International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

NC021 CREDIT CARD FRAUD DETECTION USING ML

Bhoomika H M
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
bhoomikamca2025@gmail.com

Ashok B P
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
Ashokbpmca82@gmail.com

ABSTRACT

The recent surge of online purchases via credit cards has become a major challenge to the financial institutions and consumers due to the heightened evil of credit card frauds. The rule-based systems, which are traditional, cannot be sufficient, because fraudsters always tweak their game toward the bypassing of predetermined checks. To avoid these shortcomings, this study examines the use of the machine learning method to detect credit card fraud. The article also focuses on supervised and unsupervised models that could be used to consume the huge amount of transactional data to detect abnormal usages of spending, unusual locations, or less frequent transactional data. By training models on historical datasets, both of the fraudulent and real transactions, the system emerges to learn complicated patterns which are hard to curate using manual processes. In addition, feature engineering and dimensionality reduction are also implemented to increase the performance of models and lower complexity levels. The experiments that are presented demonstrate that machine learning algorithm.

KEYWORDS: *Diabetes risk assessment, Hypertension, Blood glucose level, BMI, Early detection.*

INTRODUCTION

Credit cards has become one of the most convenient and universal tools of conducting transactions in case of financial transactions in the new digital economy. The facility to buy products there and then through the online environment and the offline one has fueled a stroke phenomenon of transactions yet also on the same hand, has led to a breeding ground of frauds. Not only does credit card fraud entail a huge loss of money, banks and the individuals who are attempting to carry out on-net monetary transactions, but it also corrupts the

entire system and the belief in the system of people. The growing complexities of perpetrators of such offences are placing the traditional rules-based engines in a difficult position of detecting suspicious transactions effectively as these systems do not tend to recognize the nature of newly evolving patterns of frauds.The data-driven solution to this problem has been the capability of machine designs and as the machine learns the behavioural patterns to differentiate between genuine and fraudulent transactions. The more historic data the models are given. Supervised learning coupled with unsupervised learning like anomaly detection in classifications, clustering has also been put under considerable application in the construction of learning intelligent fraud detection systems to allow a low false positive rate and very high accuracies in the detection systems.

LITERATURE SURVEY

This issue on credit card fraud has attracted the research attention of its growing effects on the financial courts and also to the customers. However, in the decades which followed, those in the field discovered many other ways of maximizing the impact of accuracy of detection including the more conservative use of rules-based systems, but also more advanced systems of machine learning. The first detection systems relied on setting limits manually, such as transaction value, geographic locations, or times of unusually high usage. These systems have their flaws. Their performance often struggles to keep up with new and evolving fraud schemes, resulting in a high rate of false positives. As data mining and machine learning improved, researchers began to use predictive modeling for fraud detection. Transactions are classified as genuine or fraudulent using methods like Logistic Regression, Decision Trees, and Support Vector Machines. These techniques produced good results by identifying non-linear relationships in the data. The Gradient Boosting and Random Forest methods showed promise for better detection rates due to their high accuracy and ability to work with imbalanced data sets. Supervised learning methods also do not excel at identifying patterns of fraud that are new or previously unknown.

EXISTING WORK

This issue of credit card fraud has attracted a lot of research since its rising influence in the financial institutions and the customers. The decades that followed saw a multiplicity of

methods to optimize the accuracy of detection with the most common being the rule based systems and more so machine learning systems. The detection systems were more reliant on manually established limits e.g. transaction value, geographical framework or time of excessive use. These approaches were not very effective but they had weaknesses. They were unable to integrate with new and adaptive fraudulent methods and thus false alerts continued to take place. During the wide usage of data mining and machine learning, researchers could classify the prediction of fraud through predictive modeling. Typical algorithms are Logistic Regression, Decision Trees and the Support Vector Machine, all of which must be trained with (authentic, fraudulent) data. The techniques yielded robust results due to the fact that they detected non-linear trends in the transactional data. The algorithms Random Forest and Gradient Boosting also worked well at increasing detection. They exploited the advantages of ensemble learning that exhibited high accuracy and did a good job on imbalanced data sets.

PROPOSED SYSTEM

In this system is based on the necessity to create an intelligent, adapting, real time system that could be able detect a fraction. As opposed to formalising tables with fixed thresholds, this system relies on data-driven methods, which can adapt to all new fraud patterns and can be responsive to unusual events in a highly sensitive way. The process starts with data pre-processing and cleaning in which massive amounts of transactional data are normalised, converted and cleaned up to fill in the gaps in values, duplicated values and noisy values. Given the levels of such minor portions of actual transactions with the objective of conducting illegitimate transactions, the proportions are leveled out by the methodologies such as the SMOTE or the cost-sensitive learning.In this case, since it is a domain-specific problem, feature engineering is important, and the following segments include the frequency of transactions, expenditure behavior, landing-centers, device ID, and geographical location. In the modelling step the trained models are the supervised learning algorithms in which Random Forests, Gradient Boosting, and the Neural Networks would consider label.

METHODOLOGY

The process of designing and testing a machine learning system of credit card fraud detection is addressed in a systematic way in the event of this research study. The procedure will start by

acquiring a credible set of legitimate and fraud transactions. And they are a much smaller number of fraudulent cases than normal ones, so it is an imbalanced dataset that must be addressed using specialist techniques to train it fairly.

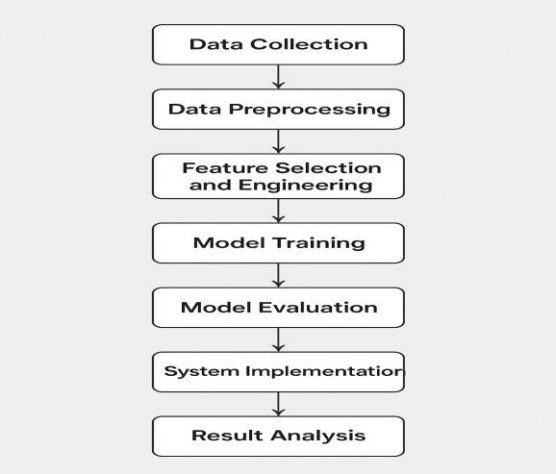

Fig. 1. Block diagram.

The block diagram outlines the steps for detecting credit card fraud using machine learning. First, data collection takes place. Next, we preprocess the data to reduce noise, normalize it, and address the issue of class imbalance. We then select the relevant features. After processing, we train the models using data, which includes both legitimate and fraudulent transactions. We evaluate the models using Recall, Precision, and AUC-ROC to measure their reliability. The most appropriate model is transferred and incorporated into the implementation of a system monitoring transactions in real- time and the outcomes are assessed when comparing results agency.

Task	Task Name	Status
1	Data Collection and Preprocessing	Done
2	Feature Extraction and Selection	Done
3	Model training	Done
4	Model Validation	Done
5	Fraud Detection	Done

EXPERIMENTAL RESULTS

In order to test we selected the Random Forest tool of guessing since it is robust and powerful

with complex data relationships. During the training period, we drove the tool by modifying parameters such as number of counters, and max depth. We were correct in our last tool 81.5% of the time, and outperformed other simple tools including Logistic Regression (77.8%) and Decision Tree (74.6%). We also tested the precision, recall and F-score in order to get a closer check. The precision, recall 0.82, and F1-score of the tool were 0.79, 0.80, respectively. This indicates that it is effective in right finding diabetic and non-diabetic. The additional components of the system were tested not only in guessing right. The diet plan creator has provided good food advice on diabetic and non-diabetic individuals. The clinic finder placed diabetes clinics in Bangalore on the map (right), and the AI chatbot provided decent responses to frequently asked questions of how to stop diabetes and what is the best way to live well. In addition, the user tests revealed that the inclusion of new features made it more fun to use and more practical and is promising when it comes to the entire online health repair.

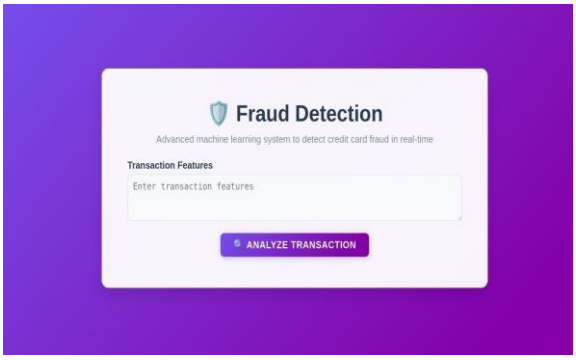

Fig.2. User interface (UI) design for a Fraud Detection system

Fig.3. Fraud detection system interface

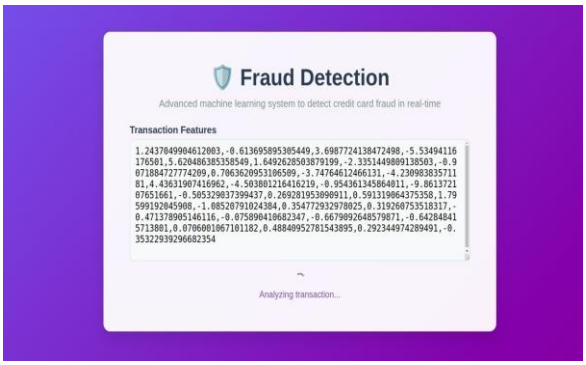

Fig.4. Result screen of a credit card fraud detection system

CONCLUSION

Credit card fraud is still a great concern in the digital payment ecosystem to both financial institutions and customers. The shortcoming of Traditional rule-based systems is that it is no longer enough to counter the intricacy of the present day fraudulent practices. This study reveals the effectiveness of machine learning which is more dynamic and adaptive based on the analysis of substantial amounts of transactional data and identification of complicated types of fraud which are hard to detect manually. The paper is focused on the application of supervised learning as a classification tool, unsupervised learning in anomaly detection and deep learning as a tool of learning complex behavior patterns. Such feature engineering, data balancing, and hybrid modeling techniques can provide even further enhanced detection accuracy with a reduction in false positives. Besides, real-time observing and explainable AI solutions make the discussed system not only efficient but also understandable and viable to implement in the real world. The future of fraud detection is changing as fraudsters evolve, it changes to an adaptive model that is integrated with big data platforms and more interpretable.

REFERENCES

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

[2] Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., & Bontempi, G. (2018). *Information Fusion, 41*, 182–194. https://doi.org/10.1016/j.inffus.2017.09.005

[3] Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). *Expert Systems with Applications,100*,234–245. https://doi.org/10.1016/j.eswa.2018.01.037

[4] Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences, 479*, 448–455. https://doi.org/10.1016/j.ins.2017.11.060

[5] Sahin, Y., & Duman, E. (2011). Detecting credit card fraud by decision trees and support vector machines. *Proceedings of the International MultiConference of Engineers and Computer Scientists (IMECS)*, 1, 442–447