iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IX **Month of publication:** September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74201

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

Fraud Detection in Financial Transactions: A Survey of Machine Learning Models and their Applications in Credit Card Security

Mohiuddin Ashraf R[1], Mrs. Jennifer Mary S[2]
[1, 2]*Department of MCA Ballari Institute of Technology and Management*

Abstract: ***The rapid explosion in e-transactions has also been accompanied by an equal explosion in credit card fraud (CCF), and this is seriously raising money and security issues with individuals as well as banks. Rule-based anti-fraud solutions are susceptible to failing to recognize advanced fraudulent patterns and thus the requirement to incorporate advanced machine learning (ML) algorithms. This review covers a broad spectrum of supervised and unsupervised learning methods, i.e., AdaBoost, and ensemble methods, in light of their capacity to identify fraudulent transactions. An elaborate discussion of most important F1-score, and AUC is done by utilizing benchmark datasets such as the European Credit Card Dataset. The paper is concentrating on the difficulties in fraud detection within real-world use cases, such as multi-modal class distribution overlap, extremely imbalanced class data, model interpretability, and real-time processing requirements. Ensemble and stacking models were found to perform outstanding accuracy and credibility, while real-time distributed processing design and explainable AI are still central to wider adoption. Deep learning, federated learning, and hybrid blockchain technologies are to increase security, transparency, and scalability. In conclusion, this review discusses the prospects of ML in creating stable, smart, and dynamic CCF detection systems.***

Keywords: CCF Detection, ML, Imbalanced Datasets, Ensemble Models, Explainable AI

I. INTRODUCTION

Internet-based financial transactions have revolutionized payment systems for both urgency and ease of use but increased fraud opportunities as well. In response to this, science has used machine learning and analytics to identify unusual patterns of transactions using statistical methods and visualisation tools [1]. Well-performing approaches such as Random Forest, Logistic Regression, and XGBoost are shown to be highly predictable with Random Forest having high recall, precision, and F1-score on actual data [2]. Feature selection models Pearson Correlation, Information Gain, and Random Forest Importance are shown to increase classification accuracy significantly when they are utilized in combination with ensemble algorithms CatBoost, AdaBoost, and XGBoost [3].

One of the classic issues is that fraud samples are extremely class imbalanced and have a very small number of fraudulent transactions Only this is being addressed by the Credit Card Outlier Detection (CCOD) model, and anomaly-based models like Cluster-Based Local Outlier Factor (CBLOF) and Isolation Forest which obtained high Matthews Correlation Coefficients on European and German datasets [4]. Scalable fraud detection pipelines are also enabled by distributed paradigms like PySpark with XGBoost, and CatBoost implementations whose optimal performance was realized from gradient boosting approaches in skewed scenarios [5]. Specifically, CatBoost and XGBoost registered precision, recall, and F1-measures over 0.999, justifying their applicability and usability to real-time large-scale fraud detection [5].

Current developments focus on scalability, interpretability, and flexibility. IoT-based platforms combine clustering algorithms, support vector machines, and deep neural networks to achieve real-time anomaly detection on large streams of transactions [6]. To explain, for purposes of illustration, Explainable AI methods such as SHAP enable explanation of complex models, with Random Forest analysis identifying transaction value and merchant category as drivers [7]. Hybrid ensembles of SMOTE-ENN with autoencoders and TOPSIS feature extraction and SVM, KNN, and Extreme Learning Machine observed to achieve near-optimal recall and accuracy [8]. Balancing and flexibility issues being overcome, ensemble methods such as SMOTE + ENN improve rarity in fraud detection, opening the door to scalable, interpretable, and hybrid architectures blending AI, IoT, and distributed learning [9].

II. LITERATURE REVIEW

Fraudulent financial transactions are analyzed starting with the examination of transaction data through statistical measures of minimum, maximum, and standard deviation. ML models such as LightGBM, AdaBoost, widely utilized to measure performance in identifying fraud. Comparison showed that AdaBoost gave the best accuracy (0.9613) and recall (0.889) and the best precision (0.986) was given by LightGBM. Random Forest was, however, computationally most effective execution time. There are unique strengths of each algorithm, model selection, in the end, system's particular priorities for fraud detection, e.g., precision, recall, or efficiency [1].

The US financial system is disapproving of fraud detection requirements, where rule-based systems fail in the face of fast-changing fraud schemes. Supervised and unsupervised ML methods have been tried in response. Logistic Regression, Random Forest, and XGBoost models have proved to be useful, with Random Forest having performed consistently in balancing precision, recall, and F1-score. ML augmented by real-time tracking is becoming a breakthrough in facilitating real-time fraud prevention. Techniques based on deep learning such as RNNs and CNNs with vision for the future are likely to capture subtle temporal and spatial patterns in transactional behavior, whereas blockchain and AI-based authentication will be the means to greater transparency and security of electronic payments [2].

The greatest challenge in detecting fraud is that the highly imbalanced nature of transaction data where the fraud transactions are an infinitesimal minority subset. In attempting to overcome this, researchers proposed a feature selection framework that is an aggregation of Pearson Correlation, Information Gain (IG), and Random Forest Importance (RFI) to select the most salient features for model training. This combination of the ensemble method and the cutting-edge algorithms like Random Forest, Extra Trees, CatBoost, AdaBoost, and XGBoost was used on five databases. The performance was found to be higher than the standard classifiers. The platform's flexibility makes it adequate for practical applications. Future research includes expansion of research on CNNs, RNNs, and Transformer models and anomaly detection with the help of autoencoders and GANs against imbalance. Privacy-preserving and secure collaborative fraud model between institutions [3].

Also exacerbated by issues such as class distribution overlap and class imbalance. The Credit Card Anomaly Detection (CCAD) model mitigated such issues through anomaly detection methods such as CBLOF and Isolation Forest with MCC scores of 0.95 and 0.97 on European and German databases, respectively. These results show the strength of ensemble learning and density-based approaches for multi-modal anomaly detection. For now, ensemble algorithms like XGBoost, CatBoost, and Random Forest are still in first place as they are able to easily avoid overfitting and imbalance. CatBoost even outperformed XGBoost in terms of precision and calibration because CatBoost is ordered boosting-friendly and is able to easily deal with categorical features [4][5].

As the number of IoT-based banks is on the rise, fraud detection systems also extensively employ advanced ML. Research evidence suggests that collective models like GBM and Random Forest work best in contrast to others in real-time detection of advanced frauds. Transaction location and chip-supported usage by IoT are characteristics that improve anomaly detection, and cloud infrastructure that is scalable has potential in real-time processing [6]. Parallelly, Explainable Artificial Intelligence (XAI) techniques like SHAP have been employed to embed inside Random Forest models so that fraud models can be explained and management and regulatory requirements fulfilled [7]. Some of the other advancements are SMOTE-ENN, autoencoders, TOPSIS feature selection, and Particle Swarm Optimization for ensemble optimization. Performance, over 99.9% precision, recall, and accuracy, and represent a step towards deployment in real-world applications in real-time financial environments. Techniques on other domains like insurance and healthcare fraud detection and create more robustness against adversarial attacks [8].

III. ML IN FRAUD DETECTION

A. *Architecture of ML-based Fraud Detection Approach*

Figure 1 represents a typical block diagram of the end-to-end process widely used in ML-based credit card fraud (CCF) detection systems. The process is initiated by data acquisition from transactional databases, followed by normalization and class balancing as preprocessing techniques to address imbalances in the data. Such as Logistic Regression, Random Forest, a training and classification. Evaluated against supreme F1-score, and ROC-AUC to analyze their fraudulent transaction detection capability.

B. *XG-Boost Classifier Modelling*

In this project, Python scripts were employed to develop and test an XGBoost classifier with our own function specification, train_and_evaluate_model, having the model built with label encoding turned off (use_label_encoder=False), metric set as log loss, and a particular random state for purposes of reproducibility. With XGBoost, six other ML classifiers namely, Random Forest (RF), Extra Trees (ET), AdaBoost, CatBoost, and an ensemble voting method were tried with five varying datasets for ensuring the

efficacy of the method, with oversampling techniques such as SMOTE, SMOTE-ENN, and ADASYN resolving extreme class imbalance [1][2]. Results indicated that Extra Trees consistently performed better, with 99.97% using SMOTE and 99.96% using SMOTE-ENN, while the highest AUC (98.72%) and MCC (89.99%) were recorded using the ADASYN-ET combination, which highlights its fraud-detecting capability [3]. Support outlier detection algorithms, Angle-Based Outlier Detection (ABOD), Cluster-Based Outlier Detection (COPOD), and Elliptic Envelope (ECOD), complemented anomaly detection, while baseline models like Logistic Regression offered interpretability. More sophisticated ensemble approaches such as Random Forest and XGBoost enhanced generalization, but CatBoost, hyperparameterized boosting, beat even XGBoost on accuracy and calibration [4][5]. Outside of tree-like algorithms, Gradient Boosting Machine (GBM) and Neural Networks also showed evidence of capacity for learning non-linear relationships in transactional data, with hypertuned also enhancing predictive performance using hyperparameterized forms [6]. In addition, interpretability remained important, as Logistic Regression and Decision Trees provided clear-cut decision paths, whereas advanced classifiers such as SVM and KNN provided boundary-based and distance-based insights. For solving convergence and scalability issues, Extreme Learning Machine (ELM) was an efficient and speedy solution for hyperparameter tuning, which controlled global and local search parameters adaptively to avoid overfitting in fraud detection tasks with class imbalance [7][8].

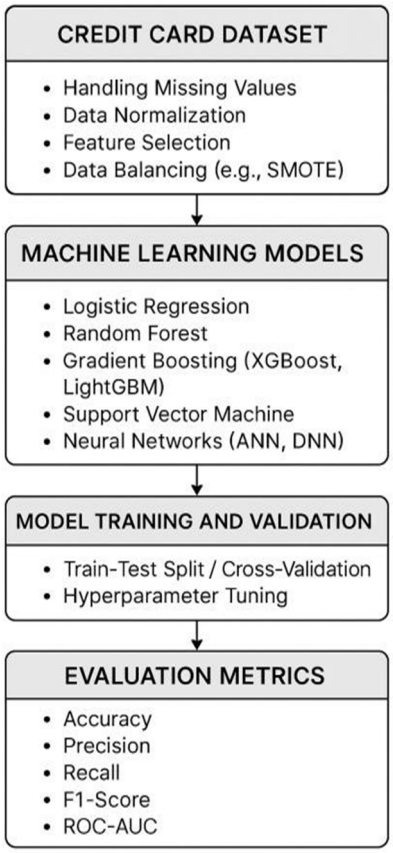


Figure 1: Block diagram illustrating the standard pipeline for CCF detection using ML models. It highlights the sequential stages from data preprocessing to evaluation, covering model types and performance metrics

C. Credit Card Dataset Fraud Detection

The European Credit Card Dataset, widely used in fraud detection research, contains 284,807 transactions over two days in September 2013, with only 492 fraud cases (0.17%). It includes 30 features—28 anonymized via PCA, plus transaction amount and time—ensuring privacy while enabling pattern extraction. Due to its severe class imbalance, this dataset serves as a benchmark for evaluating ML models in realistic fraud detection scenarios [2-9].

IV. EXISTING METHODS RESULTS

Table 1 depicts the existing ML model results with the different performance metrics.

Table 1: Existing published ML models with performance metrics.

Cite & Year	Methods	Precision	Accuracy	F1-Score	Recall	AUC
[2] 2025	XG-Boost	0.99	0.87	0.93	0.88	–
[3] 2025	Extra Trees (ET)	0.93	0.99	0.89	0.86	0.98
[4] 2025	CBLOF	0.97	0.97	0.97	0.97	0.489
[5] 2025	Logistic Regression	0.96	0.96	0.96	0.96	–
[6] 2025	Neural Network (MLP)	0.99	0.99	0.99	0.98	–
[7] 2025	Random Forest	–	0.99	0.99	–	–
[8] 2025	Stacking Ensemble	0.99	0.99	0.99	0.99	1
[9] 2025	SMOTE + ENN	0.99	0.99	1	0.99	–

V. CHALLENGES AND LIMITATIONS

Based on the extensive survey, we have identified the following limitations and challenges:

A. Limitations

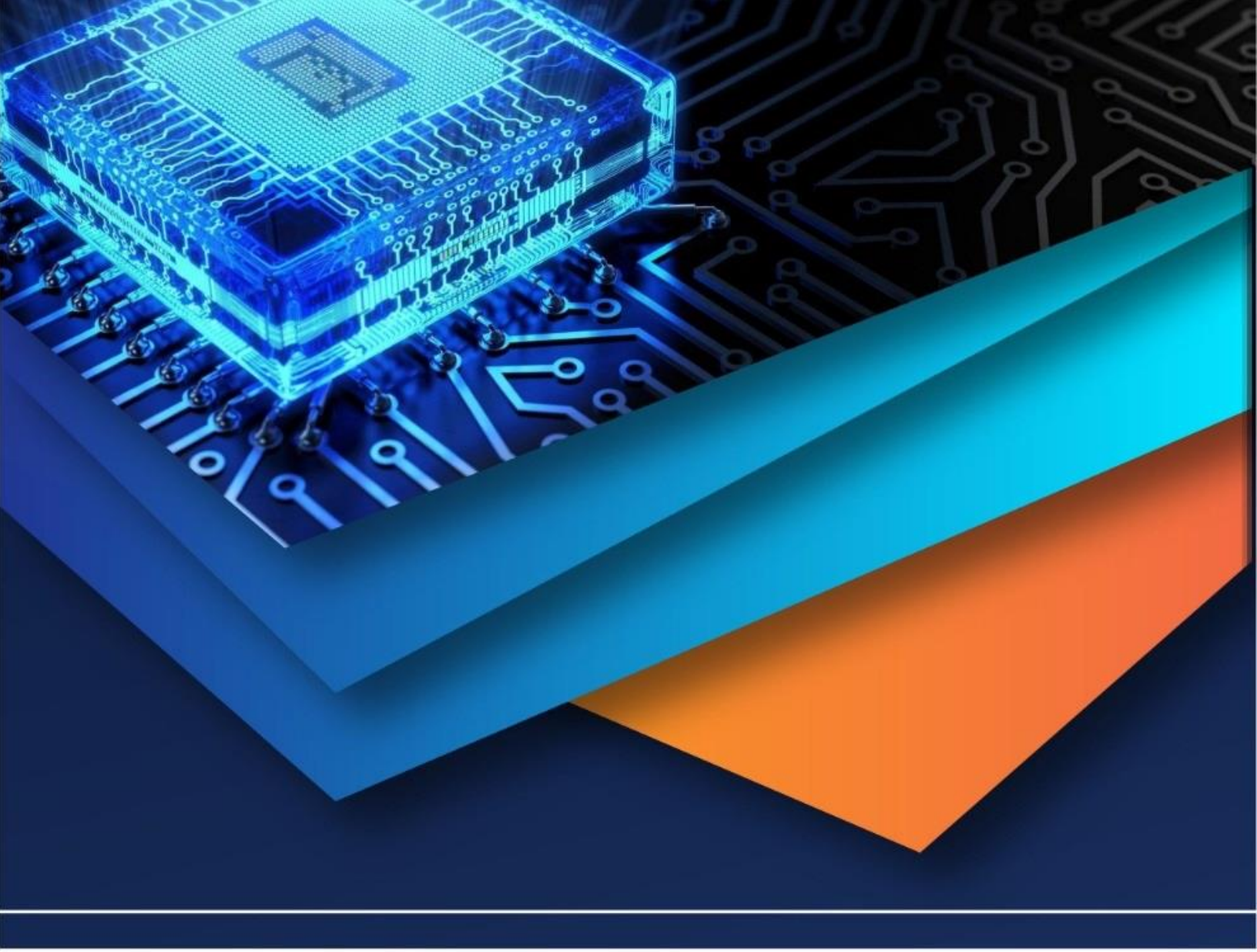
Even with ML advances in CCF detection, there are some problems. Real-world data sets are plagued by extreme class imbalance towards over-representation of majority classes and under-detection of fraudulent classes. Approaches to balancing like SMOTE and SMOTE-ENN work but have the tendency of adding noise or overfitting. More advanced Boosting, and lower interpretability, making it difficult for them to be adopted in regulated sectors where transparency is desired. Overfitting persists, particularly for small or non-sampled datasets, and even state-of-the-art models like CatBoost and XGBoost lose generalizability fraudulent patterns not seen before.

VI. CONCLUSIONS

ML algorithms and ensemble models have brought detection of CCF to high accuracy and recall. Overfitting, class imbalance, and lack of interpretability are the primary concerns. Deep learning big-data frameworks such as PySpark, and Explainable AI need to researches towards explainability. Federated Learning and blockchain-based authentication can improve security, while applying these solutions to areas such as insurance and health can facilitate effective cross-domain fraud prevention.

REFERENCES

[1] Sellam, V., Tushar, P., Rohit, G. and Sanyam, S., 2025. Credit card fraud detection using ML. Journal of Computer Graphics and Multimedia Applications, p.1.
[2] Sizan, M.M.H., Chouksey, A., Tannier, N.R., Al, M.A., Jobaer, J.A., Roy, A., Ridoy, M.H., Sartaz, M.S. and Aminul, D., 2025. Advanced ML Approaches for Credit Card Fraud Detection in the USA: A Comprehensive Analysis. Journal of Ecohumanism, 4(2), pp.883-905.
[3] Siam, A.M., Bhowmik, P. and Uddin, M.P., 2025. Hybrid feature selection framework for enhanced credit card fraud detection using ML models. PloS one, 20(7), p.e0326975.
[4] Chugh, B., Malik, N., Gupta, D. and Alkahtani, B.S., 2025. A probabilistic approach driven credit card anomaly detection with CBLOF and isolation forest models. Alexandria Engineering Journal, 114, pp.231-242.
[5] Theodorakopoulos, L., Theodoropoulou, A., Tsimakis, A. and Halkiopoulos, C., 2025. Big data-driven distributed ML for scalable credit card fraud detection using PySpark, XGBoost, and CatBoost. Electronics, 14(9), p.1754.
[6] Alatawi, M.N., 2025. Detection of fraud in IoT based credit card collected dataset using ML. ML with Applications, 19, p.100603.
[7] Muksalmina, M., Syahyana, A., Hidayatullah, F., Idroes, G.M. and Noviandy, T.R., 2025. Credit Card Fraud Detection Through Explainable Artificial Intelligence for Managerial Oversight. Indatu Journal of Management and Accounting, 3(1), pp.17-28.
[8] Gupta, R.K., Hassan, A., Majhi, S.K., Parveen, N., Zamani, A.T., Anitha, R., Ojha, B., Singh, A.K. and Muduli, D., 2025. Enhanced framework for credit card fraud detection using robust feature selection and a stacking ensemble model approach. Results in Engineering, p.105084.
[9] Ahmed, K.H., Axelsson, S., Li, Y. and Sagheer, A.M., 2025. A Credit Card Fraud Detection Approach Based on Ensemble ML Classifier with Hybrid Data Sampling. ML with Applications, p.100675.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY