Journal of Global Research in Electronics and Communication
Volume 1, No. 12, December, 2025
Available Online at: www.jgrec.info
REVIEWPAPER

A Systematic Survey of Machine Learning Methods for Fraud Identification in Credit Cards

Prachi Rajput
Lecturer ,Department of Computer Science and Engineering,
ITM SLS Baroda University
Vadodara
prachi9497@gmail.com

***Abstract*—Credit card fraud is still a huge issue for the financial industry, and over the years, it has caused the industry to lose billions of dollars across the globe. The once-efficient traditional rule-based systems are now almost entirely obsolete. The primary focus of this survey is the shift from conventional rule-based systems to astute, data-driven solutions for credit card fraud detection. It even goes so far as to thoroughly examine ML-based credit card fraud detection (CCFD). Along with the difficulties of class imbalance, idea drift, and verification delay, the study offers a comprehensive analysis of the concept and different kinds of credit card transactions. It also discloses publicly available datasets, including Kaggle, IEEE-CIS, and PaySim. This research highlights the contributions of preprocessing methods, such as data cleaning, normalization, and PCA, to enhancing data quality and also discusses ethical dilemmas related to transparency, bias reduction, and informed consent. Besides that, the paper discusses various supervised learning methods (Logistic Regression, Decision Tree, Naïve Bayes) as well as different unsupervised learning approaches (K-means, DBSCAN, Autoencoders, One-Class SVM) that can be applied to identify fraudulent transactions. The survey reveals that ML models are responsible for improving the accuracy, flexibility, and speed of detection, which, in turn, can lead to the establishment of safer, more trustworthy financial systems.**

Keywords*—Credit Card Fraud Detection (CCFD), Machine Learning (ML), Supervised Learning, Unsupervised Learning, Financial Security, Fraud Analytics.

I. INTRODUCTION

Financial services have evolved significantly from the days of grain banks and temple financing to the current financial methods. One of the main causes of banks' crucial role in ensuring quicker and more effective service delivery has been the banking industry's change[1][2]. The banking industry is characterized by fierce rivalry, with clients having many alternatives [3]. One of the most significant challenges for such a firm is keeping customers and workers. As a result of technological advancement and digitalization of the business in the banking industry, credit card usage has significantly increased[4]. Credit cards are intended to make transactions more convenient by serving as an alternative to cash or checks, providing a line of credit, and safeguarding against fraud. Credit cards serve as a means of payment for cardholders' expenses. Also, they are a way to enhance the credit scores[5]. Furthermore, they offer incentives that can be used to make purchases, such as miles, points, or cash back.

Credit cards have been the most prevalent kind of financial fraud, which has increased over the past few years. Both the frequency of card payments and the overall trend of credit card theft have been increasing[6]. Although the usage of cards has grown dramatically in recent years, regrettably, the same cannot be said for fraud[7]. Hence, the yearly losses amount to billions of euros[8]. Credit card fraud is not only a source of massive loss but also a major factor that destabilizes the financial system; therefore, concern for it is global among the financial industries[9][10]. Besides, conventional fraud detection systems, such as expert rules, are insufficient, as Fraudsters are always changing their strategies to evade discovery. Additionally, machine learning (ML) techniques may also be insufficient if they fail to adjust to new fraud schemes.

Fraud involves illegally obtaining goods, services, or money and is often difficult to detect due to hidden criminal motives. Among different types, the unlawful use of credit cards or other comparable payment methods to get funds is one of the most prevalent criminal acts[11]. The biggest obstacle facing financial systems that attempt to identify and halt fraudulent transactions is identifying and preventing credit card fraud. The old ways of detecting them are no longer sufficient, so advanced fraud-detection models must be developed. By analyzing cards' spending habits and transaction data, contemporary fraud detection systems, are designed to provide safe credit usage and increase the trust of users in digital payment systems [12]. When fraudsters overpower fraud prevention systems and initiate fraudulent transactions, fraud detection systems become involved.

Fraudulent actors perform such acts as obtaining products or services without paying for them or using account funds covertly; this can also encompass behavioural, offline, application, and bankruptcy fraud [13]. The biggest obstacle facing financial institutions trying to identify and halt fraudulent transactions is identifying and preventing credit card fraud[14]. As ML techniques have grown quickly, a number of ML models have been incorporated into credit card fraud detection[15]. These models are evaluated and trained on a range of datasets [16]. They mostly rely on several sources, in order to improve their durability and generalizability. These strategies ultimately aim to improve the precision and efficacy of fraud detection systems[17][18]. Thus, providing more effective support to financial institutions in the fight against fraudulent transactions and financial losses.

A. Structure of the Paper

The paper is organized as follows: Section II covers credit card concepts, transaction types, traditional fraud-detection systems, and their challenges. Section III reviews datasets, pre-processing methods, and ethical considerations. Section IV examines supervised and unsupervised ML approaches for fraud detection. Section V provides a literature review of recent advancements, and Section VI summarizes the main conclusions and suggests further lines of inquiry.

II. Concept of Credit Card

Customers can borrow money from banks or other financial institutions using a credit card to make purchases and pay back the balance later. Cardholders get a monthly bill for their expenses, and interest is applied to the leftover balance if the entire amount isn't paid by the due date. The card issuer establishes the maximum borrowing limit (credit limit) depending on variables such as income and credit history. Responsible use of the card can help establish credit and provide incentives and cashback.

A. Types of Credit Card Transactions

In today's culture, most customers use credit cards daily. Credit cards are widely used, according to a poll on the subject. Banks and other financial institutions must carefully examine the credit card usage situation and utilize time series data to accurately estimate the consumption trend of all clients in all age groups, because of the diverse usage habits of credit card holders from different age groups[19]. The types of credit card transactions are discussed below:

1) Card-Present

At the point of sale (POS), card-present transactions take place when the consumer physically hands over their payment card to the retailer. This typically involves swiping, inserting, or tapping the card into a card reader or terminal. CP transactions are commonly conducted in brick-and-mortar stores, where customers make in-person purchases.

2) Card-Not-Present (CNP)

The most prevalent examples of these transactions are sales done over the phone or online, in which the business does not physically view the payment card[20]. CNP fraud is when someone illegally obtains another person's payment information and then uses it for a CNP transaction without authorization.

B. Traditional Fraud Detection Systems

A structured process for identifying and stopping fraudulent activity in financial transactions is called a fraud detection pipeline. This section covers the full fraud detection process:

1) Data Acquisition

The data acquisition problem can be treated as a decision problem. If a consumer has an existing bank account and needs to apply for a credit card, gather all the information they require[21]. Data such as salary, assets, and other financial information.

2) Data Preprocessing

Data pre-processing comprises organizing the original business data with the new "business model," eliminating characteristics that are irrelevant to the data mining objective[22], and generating clear, precise, and uncomplicated data to improve the calibre and effectiveness of excavation under the direction of domain expertise. The pre-processing pipeline's tabular form is displayed in Table I.

TABLE I. TABLE I: PREPROCESSING PIPELINE

Techniques	Definition
Data Cleaning	Null values are filled in, noisy data is smoothed, isolated data is found and eliminated, and inconsistencies are fixed in order to accomplish the aim of data cleaning.
Data Integration	Data from several sources, such as databases, data cubes, or regular files, should be stored in a consistent location (such as a data warehouse).
Data Conversation	Transform the information into a format suitable for excavation; for example, proportionally zoom the attribute data so it fits within a smaller, designated area.
Data Reduction	Compressed data, which is significantly smaller than the original data but maintains its integrity, was used to create the dataset. The reduced dataset is therefore more affected by data mining, which yields the same (or nearly the same) analytical result.

3) Feature Engineering

Feature engineering is a fantastic method for improving the performance of credit card identification systems since it helps uncover the key components that make the system function better and produce better outcomes[23]. The various feature engineering techniques are given below:

- **Behavioural Analysis:** The credit card ownership and usage patterns are strongly influenced by user demographics, including age, sex, occupation, religion, education, income, marital status, culture, and debt-related attitudes.
- **Aggregated Features:** A transaction aggregation strategy is used to improve the performance of credit card fraud detection by extracting specific aggregated features, like the total sum or the quantity of transactions started with the same merchant on the same day[24], currency, or country to capture the purchasing habits of customers.
- **Time-Based Features:** Certain information is still not fully captured by the aggregated features when they are used. Specifically interested in examining the timing of the transaction. This is justified by the idea that a customer should do business at comparable times. Using the arithmetic mean while discussing transaction time is a simple mistake to make, and this is especially true when examining a characteristic like the mean of transaction time[8]. The timing of a transaction, as displayed in a 24-hour clock, is shown in Figure 1. The actual timing distribution is not well represented by the dashed line, which is the arithmetic mean of the transaction times.

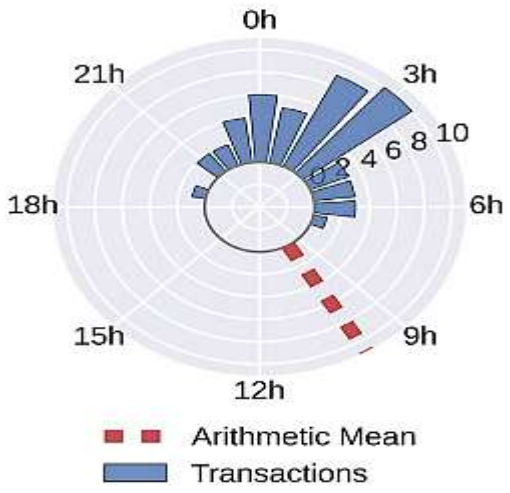

Fig. 1. Analysis of The Time of A Transaction Using A 24-Hour Clock

C. Challenges In Fraud Detection

Regardless of what CCFDS does, fraudsters continually discover new methods to get around it. Consequently, it is both difficult and necessary for all financial institutions to continue improving and investing in CCFDS. Some of the challenges are explained below:

1) Class Imbalance Challenge

The issue of unbalanced classes is one of the main CCFD difficulties that significantly impacts the effectiveness of classification models [25][26]. Because the class is not evenly distributed, the dataset of credit card transactions is thought to be unbalanced, with far fewer fraudulent transactions than typical ones.

2) Concept Drift

As the market and technology evolve, so do consumer purchasing habits and the tactics used by scammers. The aggregate term for these changes is "concept drift." Card investigators and fraudsters must thus adjust to these shifting trends. A CCFD model needs to be updated often to effectively address concept drift issues [27]. A poorly managed concept drift issue can lead to inconsistent FD model updates and subpar fraud detection.

3) Verification Latency

Verification latency, which arises when investigators are unable to review every transaction in an actual FDS, is the third difficulty [28]. Many transactions cannot be verified unless they are reported as fraudulent by a cardholder[29] Or a fair amount of time has elapsed without a dispute, they are often regarded as valid. As a result, the interplay of alarm feedback delays the majority of the trained samples required to update the classifier.

III. Datasets Used In Credit Card Fraud Detection

The identification of credit card fraud has become increasingly important as more digital transactions occur each minute. CCFD uses specific datasets to identify instances of credit card fraud. The datasets are more briefly discussed in this section.

A. Common Public Datasets

The finance industry utilizes a variety of datasets to detect fraud across multiple domains, including credit card fraud, banking transaction fraud, and others. In banking and finance, publicly accessible data is frequently utilized to detect credit card fraud[30]. The datasets that are freely available and mostly used are discussed below:

1) Credit Card Fraud Detection Dataset

The dataset of European credit cardholders was established because it is hard to get real credit card transaction data from companies. There are 284,807 samples in the non-fraud group and 492 samples in the fraud category (i.e., 0.172% of the total)[31]. The associated research has extensively used this openly accessible dataset on Kaggle.

Figure 2 presents a line chart showing the intensity (μ) of 'Fraud' (orange) and 'Not Fraud' (blue) transactions over time (0–175,000 seconds). The 'Not Fraud' category displays higher overall magnitudes with sharper fluctuations, peaking around 75,000 seconds (9μ) and dipping near 110,000 seconds (1.3μ) before rising again. In contrast, 'Fraud' starts at about 2.5μ, reaches a peak around 40,000 seconds (8μ), then declines. It also shows a smaller increase near 150,000 seconds (5.7μ).

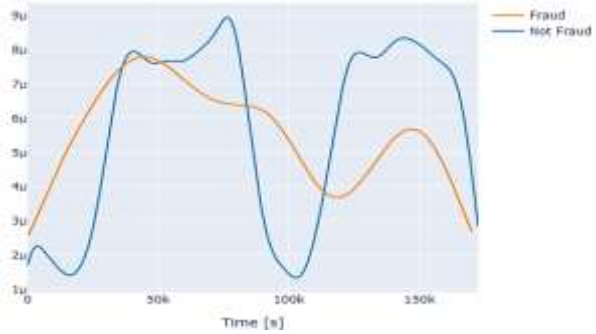

Fig. 2. Credit Card Transactions Density Plot

2) IEEE-CIS Fraud Detection Dataset

The method's robustness and generalizability are assessed using the IEEE-CIS fraud detection dataset[32]. The test transaction, train identity, and test transaction files make up the IEEE-CIS fraud detection dataset. The respective attribute columns of these files are 394, 41, 393, and 41. TransactionID links the transaction to the identification.

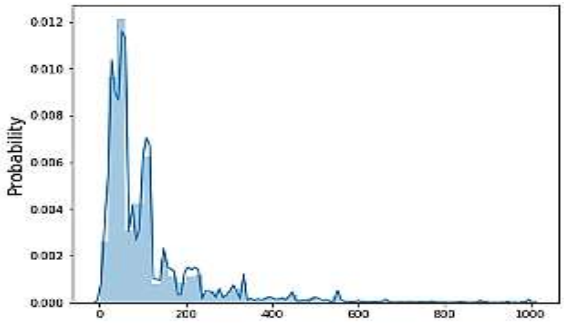

Fig. 3. Transaction Values Distribution in IEEE-CIS Fraud Detection Data

A histogram combined with a KDE curve is shown in Figure 3, which illustrates how the data values between 0 and 1000 are likely distributed. The distribution is right-skewed, and most of the data lie between 0 and 200. There is a pronounced primary peak at 25, which is followed by a more subtle secondary peak at 100. The area of 200 and beyond shows a very rapid decline in frequencies, forming a long, low-probability tail that extends to 1000.

3) PaySim (Synthetic) Dataset

To identify financial fraud, a synthetic dataset created with the PaySim simulator is provided [33] For the purpose of recognizing financial fraud. PaySim generates a synthetic dataset that mimics the typical transaction flow while introducing malicious activity by combining data from the private dataset. Thus, the fraud detection systems can be assessed[34]. Figure 4 shows the percentage of fraud by transaction type.

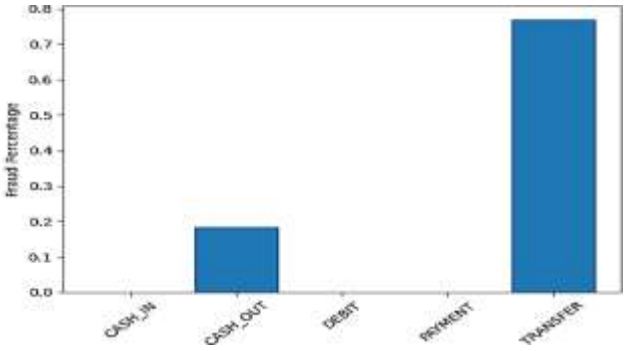

Fig. 4. Fraud Percentage by Transaction Type

B. Preprocessing Needs

To improve the raw data quality, a systematic pre-processing pipeline is applied.

1) Handling Multicollinearity

The computation of Pearson correlation coefficients was used to examine multicollinearity among characteristics. Principal Component Analysis (PCA), which separates correlated variables into uncorrelated components while preserving most of the variation, can be used to reduce redundancy.

2) Normalizing the Data

The feature ranges were normalized by the use of standardization, especially for distance-based algorithms such as SVM. Every numerical attribute was standardized to have a variance of 1 and a mean of 0.

3) Removal of Missing and Null Values

Missing and null value removal refers to the process where missing data entries, incomplete or null data entries, are identified and removed to guarantee the quality of data and avoid analysis or model training errors. The step ensures the integrity of the datasets and enhances the trustworthiness of ML models.

4) Prevention of Data Leakage

To avoid data leakage, training and test datasets were stored in a highly isolated manner so that there was no information about the test set that influenced the model during the training phase.

C. Ethical Considerations

Technological development should be accompanied by ethical responsibility. Financial institutions not only handle sensitive information but are also crucial to ensuring the accountability and fairness of automated decision-making processes. This section addresses the major ethical concerns and the necessity to actively solve them.

1) Algorithmic Transparency

ML systems are transparent when they can be interpreted and comprehended as to how they arrive at their decisions. The interpretability of the model logic is also essential in fraud detection, where the ML model is likely to be used autonomously because stakeholders like regulators, auditors [35]Data scientists need to understand the model's logic to inform their decision-making. When such actions as transaction blocking affect users, clear explanations are provided, and Explainable AI (XAI) systems, like SHAP or LIME, are used to improve comprehension, accountability, and model prediction confidence.

2) Bias Mitigation

The AI and ML systems that are trained based on historical or unbalanced data have a risk of reproducing or enhancing pre-existing biases, leading to discriminatory effects towards a specific demographic group or a specific pattern of behavior. It may result in inequity and unfair treatment of certain users, which compromises equity and fairness in terms of financial services [9] and decision-making.

3) Informed Consent

Users ought to be able to understand and manage how ML algorithms use their financial and personal information. Ethical ML design involves clearly communicating how data is used in fraud detection, offering opt-in or opt-out options where feasible, and ensuring data is anonymized or pseudonymized when obtaining full consent is not practical.

IV. Machine Learning Approaches In Fraud Detection

Attacks by fraudsters on credit card transactions are more frequent now than in the past [36]. Developments in data science and ML have led to the creation of several algorithms to determine if a transaction is fraudulent.

A. Supervised Learning Methods

The aim of supervised learning algorithms is to translate inputs to intended outputs[37]. The model learns to classify input vectors into one of many classes using labelled examples. The supervised ML models for fraud classification—This section covers decision trees, logistic regression, and naïve bayes. Figure 5 shows the supervised learning process.

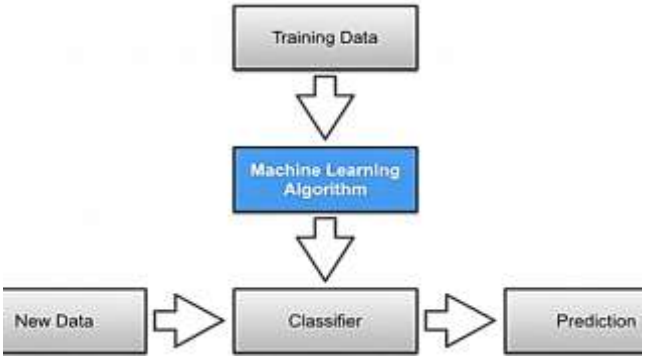

Fig. 5. Supervised Learning Procedure

1) Logistic Regression

A set of weighted characteristics has to be taken out of the input for logistic regression to work. Logs are then joined together linearly, which means that each characteristic is multiplied by a weight. A classification technique called logistic regression (1/0, Yes/No, True/False) is utilized to predict binary outcomes using a set of independent variables.

2) Decision Tree

DT are a type of classifier that are shown as recursive splits of the instance space. The root the fundamental node of the

decision tree is a scattered tree with no incoming edges. It is composed of nodes arranged in a rooted tree. A DT example is shown in Figure 6.

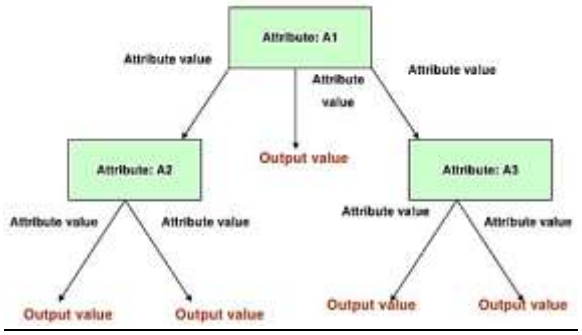

Fig. 6. Example of a Decision Tree

3) Naïve Bayes

Another supervised learning technique is the Bayesian classification, which is also a statistical classification method. The model is assumed to be probabilistic, and principled capture of model uncertainty is enabled by calculating outcome probabilities. Resolving prediction problems is the main goal of Bayesian classification.

B. Unsupervised Learning Methods

Unsupervised detection methods aim to describe the transaction data distribution and don't need to understand the transaction labels[38]. Since they don't distribution of transaction data and don't require understanding of the transaction labels rely on transactions that have already been deemed fraudulent, they can be used to identify hidden forms of fraud, as they are based on the notion that fraud is present in transaction distribution outliers.

1) Clustering Techniques (K-means and DBSCAN)

The DBSCAN density clustering algorithm is used in conjunction with the K-means clustering approach. The DBSCAN clustering method is based on the density between items in the dataset. The basic concept is to predefine a density threshold and build comparable clusters if the density of nearby regions exceeds it. Eps and MinPts are its primary parameters. MinPts determines the neighbourhood point threshold, whereas Eps determines the neighbourhood radius. The combination of two factors determines the impact of density clustering. Dense datasets of any type may be clustered using the DBSCAN method [39]. It addresses the drawback that distance-based clustering techniques can only produce spherical clusters.

2) Autoencoders

Autoencoder learning is an unsupervised learning process that aims to provide an output that corresponds to its input. As such, it may be thought of as a network that performs supervised learning; the output is the reconstruction of the initial input, x. In two stages encoding and decoding an autoencoder learns to map an input to an output. The autoencoder has a bottleneck; the input data must be learnedly compressed since a bottleneck limits the amount of information that can move throughout the whole network [40].

3) One-Class SVM

One-class SVM is a method of SVM that is based on kernels. Training data is translated from the input space to the feature space using a kernel function, which then separates the mapped data from the origin by finding the feature space hyperplane with the largest margin. This is the basic idea behind one-class SVM. In one-class SVM, there are two methods for creating a decision boundary [41]. The v parameter determines the form of the boundary by balancing the proportion of positive data points and outliers. The second method involves separating a certain proportion of the outliers from the remaining data by training the decision boundary as a hyperplane that passes through the origin of the coordinate system and the data points.

V. Literature Review

This review summarizes the use of ML methods to detect credit card fraud, with an emphasis on improving detection precision, effectiveness, and adaptability. The use of multiple techniques, including ensemble, supervised, and unsupervised learning models, represents a significant leap toward creating intelligent, safe, and effective fraud detection systems.

Mahesh et al. (2025) This paper primarily discusses features, models and real-time detection mechanisms that together give rise to better accuracy and reduction of false alarms. The experiment's findings have demonstrated the superiority of ML-based techniques over conventional techniques while also, provide a robust solution for fraud risk reduction. The present research has dedicated itself to showing that ML can indeed bring about the much-needed metamorphosis in the area of bank fraud detection that would ultimately lead to delighted and secure customers[42].

Nair et al. (2025) The research counts on a soft voting ensemble with a total of five robust ML models, comprising two bagging and three boosting ensemble classifiers, namely RF, ET, XGBoost, LightGBM, and CatBoost. The averaged posterior probabilities of the five models are then used to make the final prediction. To ensure balanced data size for legitimate and fraudulent transactions, SMOTE is applied[43].

Gupta et al. (2025) This research is a ML-based CCFD method that attains a very high accuracy rate by using an RF classifier. A publicly available data set was applied to, and many diverse data pre-processing methods were carried out, to resolve class imbalance, such as under sampling, feature selection, and missing value imputation. This exhaustive research not only reveals but also provides recommendations for implementing safer and more efficient centers for the detection of financial services fraud[44].

Jain, Sharma and Kumar (2024) The paper highlights The techniques used by the researcher to identify credit card fraud. Credit card fraud detection was enabled by implementing an elaborate system, Fraud Fort, using algorithms such as RF and LR. Additionally, the study examined how combining RF and LR may improve the efficacy and accuracy of existing fraud detection systems. By closely examining the algorithms' performance on credit card transactions, Fraud Fort's integration of the two approaches has been demonstrated to be effective. It is found that RF and LR can be so effective when combined that a fraud detection system can be reinforced in a way that eventually leads to a more secure and safe economic environment[45].

Vejalla et al. (2023) suggested utilizing machine learning (ML) based on labeled data to identify credit card fraud and separate legitimate from fraudulent transactions. To experiment, supervised machine-learning techniques were employed. In their everyday lives, they encounter many forms

of deception. Credit card fraud is one of the most common forms of theft these days. Using credit cards worldwide may result in fraudulent purchases. They need to understand the trends and the variations in credit card fraud values to prevent it[46].

Nijwala et al. (2023) The XGBoost classifier is used in this work's proposed methodology to handle imbalanced data by identifying fraudulent transactions. Inefficiently, the standard method pre-determines the threshold value. Therefore, Several threshold values are computed and contrasted in their suggested method to get the optimal value that yields the best results and the most efficiency[47].

Singh et al. (2022) This research looks at the most recent developments in ML-based CCFD and uses. This study has looked at and compared the accuracy of four ML algorithms. Catboost is the best algorithm for finding credit card fraud. Credit card fraud was discovered using a dataset that was made available by Kaggle[48].

A summary of recent studies on detecting credit card fraud is presented in Table II, highlighting notable improvements in effectiveness, reliability, and flexibility. However, important challenges remain in achieving scalability and real-world implementation. Future research focuses on different types of integration and better ML adaptation.

TABLE II. SUMMARY OF RELATED STUDIES ON CREDIT CARD FRAUD DETECTION

Reference	Study On	Approach	Key Findings	Challenges / Limitations	Future Directions
Mahesh et al. (2025)	Credit card fraud detection	Feature engineering, model estimation, and real-time detection	ML techniques surpass traditional methods; improve accuracy and reduce false positives	Real-time deployment complexity; dataset not specified	Develop adaptive real-time detection models for evolving fraud patterns
Nair et al. (2025)	Ensemble-based fraud detection	Soft voting ensemble of RF, Extra Trees, XGBoost, LightGBM, CatBoost; SMOTE for class balancing	An ensemble approach improves prediction accuracy and handles class imbalance	Computationally intensive; ensemble interpretability	Optimize ensemble efficiency; explore hybrid models combining bagging and boosting
Gupta et al. (2025)	Random Forest-based fraud detection	Random Forest classifier; feature selection; handling missing values; undersampling	Accurate detection of fraudulent transactions provides practical insights for secure systems	May not generalize across datasets; undersampling may discard useful information	Apply to larger and more diverse datasets; compare with deep learning methods
Jain, Sharma & Kumar (2024)	Fraud Fort system for credit card fraud	Logistic Regression & Random Forest integration	Integration improves detection precision and efficiency; strengthens economic security	Limited to selected algorithms; scalability not fully addressed	Incorporate additional ML models; implement real-time fraud detection
Vejalla et al), (2023)	Supervised fraud detection	Supervised ML on labeled data	Differentiates fraudulent vs legitimate transactions; identifies fraud patterns	Dependent on labeled data; may miss novel fraud patterns	Explore semi-supervised or unsupervised methods for unknown fraud
Nijwala et al. (2023)	Handling imbalanced data in fraud detection	XGBoost with dynamic threshold optimization	Optimal threshold improves efficiency and detection performance	Threshold selection may be dataset-specific; it may not generalize	Automate threshold selection; adapt to changing transaction trends
Singh et al. (2022)	Comparative ML study for fraud detection	Four ML algorithms, including CatBoost, for performance comparison	CatBoost performs best for detecting credit card fraud	Limited algorithm selection; dataset restricted to Kaggle	Explore additional algorithms and datasets; hybrid approaches for improved accuracy

VI. CONCLUSION AND FUTURE WORK

Credit card fraud occurs when a credit card account is used by an unapproved third party without the issuer's or cardholder's knowledge. The document is an in-depth review of the history and significance of credit card fraud detection systems (CCFDS), with a particular emphasis on their role in addressing the growing complexity of fraud cases. Conventional methods, despite being somewhat effective, are unable to cover all aspects of fraud patterns, which are complex and dynamic, leading to using state-of-the-art methods for supervised and unsupervised learning. Looking at the research, it can be inferred that the suggested models—Logistic Regression, Random Forest, XGBoost, and CatBoost—are some of the most precise and trustworthy for identifying fraudulent transactions. But the issues of idea drift, class imbalance, and the requirement for real-time adaptability still exist. The comparison study's findings show that ensemble and hybrid learning strategies routinely perform better than solo models, improving detection rates and minimizing false positives.

Future studies will focus on applying DL and hybrid models for developing adaptable, real-time fraud detection systems. Giving priority to issues of class imbalance, model interpretation, and the application of explainable AI (XAI) will help increase the credibility, scalability, and transparency of banking industry fraud prevention systems.

REFERENCES

[1] D. Patel, “Enhancing Banking Security: A Blockchain and Machine Learning- Based Fraud Prevention Model,” *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 576–583, 2023, doi: 10.14741/ijcet/v.13.6.10.

[2] W. Gaviyau and J. Godi, “Banking Sector Transformation: Disruptions, Challenges and Opportunities,” *FinTech*, vol. 4, no. 3, 2025, doi: 10.3390/fintech4030048.

[3] A.-G. Văduva, S.-V. Oprea, A.-M. Niculae, A. Bâra, and A.-I. Andreescu, “Improving Churn Detection in the Banking Sector: A Machine Learning Approach with Probability Calibration Techniques,” *Electronics*, vol. 13, no. 22, 2024, doi: 10.3390/electronics13224527.

[4] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, “Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms,” *IEEE*

Access, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[5] C. I. Giannikos and E. D. Korkou, "Financial Literacy and Credit Card Payoff Behaviors: Using Generalized Ordered Logit and Partial Proportional Odds Models to Measure American Credit Card Holders' Likelihood of Repaying Their Credit Cards," *Int. J. Financ. Stud.*, vol. 13, no. 1, 2025, doi: 10.3390/ijfs13010022.

[6] G. L. Sahithi, V. Roshmi, Y. V. Sameera, and G. Pradeepini, "Credit Card Fraud Detection using Ensemble Methods in Machine Learning," in *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, Apr. 2022, pp. 1237–1241. doi: 10.1109/ICOEI53556.2022.9776955.

[7] K. B. Thakkar and H. P. Kapadia, "The Roadmap to Digital Transformation in Banking: Advancing Credit Card Fraud Detection with Hybrid Deep Learning Model," in *2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST)*, 2025, pp. 1–6. doi: 10.1109/ICTEST64710.2025.11042822.

[8] A. Correa Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Feature engineering strategies for credit card fraud detection," *Expert Syst. Appl.*, vol. 51, pp. 134–142, Jun. 2016, doi: 10.1016/j.eswa.2015.12.030.

[9] S. B. Shah, "Advancing Financial Security with Scalable AI: Explainable Machine Learning Models for Transaction Fraud Detection," in *2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, IEEE, Apr. 2025, pp. 1–7. doi: 10.1109/ICDCECE65353.2025.11034838.

[10] 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, pp. 1–18, 2025, doi: 10.3390/math13050819.

[11] V. Verma, "Deep Learning-Based Fraud Detection in Financial Transactions : A Case Study Using Real-Time Data Streams," vol. 3, no. 4, pp. 149–157, 2023, doi: 10.56472/25832646/JETA-V3I8P117.

[12] P. Soni and M. Kumar, "Review on Credit Card Fraud Detection Techniques," *Proc. - 2022 5th Int. Conf. Comput. Intell. Commun. Technol. CCICT 2022*, vol. 45, no. 1, pp. 520–525, 2022, doi: 10.1109/CCiCT56684.2022.00097.

[13] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M. S. Hacid, and H. Zeineddine, "An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2927266.

[14] H. P. Kapadia, "Reducing Cognitive Load in Online Financial Transactions," *Int. J. Curr. Sci.*, vol. 12, no. 2, pp. 732–797, 2022.

[15] S. J. Wawge, "A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3345–3352, May 2025, doi: 10.38124/ijisrt/25apr1813.

[16] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 10, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[17] V. Pal and S. K. Chintagunta, "Transformer-Based Graph Neural Networks for RealTime Fraud Detection in Blockchain Networks," pp. 1401–1411, 2023, doi: 10.48175/IJARSCT-11978Y.

[18] X. Feng and S.-K. Kim, "Statistical Data-Generative Machine Learning-Based Credit Card Fraud Detection Systems," *Mathematics*, vol. 13, no. 15, p. 2446, 2025, doi: 10.3390/math13152446.

[19] W. Nai, L. Liu, S. Wang, and D. Dong, "Modeling the Trend of Credit Card Usage Behavior for Different Age Groups Based on Singular Spectrum Analysis," *Algorithms*, vol. 11, no. 2, p. 15, Jan. 2018, doi: 10.3390/a11020015.

[20] A. Bodker, P. Connolly, O. Sing, B. Hutchins, M. Townsley, and J. Drew, "Card-not-present fraud: using crime scripts to inform crime prevention initiatives.," *Secur. J.*, pp. 1–19, Nov. 2022, doi: 10.1057/s41284-022-00359-w.

[21] L. Barua, A. Rahman, S. Ahamed, R. Mia, R. A. Aenney, and K. Newaz, "Credit card application handling using data mining technique," *World J. Adv. Res. Rev.*, vol. 17, no. 2, pp. 839–843, Feb. 2023, doi: 10.30574/wjarr.2023.17.2.0330.

[22] Z. Yan-li and Z. Jia, "Research on Data Preprocessing In Credit Card Consuming Behavior Mining," *Energy Procedia*, vol. 17, pp. 638–643, 2012, doi: 10.1016/j.egypro.2012.02.147.

[23] M. Alamri and M. Ykhlef, "Hybrid Feature Engineering Based on Customer Spending Behavior for Credit Card Anomaly and Fraud Detection," *Electronics*, vol. 13, no. 20, 2024, doi: 10.3390/electronics13203978.

[24] A. Yeşilkanat, B. Bayram, B. Köroğlu, and S. Arslan, "An adaptive approach on credit card fraud detection using transaction aggregation and word embeddings," in *IFIP Advances in Information and Communication Technology*, 2020. doi: 10.1007/978-3-030-49161-1_1.

[25] G. Sarraf, "BalanceNet: Addressing Class Imbalance in AI-Powered Intrusion Detection Through Adaptive Sampling," *Asian J. Comput. Sci. Eng.*, vol. 8, Dec, no. 4, pp. 1–9, 2023.

[26] H. Ahmad, B. Kasasbeh, B. Aldabaybah, and E. Rawashdeh, "Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS)," *Int. J. Inf. Technol.*, vol. 15, no. 1, pp. 325–333, 2023, doi: 10.1007/s41870-022-00987-w.

[27] I. Mekterović, M. Karan, D. Pintar, and L. Brkić, "Credit Card Fraud Detection in Card-Not-Present Transactions: Where to Invest?," *Appl. Sci.*, vol. 11, no. 15, p. 6766, Jul. 2021, doi: 10.3390/app11156766.

[28] S. S. Sulaiman, I. Nadher, and S. M. Hameed, "Credit Card Fraud Detection Challenges and Solutions: A Review," *Iraqi J. Sci.*, vol. 65, no. 4, pp. 2287–2303, 2024, doi: 10.24996/ijs.2024.65.4.42.

[29] V. Shah, "Network Verification Through Formal Methods : Current Approaches and Open Issues," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 90–94, 2021.

[30] S. Pandya, "Comparative Analysis of Large Language Models and Traditional Methods for Sentiment Analysis of Tweets Dataset," *Int. J. Innov. Sci. Res. Technol.*, vol. 9, no. 12, 2024, doi: 10.5281/zenodo.14575886.

[31] X. Feng and S.-K. Kim, "Novel Machine Learning Based Credit Card Fraud Detection Systems," *Mathematics*, vol. 12, no. 12, 2024, doi: 10.3390/math12121869.

[32] S. Jiang, R. Dong, J. Wang, and M. Xia, "Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network," *Systems*, vol. 11, no. 6, p. 305, Jun. 2023, doi: 10.3390/systems11060305.

[33] B. Stojanović *et al.*, "Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications," *Sensors*, vol. 21, no. 5, p. 1594, Feb. 2021, doi: 10.3390/s21051594.

[34] S. B. Shah, "Advanced Machine Learning Models for Anti-Money Laundering (AML): Improving Detection Accuracy and Efficiency," in *2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC)*, 2025, pp. 1–5. doi: 10.1109/SATC65530.2025.11137255.

[35] M. Clement, "Data Privacy and Ethical Considerations in AI-Powered Fraud Detection for Data Privacy and Ethical Considerations in AI-Powered Fraud Detection for Financial Services," no. July, 2025.

[36] H. Kali, "Optimizing Credit Card Fraud Transactions identification and classification in banking industry Using Machine Learning Algorithms," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 11, pp. 85–96, 2024.

[37] V. Nasteski, "An overview of the supervised machine learning methods," *HORIZONS.B*, 2017, doi: 10.20544/horizons.b.04.1.17.p05.

[38] F. Carcillo, Y. A. Le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, "Combining unsupervised and supervised learning in credit card fraud detection," *Inf. Sci. (Ny).*, 2021, doi: 10.1016/j.ins.2019.05.042.

[39] J. Li, A. Zheng, W. Guo, N. Bandyopadhyay, Y. Zhang, and Q. Wang, "Urban flood risk assessment based on DBSCAN and K-means clustering algorithm," *Geomatics, Nat. Hazards Risk*, vol. 14, no. 1, p., 2023, doi: 10.1080/19475705.2023.2250527.

[40] S. Misra, S. Thakur, M. Ghosh, and S. K. Saha, "An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction," *Procedia Comput. Sci.*, vol. 167, pp. 254–262, 2020, doi: 10.1016/j.procs.2020.03.219.

[41] M. Hejazi and Y. P. Singh, "One-class support vector machines

approach to anomaly detection," *Appl. Artif. Intell.*, vol. 27, no. 5, pp. 351–366, 2013, doi: 10.1080/08839514.2013.785791.

[42] P. Mahesh, S. C. M, P. M, J. K. C, A. R, and K. G, "Credit Card Fraud Detection in Banking Using Machine Learning," in *2025 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI)*, 2025, pp. 1–7. doi: 10.1109/RAEEUCCI63961.2025.11048184.

[43] A. S. Nair, A. Krishna, S. T. Gupta, and S. Susan, "Credit Card Fraud Detection using Soft Voting Ensemble with Imbalance Treatment," in *2025 5th International Conference on Intelligent Technologies (CONIT)*, 2025, pp. 1–5. doi: 10.1109/CONIT65521.2025.11167470.

[44] I. Gupta, R. R. Kumar, D. Muduli, S. Mishra, and S. Parija, "A Machine Learning Approach for Credit Card Fraud Detection using Feature Engineering and Ensemble Models," in *2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3)*, IEEE, Jul. 2025, pp. 1–6. doi: 10.1109/ISAC364032.2025.11156887.

[45] S. Jain, N. Sharma, and M. Kumar, "FraudFort: Harnessing Machine Learning for Credit Card Fraud Detection," in *2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP)*, 2024, pp. 41–46. doi: 10.1109/TIACOMP64125.2024.00017.

[46] I. Vejalla, S. P. Battula, K. Kalluri, and H. K. Kalluri, "Credit Card Fraud Detection Using Machine Learning Techniques," in *2023 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing (PCEMS)*, 2023, pp. 1–4. doi: 10.1109/PCEMS58491.2023.10136040.

[47] D. S. Nijwala, S. Maurya, M. P. Thapliyal, and R. Verma, "Extreme Gradient Boost Classifier based Credit Card Fraud Detection Model," in *2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT)*, 2023, pp. 500–504. doi: 10.1109/DICCT56244.2023.10110188.

[48] A. Singh, A. Singh, A. Aggarwal, and A. Chauhan, "Design and Implementation of Different Machine Learning Algorithms for Credit Card Fraud Detection," in *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 2022, pp. 1–6. doi: 10.1109/ICECCME55909.2022.9988588.

