RESEARCH ARTICLE OPEN ACCESS

Credit Card Fraud Detection Using Machine Learning Techniques: A Comparative Analysis of Classification Algorithms

Suraj Yadav
Department of Engineering and Technology, Jagannath University, Jaipur, India

ABSTRACT: Credit card fraud is a growing concern in present world with growing fraud in the corporate industries, government offices, finance industries, and many other organizations. Credit card fraud poses a significant threat to financial institutions and consumers worldwide. In recent years, the proliferation of online transactions and digital payment systems has increased the vulnerability to fraudulent activities. The increase of credit card fraud is growing rapidly worldwide, which is the reason actions should be taken to stop fraudsters. Putting a limit for those actions would have a positive impact on the customers as their money would be recovered and retrieved back into their accounts and they will not be charged for items or services that were not purchased by them.
This paper presents a comprehensive review of the state-of-the-art techniques for detecting credit card fraud, with a focus on machine learning algorithms. Furthermore, we discuss the challenges and limitations associated with existing approaches and propose potential avenues for future research in this domain.

Keywords — Credit Card Fraud Detection, Fraud Detection, Fraudulent Transactions, K-Nearest Neighbours, Support Vector Machine, Logistic Regression, Naïve Bayes.

1. Introduction

The rapid growth of digital banking, e-commerce platforms, and online payment systems has significantly increased the use of credit cards for everyday financial transactions [1]. Credit cards offer convenience, flexibility, and accessibility, making them one of the most widely used payment methods worldwide [2]. However, the increasing reliance on electronic transactions has also led to a substantial rise in fraudulent activities, creating serious financial and security challenges for both customers and financial institutions [3]. As a result, credit card companies must place greater emphasis on ensuring the security and protection of customer accounts and transaction data. Credit card fraud detection involves the use of various techniques and technologies to identify potentially fraudulent transactions either in real time or through post-transaction analysis [5]. Traditional rule-based fraud detection systems often struggle to keep pace with evolving fraud patterns and the growing volume of transaction data. Consequently, machine learning has emerged as a powerful solution for detecting suspicious activities by automatically learning patterns and behaviors from historical transaction records. Machine learning models can quickly identify deviations from normal customer behavior and transaction patterns. By recognizing anomalies such as sudden increases in transaction amounts, unusual spending behavior, changes in geographical location, or abnormal transaction frequency, these models can significantly reduce the risk of fraud and improve transaction security. The increasing prevalence of credit card fraud has become a major concern worldwide. According to reports, credit card fraud cases in the United States increased by approximately 44.7%, rising from 271,927 reported incidents in 2019 to 393,207 incidents in 2020. Credit card fraud generally occurs in two major forms. The first type involves identity theft, where fraudsters open new credit card accounts using stolen personal information. Reports of this type of fraud increased by 48% between 2019 and 2020. The second type occurs when criminals gain unauthorized access to an existing credit card account by stealing card information and conducting fraudulent transactions. Reports of

this category increased by 9% during the same period (Daly, 2021). These alarming statistics highlight the growing severity of the problem and emphasize the need for more intelligent and efficient fraud detection mechanisms.

The detection of fraudulent transactions presents several challenges due to the massive volume of financial transactions processed daily and the highly imbalanced nature of fraud datasets. Fraudulent transactions typically represent only a small fraction of total transactions, making them difficult to identify accurately. Moreover, fraudsters continuously adapt their strategies to bypass traditional security systems. Therefore, advanced analytical techniques capable of learning complex transaction patterns are essential for improving detection accuracy and minimizing financial losses. Machine learning provides an effective framework for addressing these challenges. By analyzing historical transaction data, machine learning algorithms can automatically distinguish between legitimate and fraudulent activities. Various supervised learning techniques, including Logistic Regression, Naïve Bayes, k-Nearest Neighbour (KNN), Decision Trees, and Random Forest, have been widely used for fraud detection applications. These algorithms learn from labeled transaction data and classify future transactions based on previously observed patterns. Among these methods, Random Forest has gained considerable attention due to its robustness, ability to handle large datasets, resistance to overfitting, and high classification performance. This research focuses on developing a machine learning-based credit card fraud detection system and conducting a comparative analysis of multiple classification algorithms. The study utilizes a publicly available credit card transaction dataset containing anonymized transaction features, transaction amounts, timestamps, and fraud labels. Various machine learning models are trained and evaluated using performance metrics such as accuracy, sensitivity, specificity, precision, Matthews Correlation Coefficient (MCC), and Balanced Classification Rate (BCR). The objective is to identify the most effective classification technique for detecting fraudulent transactions while minimizing false positives and false negatives.

The proposed framework aims to support financial institutions in strengthening fraud prevention mechanisms and enhancing transaction security. By leveraging machine learning techniques, the system can provide faster and more accurate fraud detection, reduce financial losses, and improve customer confidence in digital payment systems. Furthermore, the comparative analysis presented in this study contributes to a better understanding of the strengths and limitations of different classification algorithms in real-world fraud detection scenarios.

2. Machine Learning Algorithms for Fraud Detection

There are various fraudulent activities detection techniques has implemented in credit card transactions have been kept in researcher minds to methods to develop models based on artificial intelligence, data mining, fuzzy logic and machine learning. Credit card fraud detection is a very troublesome, but also a popular problem to solve. In our proposed system we built the credit card fraud detection using Machine learning [8]. With the advancement of machine learning techniques. Machine learning has been recognized as a no-hit live for fraud detection. A great deal of data is transferred throughout on-line transaction processes, resulting in a binary result: genuine or fraudulent [9]. Online businesses are able to identify fraudulent transactions accurately because they receive chargebacks on them. Within the sample fraudulent datasets, features are constructed [10].

These area unit information points like the age and price of the client account, as well as the origin of the credit card. There are many options and everyone contributes, to varying extents, towards the fraud probability. Note, the degree within which every feature

contributes to the fraud score isn't determined by a fraud analyst, but is generated by the artificial intelligence of the machine which is driven by the training set. So, in regard to the card fraud, if the use of cards to commit fraud is proven to be high, the fraud weighting of a transaction that uses a credit card will be equally so.

However, if this were to diminish, the contribution level would parallel. Simply put, these models self-learn while not express programming like with manual review. Credit card fraud detection using Machine learning is done by deploying the classification and regression algorithms. We use a supervised learning algorithm such as Random Forest algorithm to classify the fraud card transaction online or by offline. Random forest is an advanced version of the Decision tree. The random forest has better efficiency and accuracy than the other machine learning algorithms. Random forest aims to reduce the previously mentioned correlation issue by choosing only a subsample of the feature space at each split. Essentially, it aims to make the trees decorrelated and prune the trees by setting a stopping criterion for node splits

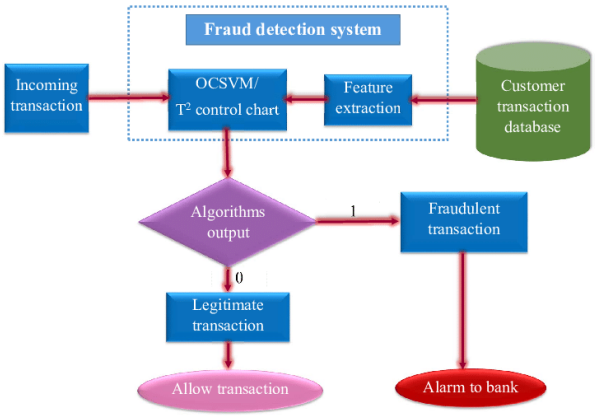

Figure 1: Fraud Detection System

3. Purpose of the Project

The primary objective of this project is to develop a machine learning-based system capable of detecting fraudulent credit card transactions in online financial systems. Due to the enormous volume of daily transactions and the complexity of transaction patterns, manual identification of fraudulent activities is impractical and inefficient. Machine learning provides an effective solution by automatically analyzing transaction data and identifying suspicious patterns that may indicate fraudulent behavior. The proposed system aims to classify transactions into two categories: legitimate and fraudulent. This classification is achieved using supervised machine learning algorithms, particularly the Random Forest algorithm, which is known for its high accuracy, robustness, and ability to handle large datasets. By learning from historical transaction data, the system can identify unusual transaction behavior and assist financial institutions in preventing fraud before significant financial losses occur.

The project also seeks to improve awareness regarding credit card fraud and demonstrate how artificial intelligence can be applied to enhance transaction security. Ultimately, the proposed framework aims to support safer digital payment systems and strengthen fraud prevention mechanisms within the banking and financial sectors.

4. Methodology

The proposed fraud detection framework utilizes machine learning algorithms to identify anomalous transaction patterns, commonly referred to as outliers, within large volumes of financial transaction data. The overall methodology consists of data collection, preprocessing, exploratory data analysis, model training, classification, and performance evaluation. The dataset used in this study was obtained from Kaggle, a widely recognized platform for data science and machine learning research. The dataset contains 31 attributes representing credit card transaction information. To protect customer privacy and maintain confidentiality, 28 of the attributes have been anonymized and labeled as V1 through V28. The remaining attributes include Time, Amount, and Class. The Time attribute represents the elapsed time between the first recorded transaction and subsequent transactions. The Amount attribute indicates the monetary value of each transaction. The Class attribute serves as the target variable,

where a value of 0 represents a legitimate transaction and a value of 1 represents a fraudulent transaction. Prior to model development, the dataset undergoes preprocessing and exploratory analysis to identify inconsistencies, missing values, and potential anomalies. Various graphical visualization techniques are employed to better understand transaction distributions and fraud patterns. Data normalization and feature analysis are performed to improve model performance and ensure reliable classification results.

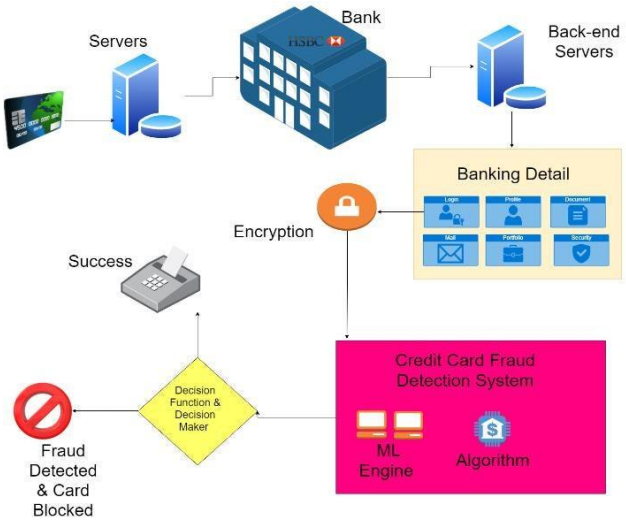

Figure 2: Credit Card Fraud Detection and Card Blocked

Following preprocessing, multiple machine learning algorithms are trained and evaluated for fraud detection. The primary focus is placed on the Random Forest classifier due to its ability to reduce overfitting, handle high-dimensional datasets, and provide robust classification performance. The Random Forest algorithm constructs multiple decision trees using random subsets of features and combines their outputs to generate more accurate predictions. The performance of the developed models is evaluated using standard classification metrics, including accuracy, sensitivity, specificity, precision, Matthews Correlation Coefficient (MCC), and Balanced Classification Rate (BCR). These metrics provide a comprehensive assessment of the model's ability to correctly identify fraudulent transactions while minimizing false positives and false negatives. The proposed methodology aims to develop an intelligent and reliable fraud detection system capable of assisting financial institutions in securing electronic transactions and reducing financial risks associated with credit card fraud.

Performance of all learning algorithms used for fraud detection in credit card transactions is compared in table 1. The comparison is based on their accuracy, precision and specificity.

TABLE 1: Accuracy result for un-sampled data distribution.

Metrics	Naïve Bayes	k-Nearest Neighbour	Logistic Regression
Accuracy	0.9737	0.9691	0.9824
Sensitivity	0.8072	0.8835	0.9767
Specificity	0.9741	0.9711	0.9824
Precision	0.0505	0.4104	0.0873
Matthews Correlation Coefficient	+0.1979	+0.5903	+0.2893
Balanced Classification Rate	0.8907	0.9273	0.9796

5. Future Enhancements

While we couldn't reach out goal of 100% accuracy in fraud detection, we did end up creating a system that can, with enough time and data, get very close to that goal. As with any such project, there is some room for improvement here. The very nature of this project allows for multiple algorithms to be integrated together as modules and their results can be combined to increase the accuracy of the final result. This model can further be improved with the addition of more algorithms into it. However, the output of these algorithms needs to be in the same format as the others. Once that condition is satisfied, the modules are easy to add as done in the code. This provides a great degree of modularity and versatility to the project. More room for improvement can be found in the dataset. As demonstrated before, the precision of the algorithms increases when the size of

dataset is increased. Hence, more data will surely make the model more accurate in detecting frauds and reduce the number of false positives. However, this requires official support from the banks themselves.

6. Conclusion

The increasing use of credit cards and digital payment systems has made fraud detection a critical challenge for financial institutions worldwide. Fraudulent transactions not only cause significant financial losses but also undermine customer trust and confidence in electronic payment systems. Therefore, the development of intelligent and automated fraud detection mechanisms has become essential for ensuring secure financial transactions. This study presented a machine learning-based credit card fraud detection framework designed to identify fraudulent transactions from large volumes of transaction data. Various classification algorithms, including Naïve Bayes, k-Nearest Neighbour, Logistic Regression, and Random Forest, were investigated and evaluated using a credit card transaction dataset. The performance of these algorithms was analyzed through multiple evaluation metrics such as accuracy, sensitivity, specificity, precision, Matthews Correlation Coefficient, and Balanced Classification Rate. The experimental results demonstrate that machine learning algorithms are capable of effectively distinguishing between legitimate and fraudulent transactions. The models successfully identify abnormal transaction patterns and provide a reliable mechanism for detecting potential fraud. Among the evaluated techniques, Logistic Regression achieved strong overall classification performance, while Random Forest demonstrated robustness and effectiveness in handling complex transaction data. The findings confirm that machine learning-based fraud detection systems can significantly enhance transaction security and assist financial institutions in reducing fraud-related losses. One of the major advantages of the proposed approach is its ability to automatically learn patterns from historical transaction data without requiring manually defined rules. This enables the system to adapt to evolving fraud strategies and improve detection performance over time. Furthermore, the framework can support real-time fraud monitoring, allowing suspicious transactions to be identified before significant financial damage occurs. Although the proposed system achieved promising results, there is still scope for improvement. Future work may focus on incorporating ensemble learning techniques, deep learning models, and larger real-world datasets to enhance predictive performance. The integration of multiple algorithms and real-time transaction processing systems can further reduce false positives and improve fraud detection accuracy. Additionally, collaboration with financial institutions for access to larger datasets can contribute to the development of more robust and scalable fraud detection solutions. In conclusion, machine learning provides an effective and intelligent approach to credit card fraud detection. The proposed framework demonstrates the potential of data-driven techniques in enhancing financial security, minimizing fraudulent activities, and supporting safer electronic payment systems in the modern digital economy.

References

[1] K. Gautam, G. K. Soni, R. Ajmera, N. Hemrajani, J. Ahuja, and M. K. Jha, “Deep Reinforcement Learning for Stock Market Portfolio Optimization,” in Proceedings of the 5th International Conference on Communication, Computing and Electronics Systems (ICCCES), pp. 1835–1839, 2026.

[2] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, “Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy,” IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3784–3797, 2018.

[3] S. Yadav, S. Sharma, and R. Bagoria, “AI-Powered Teaching and Learning Frameworks for Technical Education,”

International Journal of Engineering Trends and Applications (IJETA), vol. 13, no. 3, pp. 17–22, 2026.

[4] R. Misra and M. Jain, "The Role of Artificial Intelligence in Transforming Cybersecurity Systems," International Journal of Engineering Trends and Applications (IJETA), vol. 13, no. 3, pp. 151–156, 2026.

[5] A. Alneyadi, H. Lamaazi, M. Alshamsi, M. Albaloushi, M. Alneyadi, and N. Megrez, "Toward an Efficient Credit Card Fraud Detection," in Proceedings of the Arab Information and Communication Technologies Conference (AICTC), pp. 73–78, 2024.

[6] H. Sharma and R. Ajmera, "Comprehensive Review and Analysis on Machine Learning-Based Twitter Opinion Mining Framework," Tuijin Jishu/Journal of Propulsion Technology, vol. 44, no. 5, 2023.

[7] A. Jangir, A. Agrawal, C. Sharma, G. K. Soni, R. Ajmera, and A. Johari, "Comparative Performance Analysis of Deep Learning and Traditional Algorithms for Facial Recognition and Image Classification," in Proceedings of the 4th International Conference on Automation, Computing and Renewable Systems (ICACRS), pp. 1172–1175, 2025.

[8] P. Pandey and K. K. Garg, "Credit Card Fraud Detection Using K-Nearest Neighbour, Support Vector Classifier, and Decision Tree Machine Learning Algorithms," in Proceedings of the IEEE 4th International Conference on Artificial Intelligence in Cybersecurity (ICAIC), pp. 1–3, 2025.

[9] S. K. K., P. R., R. Senthamil Selvan, P. G. D., and B. R. A., "Evaluation and Implementation of Optimal Classification Algorithms for Credit Card Fraud Detection," in Proceedings of the 2nd International Conference on Computational and Characterization Techniques in Engineering and Sciences (IC3TES), pp. 1–4, 2024.

[10] S. Thapar, G. K. Soni, H. Kaushik, R. Singh, S. Bisht, and S. K. Bansal, "A Comparative Machine Learning Framework for Detecting Fake Accounts on Facebook," in Proceedings of the 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 1567–1571, 2025.

[11] Yadav, V. Shekhawat, K. Gautam, G. K. Soni, and R. Yadav, "Artificial Intelligence for Cybersecurity: Emerging Techniques, Challenges, and Future Trends," in Proceedings of the 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), pp. 1176–1180, 2025.

[12] M. K. Jha, K. Kumar, N. Hemrajani, D. S. Rao, A. Goyal, and R. Ajmera, "AI Powered Student Performance Prediction Using Explainable Machine Learning," in Proceedings of the 4th International Conference on Automation, Computing and Renewable Systems (ICACRS), pp. 1140–1144, 2025.

[13] M. K. Jha, G. K. Soni, G. Jain, S. Tiwari, K. Gupta, and B. Singhal, "Comparative Analysis of Classical Machine Learning Models for Twitter Sentiment Classification," in Proceedings of the 5th International Conference on Communication, Computing and Electronics Systems (ICCCES), pp. 1949–1954, 2026.

[14] M. Kumar, R. Ajmera, and D. Kumar, "Statistical Analysis and Accuracy Assessment of Improved Machine Learning-Based Opinion Mining Framework," Advances in Nonlinear Variational Inequalities, vol. 27, no. 1, 2024.

[15] A. Kumar and N. Hemrajani, "Comparative Analysis of Different

Transport Layer Protocol Techniques in Cognitive Network," Recent Advances in Computer Science and Communications, Bentham Science Publishers, vol. 17, 2024.

[16] Johari, R. Sharma, A. Meena, and V. Tiwari, "Advancements in Pre-Trained Language Models and Their Impact on Various Natural Language Processing Tasks," International Journal of Engineering Trends and Applications (IJETA), vol. 11, no. 3, pp. 201–209, 2024.

[17] R. Ajmera, A. Johari, A. Goyal, A. Purohit, A. Kumar, and J. A. Ashok, "Multilingual Sentiment Analysis Based on Fine-Tuned Transformer Architectures," in Proceedings of the 5th International Conference on Communication, Computing and Electronics Systems (ICCCES), pp. 1589–1592, 2026.