A Comprehensive Review on Credit Card Fraud Detection: Addressing Data Imbalance and Advancements in Machine Learning Techniques

Deepika Tiwari, Meenakshi Nawal
Department of Computer Science & Engineering, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur – 302017(India)
Email: deepika.tiwari0044@gmail.com , Meenakshi.nawal.02@gmail.com
Received 07.10.2025 **received in revised form** 09.06.2025, **accepted** 14.12.2025
DOI: 10.47904/IJSKIT.15.2.2025.13-18

Abstract- The demand for precise, real-time fraud detection systems is growing in direct correlation with the proliferation of online purchases, since credit card fraud is still a major problem in the banking industry and poses significant dangers to both customers and businesses. This review paper explores various approaches and methodologies developed to detect fraudulent credit card activities, focusing on their applicability, effectiveness, and adaptability in dynamic transaction environments. The paper categorizes existing research based on learning paradigms and detection strategies, highlighting the importance of pattern recognition, anomaly detection, and behavioral analysis in combating fraud. The review concludes by identifying gaps in current research and proposing future directions, including the development of more adaptive, interpretable, and privacy-preserving fraud detection systems capable of operating efficiently in real-world, large-scale environments.
Keywords: Credit Card Fraud, Fraud Detection, Financial Security, Anomaly Detection, Machine Learning, Data Imbalance

1. INTRODUCTION

In this context, "fraud" means getting money or things through dishonest means. Crimes with dishonest, often nebulous, intents are the stuff of fraud. Of course, credit card fraud isn't the only kind that happens. To commit credit card fraud is to make a purchase using a credit card or other comparable payment method using money that has been stolen or obtained falsely. There has been a growing problem with credit card fraud in the sector. Because it is so challenging to detect credit card fraud using standard procedures, research into and implementation of models to do so has recently gained traction in both academic and corporate circles. Also, with the development of new technology, the function of fraud has seen a dramatic shift in the past few decades. Among the most pressing problems facing modern businesses is credit card fraud. The most basic definition of credit card fraud is "when someone else uses another person's credit card for personal use without the owner's or issuer's knowledge." There are a lot of systems/models, processes, and preventative measures that may be put in place to stop credit card fraud and financial hazards. [1] Massive quantities of credit card account transactions have been collected by banks and credit card issuers. Credit cards, which are plastic cards distributed to a large number of individuals, are one kind of payment. Because of their promise, customers are able to use their cards to buy stuff. Even while the number of Chinese citizens using credit cards has been steadily increasing, most customers still do not use them. Why? For the simple reason that cardholders lack faith in the payment system. The expansion of online shopping and banking services that protect client money The safety of credit card purchases depends on a reliable system that can identify fraudulent behavior. Analyzing the cardholder's present spending habits and purchase history is one possible way to reduce the occurrence of credit card fraud. When criminals circumvent fraud protection systems and begin fraudulent transactions, fraud detection systems step in to help. The global expansion of fraud and the massive amounts of money lost to it are both accompanied by advancements in information technology and better communication methods. The various forms of fraud have been defined and named by [2-3]. Many various types of credit card fraud exist, including online/electronic fraud (in which the cardholder is not physically present), application fraud, Never Received Issue (NRI), and simple theft. Finding a solution to the problem of credit card fraud is frequent yet extremely challenging. Since there is a restriction on the amount of data associated with financial transactions, such as the amount, acquirer number, date/time, and merchant address, among other things. Numerous fraud detection systems and models have been developed using various knowledge discovery techniques, including decision trees, neural networks, and case-based reasoning. A sufficient amount of both legitimate and fraudulent transactions is typically required for these methods to understand fraud tendencies. [4] As a whole, though, the percentage of fraudulent transactions relative to the bank's typical transactions is quite low.

Motivation

Financial fraud represents a significant global issue, incurring billions in losses while eroding consumer trust. Detection systems must evolve rapidly to identify increasingly sophisticated fraudulent patterns. However, the inherent imbalance in fraud datasets—where legitimate transactions vastly outnumber fraudulent ones—leads to machine learning models that poorly detect fraud. Traditional detection methods face challenges from data skewness, concept drift, and adversarial behaviors. Recent advances in machine learning, such as ensemble techniques and anomaly detection, show promise for improving fraud detection accuracy, yet the literature lacks cohesion across various sectors. A structured review is critical to address data imbalance issues and consolidate advancements in the field.

Contribution of the Study

This review makes several significant contributions to the field of credit card fraud detection by providing a comprehensive and structured analysis of how modern machine learning techniques address the persistent challenge of data imbalance. First, it synthesizes and evaluates a wide range of imbalance-handling strategies—from traditional resampling methods such as random oversampling, random under sampling, SMOTE, and ADASYN, to more advanced approaches including class-weight adjustment, cost-sensitive learning, anomaly detection, GAN-based synthetic data generation, and balanced ensemble algorithms. Second, the review integrates recent advancements in machine learning and deep learning models, including hybrid ML–DL architectures, generative models, unsupervised learning frameworks, and distributed learning systems, highlighting how these innovations enhance fraud detection performance in highly skewed datasets.

Types of Fraud

This article covers a wide range of fraud categories, including: bankruptcy fraud; application fraud; behavioral fraud; theft/counterfeit; telecommunications fraud; computer intrusions; and credit card fraud.

Embezzlement – A trusted individual misappropriates funds or assets given to them for personal use.

Money Laundering – Funds obtained illegally are processed through complex transactions to obscure their origin and “clean” them.

Identity Theft – Personal identity data (e.g. credit card or SSN) is stolen and used to commit financial fraud in the victim’s name.

Credit/Debit Card Fraud – Unauthorized purchases or withdrawals are made possible when criminals exploit stolen card details.

Financial Statement Fraud – A company manipulates its financials to misrepresent performance or stability.

Invoice Fraud – Fake or altered invoices are submitted to extract unauthorized payments.

Expense Fraud – Employees exaggerate or fabricate expense reports to get increased reimbursements.

Tax Fraud / Tax Evasion – Individuals or businesses falsify tax filings to underpaid liabilities or evade tax altogether.

Insurance Fraud – Includes false claims or fabricated incidents to claim insurance benefits.

Ponzi Scheme – Funds from newer investors, rather than actual profits, are used to provide returns to early investors.

Pyramid Scheme – Members make most of their money not from selling products or services directly but from recruiting new members.

Affinity Fraud – Scammers exploit trust within communities or shared associations to promote fraudulent investments.

[4] Forecasted instances of managerial fraud using a robust generalized response model. Model components include the "probit and logit" procedures. Credit cards and their many varieties are defined at the outset of this paper, which then moves on to discuss relevant research and potential methods and models for identifying legitimate and fraudulent purchases.

Computer Intrusion: Intrusion Is Defined As

An unauthorized attempt to gain access to or compromise a computer system, network, or digital asset is referred to as an intrusion in the context of computer security. This involves getting around security safeguards to access resources without authorization. Numerous malevolent actions, including data theft, system disruption, and damage, can be a part of intrusions. Here's a more thorough explanation:

Unauthorized Access: At its most basic, intrusion is the acquisition of access to a resource or system that the intruder is not permitted to use.

Putting Security at Risk:

Bypassing or evading security measures like firewalls, passwords, or access controls, this access is made possible.

Possibility of Damage: Once inside, an intruder may carry out a number of destructive tasks, such as denial of service attacks, system alteration, data theft, and other nefarious deeds.

Instances of Intrusion:

Hacking: A common form of intrusion where an attacker uses technical skills to bypass security measures.

Insider threats are people who have authorized access to a system but misuse it for nefarious ends.

Malware Infections: Unauthorized access and control of a system can be achieved using malicious software, such as Trojan horses or viruses.

Phishing attacks are dishonest attempts to fool people into disclosing private information that could be used to obtain illegal access.

Credit Card Fraud Detection

Issues with credit cards, both theoretical and practical, are discussed in this section.

Terms

- **Credit Card:** They can buy things online without actually having the cash on hand through the

use a credit card. The use of a credit card streamlines the process of automatically extending credit to consumers. Almost all credit cards now include a unique identifier that speeds up online purchases.

- **Fraud:** Any dishonesty perpetrated with the aim to deceive another person or entity for one's own benefit or harm is considered fraudulent. The concept of fraud is defined differently in different legal systems. In addition to being a violation of civil law, deceit is a criminal offense. Rigging people or businesses out of their money is a common objective of fraud.

Credit Card Fraud

The fraud rate is incredibly low despite the high volume of credit card transactions in the US. Ukraine has an alarming 19% fraud rate, second only to Indonesia's 18.3%; other high-risk countries facing the threat of credit card theft include Yugoslavia (17.8%), Malaysia (5.9%), and Turkey (9%). The factors that authorize users to make credit card transactions include the credit card number, signatures, the address of the cardholder, the expiration date, and so on. Credit card fraud is the unlawful use of a card or card information without the owner's knowledge, which constitutes a criminal deceit. The public pays less attention to the delicate topic of credit card fraud detection. [5-6] It is usual practice to employ ANNs, rule-induction techniques, decision trees, SVMs, LRs, and meta-heuristics such as k-means clustering, evolutionary algorithms, and closest neighbor algorithms in order to identify instances of fraud. Humans are capable of committing various forms of fraud, including but not limited to stealing, miscommunication, deceit, dishonesty, and the making of clever but deceptive recommendations. Manually verifying the activities and identities of most external parties can be too costly for companies dealing with millions of them. Sure, investigating each dubious deal adds up in the bureaucratic ante. If the total is less than the cover cost, it is not worthwhile to investigate any transaction, regardless of how fishy it looks. [7]

2 LITERATUE STUDY ON CREDIT CARD FRAUD

Abdul Rehman Khalid and colleagues (2024) made use of Using European datasets, recent fraud detection advancements have shown superior accuracy, precision, recall, and F1-scores by integrating ensemble methods like Bagging, Boosting, Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (KNN) with SMOTE and advanced preprocessing techniques. This has effectively addressed class imbalance. By reducing features using Compact Data Learning (CDL), which Xiaomei Feng et al. (2024) suggested, the accuracy of fraud detection is greatly enhanced compared to conventional approaches. Using SVM and RF, Diana T. Mosa et al. (2024) applied 15 MHO approaches to Kaggle datasets, and the results were impressive: 97% accuracy after 90% feature reduction. Among seven hybrid ML frameworks tested, Esraa Faisal Malik et al. (2022) found that Adaboost paired with LGBM produced the best results, highlighting the strength of hybrid models. Igor Mekterović et al. (2021) tackled the difficulties of real-world data by concentrating on feature engineering and the practical obstacles of detecting fraud using actual CNP transaction data**.**Emilija Strelcenia et al. (2023) introduced K-CGAN for superior data augmentation, outperforming traditional methods like SMOTE and B-SMOTE in both F1-score and accuracy. Further enhancing data generation, Ibomoiye Domor Mienye et al. (2024) developed a GAN-GRU model, effectively integrating RNNs and GANs to synthesize fraud data and significantly improve model sensitivity and accuracy. Mengqiu Li et al. (2024) proposed the innovative FEDGAT-DCNN—a federated learning framework combining dilated CNN and Graph Attention Networks (GAT)—which effectively addressed sparse data and privacy challenges, outperforming existing federated approaches. Additionally, Abdullah Alharbi et al. (2024) introduced a novel text2IMG method, transforming textual transaction data into image representations for CNN processing, which enhanced class imbalance management and fraud detection performance.

Dataset description

The dataset contains transactions made by credit cards in September 2013 by European cardholders. This dataset presents transactions that occurred in two days, where we have 492 frauds out of 284,807 transactions. The dataset is highly unbalanced, the positive class (frauds) account for 0.172% of all transactions.

It contains only numerical input variables which are the result of a PCA transformation. Unfortunately, due to confidentiality issues, we cannot provide the original features and more background information about the data. Features V1, V2, … V28 are the principal components obtained with PCA, the only features which have not been transformed with PCA are 'Time' and 'Amount'. Feature 'Time' contains the seconds elapsed between each transaction and the first transaction in the dataset. The feature 'Amount' is the transaction Amount, this feature can be used for example-dependant cost-sensitive learning. Feature 'Class' is the response variable and it takes value 1 in case of fraud and 0 otherwise.

Table 1: Literature Study

Author(s) & Year	Technique(s) / Model(s)	Key Outcomes
Abdul Rehman Khalid et al. (2024)[11]	Bagging, Boosting, RF, SVM, KNN; SMOTE + Under-sampling	Ensemble models outperformed conventional ML; strong accuracy, precision, recall, F1.
Xiaomei Feng et al. (2024)[12]	Compact Data Learning (CDL), Feature Reduction	Reduced dataset size without losing accuracy; CDL outperformed baseline models.
Diana T. Mosa et al. (2024)[13]	Meta-Heuristic Optimization (15 MHOs), Feature Selection, SMOTE	Achieved **97% accuracy**, **90% feature reduction**; strong evidence for feature selection benefits.
Esraa Faisal Malik et al. (2022)[14]	Hybrid Adaboost + LightGBM	Hybrid model outperformed all standalone ML methods.
Igor Mekterović et al. (2021)[15]	Feature Engineering, Cost-Benefit Analysis	Identified key fraud risk areas; aligned ML outputs with business investment needs.
Emilija Strelcenia et al. (2023)[6]	K-CGAN, B-SMOTE, SMOTE	K-CGAN achieved superior accuracy and F1; augmentation improved minority detection.
Ibomoiye Domor Mienye et al. (2024)[17]	GANs + RNN (LSTM, GRU, Simple RNN)	GAN-GRU reached **0.992 sensitivity** and **1.000 specificity**; excellent on imbalanced data.
Btoush et al. (2025)[18]	Hybrid ML + DL (BiLSTM, CNN-attention + DT, RF, SVM, XGBoost, CatBoost, LR), Stacking	Achieved **94.63% F1**; handled imbalance effectively; outperformed individual ML/DL models.
L. Theodorakopoulos et al. (2025)[19]	Distributed ML (PySpark): LR, DT, RF, XGBoost, CatBoost	XGBoost & CatBoost gave near-ideal accuracy; scalable for large datasets; supports real-time fraud detection.
J. Adejoh et al. (2025)[20]	Distributed ML System (PySpark) using LR, DT, RF, XGBoost, CatBoost	Similar findings: high accuracy, scalable analytics, strong handling of imbalance.
M. Jabeen et al. (2025)[21]	Unsupervised Ensembles (AE-ASOM, RBM-ASOM), Adaptive Reconstruction Threshold	AE-ASOM: **Accuracy 0.980**, **F1 0.967**; RBM-ASOM: **Accuracy 0.975**, **F1 0.955**; low false positives; memory-efficient.
C. Li et al. (2025)[22]	Hybrid CNN-LSTM + SMOTE + Hyperparameter Tuning	Pre-tuning F1: 76%; Post-tuning: **Recall 99%**, **Precision 83%**, **F1 91%**, **ROC-AUC 0.9995**.
M. Tayebi et al. (2025)[23]	Multi-Module System: anomaly cleaning, resampling, feature governance, LSTM + RF dual-channel	**99.98% accuracy**, **90.46% F1**, **96.39% AUC**; enhanced robustness and sequence modeling.
A. A. Compagnino et al. (2025)[24]	Generative Models (VAE, AE, GAN, AE-GAN) vs. SMOTE/ADASYN	Generative models produced better synthetic fraud samples; outperformed traditional oversampling in BEFS metrics.
N. Baisholan et al. (2025)[25]	Review: ML for financial fraud (supervised, unsupervised, hybrid)	Identified trends in DL & ensembles; highlighted challenges: imbalance, concept drift, privacy, deployment issues.
Y. Wu et al. (2025)[26]	FraudX AI (RF + XGBoost ensemble), SHAP Interpretability	Achieved **95% recall**, **97% AUC-PR**; strong interpretability; outperformed eight baseline ML models.
K. Hayat et al. (2025)[27]	Mode Imputation, ANN, CNN, Gradient Boosted Trees	GBDT achieved **96.02% accuracy**; mode imputation improved dataset quality; robust under 50% missing data.

Table 2: how data imbalance is addressed and the advancements in machine learning techniques:

Method / Technique	Description	Advantages	Limitations / Disadvantages
Random Oversampling	Duplicates existing minority class samples to balance class distribution.	Simple to apply; improves minority representation; can enhance recall.	High risk of **overfitting** due to repeated samples; reduced generalization capacity.
Random Undersampling	Removes a portion of majority samples to equalize class proportion.	Reduces dataset size → faster training; useful for very large datasets.	Loss of potentially **valuable information**; may cause underfitting.
SMOTE (Synthetic Minority Over-sampling Technique)	Generates synthetic minority samples by interpolating neighbors.	Produces more diverse samples; reduces overfitting seen in simple oversampling.	Can introduce **noise or unrealistic samples**; sensitive to parameter tuning.
ADASYN (Adaptive Synthetic Sampling)	A SMOTE variant that generates more synthetic samples in regions where minority samples are harder to learn.	Focuses on difficult cases; improves minority-class learning.	Risk of **amplifying noise**; higher computational cost.
Class-Weight Adjustment (e.g., SVM, Logistic Regression)	Assigns higher penalties for misclassifying the minority class during training.	No data duplication required; prevents model bias toward majority class.	Requires careful tuning; may lead to over-compensation and instability.
Ensemble Methods (Bagging, Boosting, Stacking)	Combines multiple learners to reduce bias, variance, and improve detection of rare events.	High predictive power; Boosting excels at minority detection; Stacking integrates strengths of multiple models.	Computationally expensive; **harder to interpret**; risk of overfitting if not regularized.
Anomaly Detection Techniques	Treats fraudulent cases as anomalies or outliers rather than a separate class.	Very effective for **extremely imbalanced datasets**; requires no balanced training set.	Poor performance if minority class does not have clear anomaly characteristics.
Balanced Random Forest	Uses balanced bootstrapped samples for	Reduces bias toward majority class; retains robustness of Random Forest.	Still sensitive to noise; may require careful tuning of tree depth and sampling size.

	each tree by undersampling the majority class.		
Cost-Sensitive Learning	Incorporates misclassification costs directly into training to penalize minority-class errors more heavily.	Aligns learning with real-world costs; effective when fraud is costly.	Requires **domain knowledge** to set appropriate costs; may lead to conservative predictions.
Transfer Learning	Uses pretrained models or representations from related tasks to overcome limited or imbalanced data.	Reduces dependency on large balanced datasets; improves generalization.	Requires high computational resources; pretrained models may not align with financial data structure.
GAN-based Oversampling (e.g., CGAN, K-CGAN)	Uses Generative Adversarial Networks to create realistic synthetic minority samples.	Produces highly realistic fraud samples; avoids noise issues seen in SMOTE; improves minority detection.	Training GANs is challenging; risk of mode collapse; computation-heavy.
Hybrid ML + DL Models (e.g., CNN-LSTM, BiLSTM, Autoencoders + SOM, Stacking)	Combines traditional ML with deep learning for enhanced feature extraction and sequence modeling.	Achieves superior performance on complex fraud patterns; handles high-dimensional, temporal data effectively.	Computationally expensive; requires large datasets and expert tuning.
Unsupervised Learning (Autoencoders, Isolation Forest, RBM, Clustering)	Learns normal behavior patterns and flags deviations as fraud.	Useful when fraudulent labels are rare or incomplete; adaptable to evolving fraud patterns.	Susceptible to false positives; requires careful threshold selection

Table 3: Credit Card Fraud Detection Dataset

Section	Details
Context / Purpose	Credit card companies must accurately identify fraudulent transactions to protect customers from unauthorized charges. Effective fraud detection models minimize financial loss and improve consumer trust.
Dataset Source	Credit card transactions made by European cardholders in September 2013.
Time Span Covered	Transactions recorded over two consecutive days.
Total Number of Transactions	284,807
Number of Fraudulent Transactions	492
Class Imbalance Ratio	Fraud cases represent 0.172% of all transactions (highly imbalanced dataset).
Input Feature Type	All features except *Time* and *Amount* are numerical variables transformed using Principal Component Analysis (PCA).
PCA-Transformed Features	V1, V2, V3, …, V28 (principal components extracted from the original dataset).
Non-PCA Features	Time: Seconds elapsed between each transaction and the first transaction in the dataset. Amount: Monetary value of the transaction; suitable for cost-sensitive learning.
Target Variable	Class → 0 = legitimate transaction, 1 = fraud.

3 CONCLUSIONS

This review demonstrates that most recent studies report substantial improvements in fraud detection performance when moving beyond traditional machine learning methods. Ensemble models consistently outperform individual classifiers across key evaluation metrics such as precision, recall, accuracy, and F1-score, highlighting their robustness in handling highly imbalanced datasets. Likewise, advanced data augmentation techniques—including SMOTE, ADASYN, and particularly K-CGAN—show strong effectiveness in enhancing the detection of minority-class instances, with K-CGAN achieving superior F1 and accuracy results. Feature selection and dimensionality reduction also emerge as critical factors, with several studies employing meta-heuristic optimization to identify the most influential features, thereby improving efficiency while reducing computational cost. The collective findings of the reviewed literature underscore the pressing need for continuous innovation and adaptability in fraud detection systems. As fraud behaviors evolve in complexity, the integration of hybrid machine learning models, sophisticated generative techniques, and intelligent feature engineering will be essential for developing more accurate, scalable, and resilient fraud detection frameworks.

REFERENCES

[1]. Kundu, S. Panigrahi, S. Sural, and A. K. Majumdar, "BLAST-SSAHA hybridization for credit card fraud detection," IEEE Transactions on Dependable and Secure Computing, vol. 6, no. 4, pp. 309–315, (2009).
[2]. Shen, R. Tong, and Y. Deng, "Application of classification models on credit card fraud detection," (2007).
[3]. J. Dahl, "Card fraud," Credit Union Magazine, (2006).
[4]. S. Ghosh and D. L. Reilly, "Credit card fraud detection with a neural-network," in Proceedings of the 27th Hawaii International Conference on System Sciences, vol. 3, pp. 621–630, (1994).
[5]. K. Deng, R. Zhang, H. Guo, D. Zhang, W. Jiang, and X. Niu, "Analysis and study on detection of credit fraud in e-commerce," (2011).
[6]. L. Seyedhossein and M. R. Hashemi, "Mining information from credit card time series for timelier fraud detection," in International Symposium on Telecommunications, (2010).

[7]. L. Delamaire, H. Abdou, and J. Pointon, “Credit card fraud and detection techniques: A review,” (2009).
[8]. M. F. Gadi, X. Wang, and A. P. Lago, “Comparison with parametric optimization in credit card fraud detection,” (2008).
[9]. M. D. H. Mahdi, K. M. Rezaul, and M. A. Rahman, “Credit fraud detection in the banking sector in UK: A focus on e-business,” (2010).
[10]. M. Pejić-Bach, “Profiling intelligent systems applications in fraud detection and prevention: Survey of research articles,” (2010).
[11]. A. R. Khalid, N. Owoh, O. Uthmani, M. Ashawa, J. Osamor, and J. Adejoh, “Enhancing credit card fraud detection: An ensemble machine learning approach,” Big Data and Cognitive Computing, vol. 8, no. 1, p. 6, (2024), doi: 10.3390/bdcc8010006.
[12]. X. Feng and S.-K. Kim, “Novel machine learning based credit card fraud detection systems,” Mathematics, vol. 12, no. 12, p. 1869, (2024), doi: 10.3390/math12121869.
[13]. D. T. Mosa, S. E. Sorour, A. A. Abohany, and F. A. Maghraby, “CCFD: Efficient credit card fraud detection using meta-heuristic techniques and machine learning algorithms,” Mathematics, vol. 12, no. 14, p. 2250, (2024), doi: 10.3390/math12142250.
[14]. E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Y. Chew, “Credit card fraud detection using a new hybrid machine learning architecture,” Mathematics, vol. 10, no. 9, p. 1480, (2022), doi: 10.3390/math10091480.
[15]. Mekterović, M. Karan, D. Pintar, and L. Brkić, “Credit card fraud detection in card-not-present transactions: Where to invest,” Applied Sciences, vol. 11, no. 15, p. 6766, (2021), doi: 10.3390/app11156766.
[16]. E. Strelcenia and S. Prakoonwit, “Improving classification performance in credit card fraud detection by using new data augmentation,” AI, vol. 4, no. 1, pp. 172–198, (2023), doi: 10.3390/ai4010008.
[17]. D. Mienye and T. G. Swart, “A hybrid deep learning approach with generative adversarial network for credit card fraud detection,” Technologies, vol. 12, no. 10, p. 186, (2024), doi: 10.3390/technologies12100186.
[18]. X. Btoush, X. Zhou, R. Gururajan, K. C. Chan, and O. Alsodi, “Achieving excellence in cyber fraud detection: A hybrid ML+DL ensemble approach for credit cards,” Applied Sciences, vol. 15, no. 3, p. 1081, (2025), doi: 10.3390/app15031081.
[19]. L. Theodorakopoulos, A. Theodoropoulou, A. Tsimakis, and C. Halkiopoulos, “Big data-driven distributed machine learning for scalable credit card fraud detection using PySpark, XGBoost, and CatBoost,” Electronics, vol. 14, no. 9, p. 1754, (2025), doi: 10.3390/electronics14091754.
[20]. Adejoh, N. Owoh, M. Ashawa, S. Hosseinzadeh, A. Shahrabi, and S. Mohamed, “An adaptive unsupervised learning approach for credit card fraud detection,” Big Data and Cognitive Computing, vol. 9, no. 9, p. 217, (2025), doi: 10.3390/bdcc9090217.
[21]. M. Jabeen, S. Ramzan, A. Raza, N. L. Fitriyani, M. Syafrudin, and S. W. Lee, “Enhanced credit card fraud detection using deep hybrid CLST model,” Mathematics, vol. 13, no. 12, p. 1950, (2025), doi: 10.3390/math13121950.
[22]. Li, P. Qin, and R. Pu, “Enhancing strategic decision-making in fraud management: A dual-channel framework with TOPSIS for credit card fraud detection,” Electronics, vol. 14, no. 23, p. 4672, (2025), doi: 10.3390/electronics14234672.
[23]. M. Tayebi and S. El Kafhali, “Generative modeling for imbalanced credit card fraud transaction detection,” Journal of Cybersecurity and Privacy, vol. 5, no. 1, p. 9, (2025), doi: 10.3390/jcp5010009.
[24]. A. A. Compagnino et al., “An introduction to machine learning methods for fraud detection,” Applied Sciences, vol. 15, no. 21, p. 11787, (2025), doi: 10.3390/app152111787.
[25]. N. Baisholan et al., “FraudX AI: An interpretable machine learning framework for credit card fraud detection on imbalanced datasets,” Computers, vol. 14, no. 4, p. 120, (2025), doi: 10.3390/computers14040120.
[26]. Y. Wu, L. Wang, H. Li, and J. Liu, “A deep learning method of credit card fraud detection based on continuous-coupled neural networks,” Mathematics, vol. 13, no. 5, p. 819, (2025), doi: 10.3390/math13050819.
[27]. Hayat and B. Magnier, “Data leakage and deceptive performance: A critical examination of credit card fraud detection methodologies,” Mathematics, vol. 13, no. 16, p. 2563, (2025), doi: 10.3390/math13162563.