmi, A. A., Alashjaee, A. M., Darem, A. A., Alanazi, A. F., & Effghi, R. (2023). An ensemble-based fraud detection model for financial transaction cyber threat classification and countermeasures. *Engineering, Technology and Applied Science Research*, *13*(6), 12433–12439.

Alshawi, B. (2023). Utilizing GANs for credit card fraud detection: A comparison of supervised learning algorithms. *Engineering, Technology and Applied Science Research*, *13*(6), 12264–12270.

Alshutayri, A. (2023). Fraud prediction in movie theater credit card transactions using machine learning. *Engineering, Technology and Applied Science Research*, *13*(3), 10941-10945.

Bahnsen, A. C., Aouada, D., & Ottersten, B. (2015). Example-dependent cost-sensitive decision trees. *Expert Systems with Applications*, *42*(19), 6609–6619. https://doi.org/10.1016/j.eswa.2015.04.042

Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *Journal of Big Data*, *8*, 151. https://doi.org/10.1186/s40537-021-00541-8

Carcillo, F., Dal Pozzolo, A., Le Borgne, Y.-A., Caelen, O., Mazzer, Y., & Bontempi, G. (2018). *SCARFF*: A scalable framework for streaming credit card fraud detection with Spark. *Information Fusion*, *41*, 182–194. https://doi.org/10.1016/j.inffus.2017.09.005

Carcillo, F., Le Borgne, Y.-A., Caelen, O., & Bontempi, G. (2018). Streaming active learning strategies for real-life credit card fraud detection: Assessment and visualization. *International Journal of Data Science and Analytics*, *5*, 285–300. https://doi.org/10.1007/s41060-018-0116-z

Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences*, *557*, 317–331. https://doi.org/10.1016/j.ins.2019.05.042

Carneiro, E. M., Forster, C. H. Q., Mialaret, L. F. S., Dias, L. A. V., & da Cunha, A. M. (2022). High-cardinality categorical attributes and credit card fraud detection. *Mathematics*, *10*(20), 3808. https://doi.org/10.3390/math10203808

Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2017). Credit card fraud detection: A realistic modeling and a novel learning strategy. *IEEE Transactions on Neural Networks and Learning Systems*, *29*(8), 3784–3797. https://doi.org/10.1109/TNNLS.2017.2736643

Dal Pozzolo, A., Caelen, O., Le Borgne, Y.-A., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications*, *41*(10), 4915–4928. https://doi.org/10.1016/j.eswa.2014.02.026

Dal Pozzolo, A., Johnson, R., Caelen, O., Waterschoot, S., Chawla, N. V., & Bontempi, G. (2014). Using HDDT to avoid instances propagation in unbalanced and evolving data streams. In *International Joint Conference on Neural Networks* (pp. 588–594). IEEE. https://doi.org/10.1109/IJCNN.2014.6889638

Darwish, S. M. (2020). An intelligent credit card fraud detection approach based on semantic fusion of two classifiers. *Soft Computing*, *24*, 1243–1253. https://doi.org/10.1007/s00500-019-03958-9

Du, H., Lv, L., Guo, A., & Wang, H. (2023). AutoEncoder and LightGBM for credit card fraud detection problems. *Symmetry*, *15*(4), 870. https://doi.org/10.3390/sym15040870

Ebiaredoh-Mienye, S. A., Esenogho, E., & Swart, T. G. (2020). Integrating enhanced sparse autoencoder-based artificial neural network technique and Softmax regression for medical diagnosis. *Electronics*, *9*(11), 1963. https://doi.org/10.3390/electronics9111963

Ebiaredoh-Mienye, S. A., Esenogho, E., & Swart, T. G. (2021). Artificial neural network technique for improving prediction of credit card default: A stacked sparse autoencoder approach. International *Journal of Electrical and Computer Engineering*, *11*(5), 4392–4402. http://doi.org/10.11591/ijece.v11i5.pp4392-4402

Ebiaredoh-Mienye, S. A., Swart, T. G., Esenogho, E., & Mienye, I. D. (2022). A machine learning method with filter-based feature selection for improved prediction of chronic kidney disease. *Bioengineering*, *9*(8), 350. https://doi.org/10.3390/bioengineering9080350

Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A neural network ensemble with feature engineering for improved credit card fraud detection. *IEEE Access*, *10*, 16400–16407. https://doi.org/10.1109/ACCESS.2022.3148298

Farabi, S. F., Prabha, M., Alam, M., Hossan, M. Z., Arif, M., Islam, M. R., Uddin, A., Bhuiyan, M., & Biswas, M. Z. A. (2024). Enhancing credit card fraud detection: A comprehensive study of machine learning algorithms and performance evaluation. *Journal of Business and Management Studies*, *6*(3), 252–259. https://doi.org/10.32996/jbms.2024.6.13.21

Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences*, *479*, 448–455. https://doi.org/10.1016/j.ins.2017.12.030

Forough, J., & Momtazi, S. (2022). Sequential credit card fraud detection: A joint deep neural network and probabilistic graphical model approach. *Expert Systems*, *39*(1), e12795. https://doi.org/10.1111/exsy.12795

Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., & Bouchachia, A. (2014). A survey on concept drift adaptation. *ACM Computing Surveys*, *46*(4), 1–37. https://doi.org/10.1145/2523813

Ghosh, K. D., Jurgovsky, J., Siblini, W., & Granitzer, M. (2022). NAG: Neural feature aggregation framework for credit card fraud detection. *Knowledge and Information Systems*, *64*, 831–858. https://doi.org/10.1007/s10115-022-01653-0

Gianini, G., Fossi, L. G., Mio, C., Caelen, O., Brunie, L., & Damiani, E. (2020). Managing a pool of rules for credit card fraud detection by a game theory based approach. *Future Generation Computer Systems*, *102*, 549–561. https://doi.org/10.1016/j.future.2019.08.028

Habibpour, M., Gharoun, H., Mehdipour, M., Tajally, A., Asgharnezhad, H., Shamsi, A., Khosravi, A., & Nahavandi, S. (2023). Uncertainty-aware credit card fraud detection using deep learning. *Engineering Applications of Artificial Intelligence*, *123*(Part A), 106248. https://doi.org/10.1016/j.engappai.2023.106248

Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, *12*, 6. https://doi.org/10.1186/s40537-024-01048-8

Halvaiee, N. S., & Akbari, M. K. (2014). A novel model for credit card fraud detection using artificial immune systems. *Applied Soft Computing*, *24*, 40–49. https://doi.org/10.1016/j.asoc.2014.06.042

Han, S., Zhu, K., Zhou, M., & Cai, X. (2021). Information-utilization-method-assisted multimodal multiobjective optimization and application to credit card fraud detection. *IEEE Transactions on Computational Social Systems*, *8*(4), 856–869. https://doi.org/10.1109/TCSS.2021.3061439

Jain, Y., Tiwari, N., Dubey, S., & Jain, S. (2019). A comparative analysis of various credit card fraud detection techniques. *International Journal of Recent Technology and Engineering*, *7*(5S2), 402–407.

Jiang, C., Song, J., Liu, G., Zheng, L., & Luan, W. (2018). Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism. *IEEE Internet of Things Journal*, *5*(5), 3637–3647. https://doi.org/10.1109/JIOT.2018.2816007

Jovanovic, D., Antonijevic, M., Stankovic, M., Zivkovic, M., Tanaskovic, M., & Bacanin, N. (2022). Tuning machine learning models using a group search firefly algorithm for credit card fraud detection. *Mathematics*, *10*(13), 2272. https://doi.org/10.3390/math10132272

Karthik, V. S. S., Mishra, A., & Reddy, U. S. (2022). Credit card fraud detection by modeling behavior pattern using hybrid ensemble model. *Arabian Journal for Science and Engineering*, *47*, 1987–1997. https://doi.org/10.1007/s13369-021-06147-9

Karthikeyan, T., Govindarajan, M., & Vijayakumar, V. (2023). An effective fraud detection using competitive swarm optimization based deep neural network. *Measurement: Sensors*, *27*, 100793. https://doi.org/10.1016/j.measen.2023.100793

Kim, E., Lee, J., Shin, H., Yang, H., Cho, S., Nam, S. K., Song, Y.-K., Yoon, J.-A., & Kim, J.-I. (2019). Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning. *Expert Systems with Applications*, *128*, 214–224. https://doi.org/10.1016/j.eswa.2019.03.042

Kültür, Y., & Çağlayan, M. U. (2017). A novel cardholder behavior model for detecting credit card fraud. In *9th International Conference on Application of Information and Communication Technologies* (pp. 148–152). IEEE. https://doi.org/10.1109/ICAICT.2015.7338535

Langevin, A., Cody, T., Adams, S., & Beling, P. (2022). Generative adversarial networks for data augmentation and transfer in credit card fraud detection. *Journal of the Operational Research Society*, *73*(1), 153–180. https://doi.org/10.1080/01605682.2021.1880296

Lebichot, B., Verhelst, T., Le Borgne, Y.-A., He-Guelton, L., Oblé, F., & Bontempi, G. (2021). Transfer learning strategies for credit card fraud detection. *IEEE Access*, *9*, 114754–114766. https://doi.org/10.1109/ACCESS.2021.3104472

Li, Z., Liu, G., & Jiang, C. (2020). Deep representation learning with full center loss for credit card fraud detection. *IEEE Transactions on Computational Social Systems*, *7*(2), 569–579. https://doi.org/10.1109/TCSS.2020.2970805

Lin, T.-H., & Jiang, J.-R. (2021). Credit card fraud detection with auto-encoder and probabilistic random forest. *Mathematics*, *9*(21), 2683. https://doi.org/10.3390/math9212683

Lucas, Y., Portier, P.-E., Laporte, L., He-Guelton, L., Caelen, O., Granitzer, M., & Calabretto, S. (2020). Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. *Future Generation Computer Systems*, *102*, 393–402. https://doi.org/10.1016/j.future.2019.08.029

Mahmoudi, N., & Duman, E. (2015). Detecting credit card fraud by modified Fisher Discriminant Analysis. *Expert Systems with Applications*, *42*(5), 2510–2516. https://doi.org/10.1016/j.eswa.2014.10.037

Malik, E. F., Khaw, K. W., Belaton, B., Wong, W. P., & Chew, X. (2022). Credit card fraud detection using a new hybrid machine learning architecture. *Mathematics*, *10*(9), 1480. https://doi.org/10.3390/math10091480

Mienye, I. D., & Sun, Y. (2023). A deep learning ensemble with data resampling for credit card fraud detection. *IEEE Access*, *11*, 30628–30638. https://doi.org/10.1109/ACCESS.2023.3262020

Obaido, G., Ogbuokiri, B., Swart, T. G., Ayawei, N., Kasongo, S. M., Aruleba, K., Mienye. I. D., Arubela, I., Chukwu, W., Osaye, F., Egbelowo, O. F., Simphiwe, S., & Esenogho, E. (2022). An interpretable machine learning approach for hepatitis B diagnosis. *Applied Sciences*, *12*(21), 11127. https://doi.org/10.3390/app122111127

Padhi, B. K., Chakravarty, S., Naik, B., Pattanayak, R. M., & Das, H. (2022). RHSOFS: Feature selection using the rock hyrax swarm optimization algorithm for credit card fraud detection system. *Sensors*, *22*(23), 9321. https://doi.org/10.3390/s22239321

Prabhakaran, N., & Nedunchelian, R. (2023). Oppositional cat swarm optimization-based feature selection approach for credit card fraud detection. *Computational Intelligence and Neuroscience*, *2023*, 2693022. https://doi.org/10.1155/2023/2693022

Prusti, D., Das, D., & Rath, S. K. (2021). Credit card fraud detection technique by applying graph database model. *Arabian Journal for Science and Engineering*, *46*, 1–20. https://doi.org/10.1007/s13369-021-05682-9

Rtayli, N., & Enneya, N. (2020). Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization. *Journal of Information Security and Applications*, *55*, 102596. https://doi.org/10.1016/j.jisa.2020.102596

Sánchez, D., Vila, M. A., Cerda, L., & Serrano, J. M. (2009). Association rules applied to credit card fraud detection. *Expert Systems with Applications*, *36*(2), 3630–3640. https://doi.org/10.1016/j.eswa.2008.02.001

Seeja, K. R., & Zareapoor, M. (2014). FraudMiner: A novel credit card fraud detection model based on frequent itemset mining. *The Scientific World Journal*, *2014*, 252797. https://doi.org/10.1155/2014/252797

Seera, M., Lim, C. P., Kumar, A., Dhamotharan, L., & Tan, K. H. (2021). An intelligent payment card fraud detection system. *Annals of Operations Research*, *334*, 445–467. https://doi.org/10.1007/s10479-021-04149-2

Singh, A., & Jain, A. (2020). Cost-sensitive metaheuristic technique for credit card fraud detection. *Journal of Information and Optimization Sciences*, *41*(6), 1319–1331. https://doi.org/10.1080/02522667.2020.1809090

Somasundaram, A., & Reddy, S. (2019). Parallel and incremental credit card fraud detection model to handle concept drift and data imbalance. *Neural Computing and Applications*, *31*, 3–14. https://doi.org/10.1007/s00521-018-3633-8

Strelcenia, E., & Prakoonwit, S. (2023). Improving classification performance in credit card fraud detection by using new data augmentation. *AI*, *4*(1), 172–198. https://doi.org/10.3390/ai4010008

Tingfei, H., Guangquan, C., & Kuihua, H. (2020). Using variational auto encoding in credit card fraud detection. *IEEE Access*, *8*, 149841–149853. https://doi.org/10.1109/ACCESS.2020.3015600

Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). *APATE*: A novel approach for automated credit card transaction fraud detection using network-based extensions. *Decision Support Systems*, *75*, 38-48. https://doi.org/10.1016/j.dss.2015.04.013

Wang, D., Chen, B., & Chen, J. (2019). Credit card fraud detection strategies with consumer incentives. *Omega*, *88*, 179–195. https://doi.org/10.1016/j.omega.2018.07.001

Xie, Y., Li, A., Gao, L., & Liu, Z. (2021). A heterogeneous ensemble learning model based on data distribution for credit card fraud detection. *Wireless Communications and Mobile Computing*, *2021*, 2531210. https://doi.org/10.1155/2021/2531210

Zanin, M., Romance, M., Moral, S., & Criado, R. (2018). Credit card fraud detection through parenclitic network analysis. *Complexity*, *2018*, 5764370. https://doi.org/10.1155/2018/5764370

Zhang, Y.-F., Lu, H.-L., Lin, H.-F., Qiao, X.-C., & Zheng, H. (2022). The optimized anomaly detection models based on an approach of dealing with imbalanced dataset for credit card fraud detection. *Mobile Information Systems*, *2022*, 8027903. https://doi.org/10.1155/2022/8027903

Zhu, H., Liu, G., Zhou, M., Xie, Y., Abusorrah, A., & Kang, Q. (2020). Optimizing weighted extreme learning machines for imbalanced classification and application to credit card fraud detection. *Neurocomputing*, *407*, 50–62. https://doi.org/10.1016/j.neucom.2020.04.078