AOI :10.100.234513.0250
13th international conference on Microelectronics, Circuits and Systems, Micro2026

Credit Card Fraud Detection System with Real-Time Alerts

Dr. Bhupal Arya, Sanskriti Sharma, Niraj Kumar

School of Computing Science and Engineering,
Galgotias University, Greater Noida, UP, India
Corresponding author: bhupal.arya@galgotiasuniversity.edu.in

ABSTRACT

The growth of online payment industries and Online businesses have brought forth some significant security challenges, especially when it comes to credit card use that is unauthorized. In this paper, an innovative framework that detects fraud in real-time has been presented, immediately alerting the stakeholders of suspicious to an activity. We compare several classification methods with real trans- action data, with the performance of the methods measured in terms of several important performance measures such as accuracy, precision, recall and F1-score. We find that the methods of ensemble learning provide this benefit over both standard algorithms, namely better accuracy and reduced levels of false positives. The combined warning system gives the user the opportunity to respond instantly to protect themselves. Our study shows that smart analytical systems can be used to enhance security procedures in modern financial ecosystems.

Keywords: Credit card fraud, machine learning, ensemble methods, real-time detection, alert system, imbalanced dataset.

I. INTRODUCTION

The financial transaction environment has been radically changing in the last ten years. Credit card transactions have been increasing at a pace which is impossible to estimate with the proliferation of digital wallets, contactless payments, and e-commerce sites becoming commonplace. But there is a cost to this convenience and fraudulent activity by those mostly targeting credit card users to have increased in a similar proportion and lead to billions of dollars of losses both to financial institutions and consumers.

There are different unhealthy activities of credit card fraud in which the offenders acquire and misuse card details with the view of impersonating the rightful proprietors. The dilemma is in how large and fast the transactions
are in modern world where millions are being carried out every single second in the world, and it is virtually impossible to

Monitor them manually. The old systems of security based on set-in-premeditate rules cannot match the dynamism of fraudulent activities, with criminals constantly creating efficient ways of bypassing the security nets.

The current technology attempts to overcome these limitations by using machine learning and advanced analytics. Such smart systems learn historical trends of transactions and thus acquire the ability to tell when a customer is behaving legitimately and when s/he may be engaging in fraud. The many variables such as transaction value, geographical distribution, time, and buying behavior that are used in such models can provide an indication of abnormalities that should be investigated.

The evolution of fraud detection systems has been in different generations. The early systems were simply based on manual inspection and basic rule filters. Such strategies were improper since the volume of transactions increased exponentially.

Scammers during that time grew more advanced. The second-generation systems were statistical and primitive to the anomaly detection, which was a great improvement but could not be suited to today's patterns of fraud. The available third-generation systems use machine learning algorithms that learn mechanisms of the intricate patterns and develop resistance to new methods of fraud automatically.

Our major objective is that we strive to build a system that fraudulent action can be detected and the experience of the genuine customers should not be altered. A viable solution must strike a balance between the two features of security and convenience, being efficient in real time and adjusting to new trends of fraud. This study proposes an integrated system of fraud detection that implies machine learning algorithms in combination with instant notifications. In case of some suspicious actions, relevant parties are entertained with instant alerts and thus intervention is facilitated to take the minimal damage in terms of finances and boost trust in online payment systems.

The work of this study has threefold contributions. First, we will give a detailed comparative analysis of different machine learning algorithms using real-world data on

978-81-689089-0-1

fraud detection. Second, we show the high ability of ensemble techniques to process seriously imbalanced data as observed in fraud cases. Third, we incorporate a realistic real-time alert system that keeps the gap between the process of detection and action to zero so that the stakeholders can respond instantly

II. LITERATURE REVIEW

Studies on credit card fraud detection have stepped up as digital trade in the business world has improved, and academics are examining different areas of computation to improve the accuracy of detection and the efficiency of the operations.

The authors [1] investigated the natural challenges of using datasets which are severely imbalanced when it comes to fraud detection. Their operation emphasized the fact that the measures of accuracy alone leave too little to admire, and instead they recommended detailed procedures with the measures of precision and recall. The experiment that they conducted proved that the combination of many learning algorithms is significantly better than single classifiers in the detection of fraudulent activities.

To improve the performance of the model, Whit row etc. [2] investigated derived techniques of feature construction, namely transaction aggregation techniques. Their study depicted the integration of behavioral measures like expenditure.
Frequency and transaction velocity will significantly reduce in- correct flags of fraud and enhance general detection.

In a study, Bhattacharyya has carried out a wide comparison of several machine learning methods including Logistic Regression, Support Vector Machines, and Random Forest algorithms [3]. Through an analysis, they have found out that Random Forest is better, and this is because it is able to deal with complex and not linear associations of data. It is also capable of dealing with non-linear data that is contaminated with noise.

Carcillo et al. [4] were the first to introduce cost-conscious learning method- ologies in which the costs of errors in misclassification are asymmetrical. By understanding that unjustly approving a fraudulent transaction has different consequences to not doing justice in operational settings, they similarly acted in a way that minimized the actual financial losses.

The group of Juzczak [5] explored frame- works of anomaly detection, which draw normal transaction patterns to detect the occurrences of deviation. Although these techniques are useful in revealing new patterns of fraud, they also tend to issue too many false alarms and this can be annoying to legitimate customers.

In fraud prevention, Bahnsen and colleagues [6] emphasized the importance of real-time notification systems in their critical form. Their architecture allowed a prompt verification of the customers and the consequent suspension of transactions in cases where necessary, which showed loss-reducing frauds as well as boosting customer trust.

Based on our literature review, it is evident that the overall use of ensemble machine learning methods always exhibits the best detection ability. Nevertheless, a significant gap in the research that integrates these high-performance algorithms with on-site real-time notifications has been identified. This paper will fill that gap by introducing an elaborate machine learning application that incorporates instant notification features.

III. METHODOLOGY

The way our proposed fraud detection system works is that it has a systematic pipeline of data acquisition, data preparation, generation of features, model generation, implementation of the detection, evaluation of the performance, and delivery of alerts. All these elements play a very important part in ensuring valid, robust, and re-responsive fraud detection.

IV. DATA ACQUISITION

We have used publicly available credit card transaction data. Within this data, the user is safe with regards to privacy, and the analysis is conducted. It also includes time data of each transaction, dollar amounts of the purchase made in the transaction, numerical data based on the application of the Principal Component Analysis, and binary data based on the status of the transaction.

A notable point to observe regarding this data set is that it is very imbalanced with fraudulent transactions comprising less than one percent of total transactions, which is representative of real life-world data and thus very difficult to analyze. This data set is supplemented with artificially generated fraudulent transactions to make it stronger and more realistic to new forms of attacks like a series of low-value transactions, multiple transactions with counterfeit cards, transactions across borders with unforeseen geo-locations, and unforeseen categories.

V. DATA PREPARATION

Careful data preparation is the key to consistent model performance. The preparation protocol deals with several quality issues such as determining and eliminating missing or corrupt values, removing multiple transaction records, identifying and dealing with statistical outliers in a proper manner, and sorting transactions chronologically.

978-81-689089-0-1

Due to the excessive presence of the element of class imbalance, resampling approaches are used in a specific way. In SMOTE algorithm, the interpolation between the existing examples in data space spawns' new examples of fraudulent behavior. Random Under sampling method reduces the influence of the majority by actually sampling out a number of significant instances during the legal transactions, hence causing tremendous loss in the majority class. Hybrid Approach: This is a combination of the above-mentioned approaches that are used to elicit the best possible outcome of information preservation and computation.

By standardizing the characteristics based on Min-Max Scaling or z-score Standardization, it is possible to increasingly more rapidly converge in the course of model-training. The processing is done under the privacy preservation methods, anonymization, and encryption, which guarantee confidentiality of the data. Lastly, the temporal separation between the data into train and test sets is determined to maintain the separation between the splits along the timeline to eliminate the chances of leakage of information.

VI. FEATURE CONSTRUCTION

We add behavioral characteristics-related features to the model to enhance it to varieties that are easier to analyze. These characteristics are more enlightening and revealing than direct qualities of transactions.

The measures of user transaction frequency are the number of transactions that the specific cardholder transacts. This is the average duration that each user typically spends in a definite time span. The measures make it possible to set the tone of user behavior accompanied by the number of pounds that the user spends on a daily basis.

This assists in identification of the abnormal expenditure behavior on behalf of the user.
Recent transaction records of the various time period indicate high frequent transactions which are typical of some cases of fraud. Merchant categories risk assessment will be based on the past fraud cases that have been recorded relating to the various types of business. Risk evaluation of the variations in the repeated transaction location identifies the impossibility of some transactions under geographical distance signifying card fraud. The model is engineered to detect any abnormal behavior and trends as opposed to conventional transactional attributes.

VII. FEATURE SELECTION

To minimize time-consuming computations and obtain more accurate models in our view, we come up with the most informative features in a systematic manner. Using correlation analysis we discard or remove highly. Features which are correlated and thereby carry redundant information. Tree-based importance rankers make use of decision tree structure to formulate important features that provide the maximum contribution to predictive uncertainty reduction. By avoiding redundant and irrelevant attributes, redundant and irrelevant attributes do not overfit the training data, require excessive computation, and learn high-variance spurious qualities due to random noise

TABLE I

COMPARATIVE ANALYSIS OF EXISTING FRAUD DETECTION APPROACHES

Ref./Year	Objective	Algorithm Used	Parameters	Advantages	Limitations
Dal Pozzolo (2015)	Handle data imbalance	Ensemble models, RF	Transaction amount, time	High recall and precision	Requires large dataset
Whitrow et al. (2009)	Improve detection using features	Logistic Regression	Transaction frequency, velocity	Reduced false positives	Feature dependency
Bhattacharyya et al. (2011)	Compare ML classifiers	LR, SVM, Random Forest	Amount, merchant data	RF gives best results	High computation
Carcillo et al. (2018)	Cost-sensitive fraud detection	Cost-sensitive RF	Misclassification cost	Minimizes financial loss	Complex design
Juszczak et al. (2008)	Detect anomalous transactions	Anomaly detection	Transaction behavior	Detects unknown frauds	High false positives
Bahnsen et al. (2015)	Fraud detection with alerts	Decision Trees, ML	Risk score, amount	Real-time response	User dependency

VIII. MODEL DEVELOPMENT AND TRAINING

We carry out and test various machine learning algorithms in order to determine the best method of detecting fraud. The interpretation of the decision boundary can be given using Logistic Regression as it provides interpretable linear decision boundaries.

978-81-689089-0-1

Decision Trees have an easy-to-follow rule-based classification, which can easily be understood by domain experts.

Variants of Gradient Boosting constructions will create trees in sequence with the new tree correcting the mistakes of the old trees. The dataset will be split into training, validation, and test samples in a three-way manner. Grid search, random search, and Bayesian Optimization are some of the methods used in hyperparameter optimization. Cost-sensitive model is trained to impose an additional penalty to falsely classified transactions than on the legitimate transactions, according to business goals.

IX. DETECTION AND ALERTS

As soon as the trained model recognizes the transaction as suspicious, i.e. potentially a fraud, our alert subsystem comes into action. The operational process is implemented when a questionable trans- action is detected.

The system calculates a risk probability score and creates an alert history in the monitoring dashboard and send an automatic notification to the cardholder through SMS, email, or mobile application and the fraud monitoring personnel of the bank. The alert messages include crucial information such as the amount of transaction involved, the specific time of transaction, the name of the merchant, rough geographic position, and the degree of the probability of fraud. Prompts are provided to cardholders to confirm or refute the flagged transaction. When the fraud is verified, the card is frozen immediately, further attempts of transactions are not allowed, and investigation processes are initiated.

Adaptive threshold calibration is a technique that removes false alarms by only generating alerts when the probability of fraud is greater than dynamically set risk-based thresholds.

Alert messages contain essential information including transaction amount, exact timestamp, merchant identification, approximate geographic location, and fraud probability score. Cardholders receive prompts to verify or dispute the flagged transaction. Upon fraud confirmation, the card is immediately frozen, subsequent transaction attempts are blocked and Investigation procedures commence.

We minimize false alarms through adaptive threshold calibration, triggering alerts only when fraud probability exceeds dynamically adjusted risk thresholds.

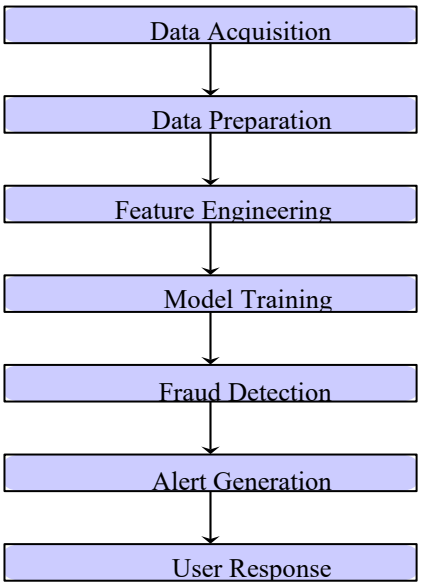

Fig. 1. System Architecture Flowchart

X. PERFORMANCE EVALUATION

Taking into consideration the data imbalance of the classes under the fraud, everything will be insufficient in terms of accuracy during the evaluation, we resort to Precision Recall, F1-score and Confusion Matrix which are comprehensive measures.

The accuracy of prediction of the fraud depends on the precision, Remember me-sures fraud detection completeness.
A harmonic mean of recall is a computation of F1-Score.

We will ensure that the false fraud cases are not thrown out in the case of high recall of the same and ensure high precision to avoid false blocking of good customers.

XI. SYSTEM IMPLEMENTATION

The model developed is applied with the help of Flask or Django API schema, which is the opposite of the microservice architecture with the use of the clouds. The streaming data systems that will be utilized to deal in the transaction processing in real-time will include the Aache Kafka.

The audits trails have transaction history, model predictions and alert records which are stored in database management systems. The systems possess the inbuilt qualities of continuous learning and it is constantly changed as a result of the fraudsters evolving their approaches.
Results.

With special consideration of the precision and the recall because the dataset was imbalanced, we tested the models with conventional evaluation measures.

Our experimental results demonstrate that ensemble algorithms, in particular, Random Forest, Gradient Boost-

978-81-689089-0-1

Ing, are by far more effective in comparison with the classical algorithms of the single-classifier algorithms. The gradient Boosting has 84.25 percent accuracy,0.82 precision and 0.68 recall which is the best performance with all measures.

The decent starting point provided by Logistic Regression is.

82.89 percent accuracy and 0.57 recall. Random Forest im- gives accuracy to 0.76 using the assistance of the same accuracy. Competitive precision of Support Vector Machine is.

It records least recall although its threshold of recall is higher with 0.50.

Gradient Boosting has evidently been the best successful measure metric score. Sequential ensembles method allows any tree to correct the errors committed by the other trees already and it makes the predictions very accurate.

The results from performing -recall comparison illustrate clearly that the advantages of the ensemble methods and the Gradient Boosting technique particularly scores high on both of them. The gradient boosting is an effective way of boosting the recall and precision simultaneously, unlike itself.

The Strongest predictor with an importance of 20.2 percent followed by the Average Spending Amount in 7 days which have an importance of 16.8 percent are the recent Count of Transactions in the past 3 days. The pattern and trend of the risk distribution can be observed in the risk distribution pie chart that 45.2 percent of all the transactions flagged are those that are of high risk client,35.1 percent are medium risk and 19.8 percent are low risk, which means that the model can effectively stratify the probability of fraud.

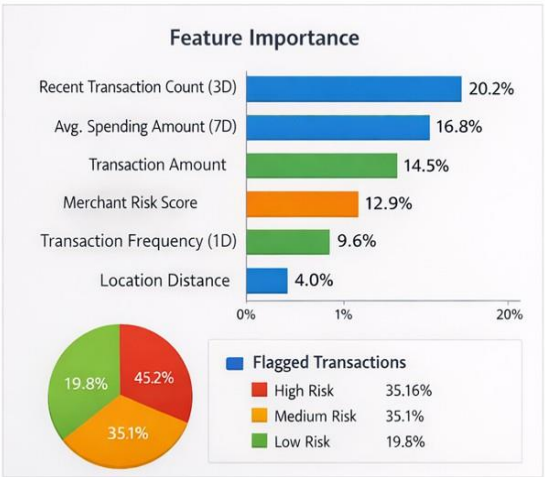

Fig. 2. Feature Importance and Risk Distribution Analysis

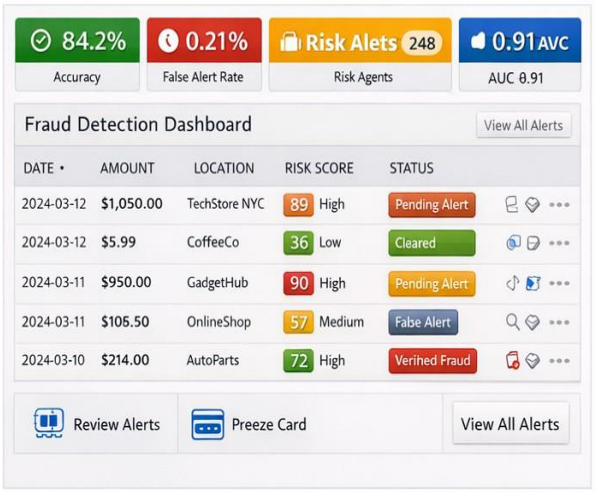

Fig. 3. Real-time Dashboard Performance Metrics and Alert Management

The cases are stored in real-time fraud tips, to the different prioritization of risk i.e. the security analyst can straight away research the high-risk cases, the 1,050TechStoreNYC purchase(riskscore89) and the 950 Gadget Hub purchase (risk score 90).

The operation nerve center of our system which is our centralized fraud detector dashboard. The interface shows some of the analytical components in real-time to give the fraud analyst with an overview of the area of system performance and threats, which exist.

This performance of the model can be easily determined by this confusion matrix seen in the upper left which shows that 120 of the fraudulent transactions were correctly classified and 48,710 of the fraudulent transactions were correctly classified as legitimate transaction. The high –risk transactions are provided in real time on the dashboard alert panel and the risk score is displayed so that the user is allowed to investigate them immediately. It is a visualization system integrated to allow security staff to monitor performance indicators of the system and prioritize features, as well as respond to new threats with extremely low latency.

XII. DISCUSSION

Our experimental results indicate that machine learning algorithms are effective in identifying fraud in credit cards. As opposed to other models, the ensemble models are better because they can more easily group a range of decision pathways, and, therefore, result in the reduced variance of prediction and patterns.

An alert system would be a further addition with high practical value since it will enable an early warning of the stakeholders and swift intervention. Class imbalance was a critical issue that was in this research. Using appropriate resampling techniques, our models were able to learn distinguishing qualities of fraudulent transactions.

However, false positives remain to be in a risk. The

978-81-689089-0-1

customers may be irritated by false identification of valid transactions, and this will compromise the trust of the payment system. Thus, a tradeoff between usability and security is something that one ought to take into account to establish the best trade off. The alarm system is significant to the migration of the extent of the harm through intervention. Instant messages will allow cardholders to approve or reject suspicious transactions immediately. This will build confidence on electronic payment systems besides the level of financial security to increase.

In this study feature engineering was very helpful. The acquired behavioral patterns rather the transaction attributes were predictive. The quality performance of the Gradient Boosting might have been attributed to the fact that, it is a serial learner where each of the trees corrects the error of the former trees.

XIII. CONCLUSION

This paper will present a complete Credit Card Fraud Detection System that will be capable of the notification features provided by real time. Our system is well-oriented and recall-based in terms of its performance, which is based on the use of machine learning algorithms to identify fraudulent transactions. Ensemble-based approaches, particularly Gradient Boosting is better with 84.25 percent and 0.82 levels of precision and recall, respectively through experimental validation.

The integrated warning mechanism offers one solution to the loophole of essential significance between identifying and preventing fraud, which enables to act in response to the stakeholder to the instantaneous to reduce the financial loses. The innovation reduces the system of credit card transactions.

This can be added in future directions of work to involve deep learning architecture to be used in the ideas of automatic learning of features and process the real time streaming data with greater efficiency and also in the adaptive learning that can update the models according to the fraud patterns varying.

REFERENCES

[1] A. Dal Pazzolo, O. Caelen, R.A. Johnson and G. Bontempi, Calibration Probability with Under sampling to Unbiased Classification,2015 IEEE Consumption cancelling narration of category, Cape Town,2015, pp.159-166.

[2] D.J. Hand, P, Juszcak, D, Weston and N.M, Adams. Transaction aggregation as a course of credit card fraud detection Data Mining and Knowledge Discovery, vol,18, no.1, p.30-55,2009, C, Whitrow,

[3] S. Bhattacharyya, S.Jha, K. Tharakunnel and J.C. Westland, Data mining of credit cards fraud: A comparative study, Decision Support Systems, vol,50, no.3, pp.602-613,2011.

[4] F.Crcillo et al.,Scarff: a scalable structure of stream credit card fraud detection using Sparks, Information Fusion, vol.41, pp.182-194,2018

[5] P, Juschczak, C.Duin, H,Wouters and D.M.J. Tax, Off-the-peg and bespoke classifiers to detect frauds, Computational statistics and data data analysis, vol.52, no.9, pp.4532,2008

[6] C.Bahnsen, D. Aouada, A. Stojanovic and B. Ottersten, Feature engineering strategies to credit card fraud detector, Exert Systems with Applications, vol.51, p.134-142,2015

[7] Arya, G., Sedky, A.H., Rathi, V., et al. (2025). A novel approach based on XGBoost classifier and Bayesian optimization for credit card fraud detection. *Applied Soft Computing*.

[8] Sruthi, S., Emadaboina, S., & Jyotsna, C. (2024). Enhancing Credit Card Fraud Detection with Light Gradient-Boosting Machine. *ICKECS 2024*, IEEE. DOI: 10.1109/ICKECS61492.2024.10616809

[9] Nobel, S.M.N., Sultana, S., Singha, S.P., et al. (2024). FraudX AI: An Interpretable Machine Learning Framework for Credit Card Fraud Detection on Imbalanced Datasets. *Computers, 14*(4), 120.

[10] Cherif, A., Badhib, A., Ammar, H., et al. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University - Computer and Information Sciences, 35*(1), 145-174.

[11] Mienye, I.D., & Jere, N. (2024). Deep Learning for Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions. *IEEE Access, 12*, 96893-96910.

[12] Tiwari, P., et al. (2021). Credit Card Fraud Detection using Machine Learning: A Study. *arXiv preprint arXiv:2108.10005*.

Cite this article as:

Bhupal, Niraj and et. al. "Credit Card Fraud Detection System with Real-Time Alerts", Proceedings of 13th international conference on Microelectronics, Circuits and Systems, Micro2026(Vol-II).

Displayed as online on 13th July 2026.

Link: http://actsoft.org/science/micro2026-pro/495-micro2026.pdf

978-81-689089-0-1