International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Credit Card Fraud Detection

Nikita Dargude[1], Shruti Niphade[2], Rutuja Gholap[3], Shweta Gangurde[4], [5]

[1234]Student, Computer Engineering, Matoshri College of Engineering and Research Centre, Nashik, Maharashtra, India.

[5]Assistant Professor, Computer Engineering, Matoshri College of Engineering and Research Centre, Nashik, Maharashtra, India.

ABSTRACT

It is essential for credit card companies to identify fraudulent transactions so that customers are not billed for purchases they never made. Data Science and Machine Learning play a crucial role in addressing this challenge. This project demonstrates the modeling of a dataset for Credit Card Fraud Detection using machine learning. The problem involves analyzing past credit card transactions, distinguishing between legitimate and fraudulent ones, and then building a model capable of detecting whether a new transaction is fraudulent.The main objective is to detect all fraudulent transactions while minimizing the number of legitimate transactions incorrectly classified as fraud. Since this is a classification problem, our approach involves analyzing and preprocessing the dataset, followed by applying multiple anomaly detection algorithms, such as the Local Outlier Factor (LOF) and the Isolation Forest algorithm, on the PCA-transformed credit card transaction data.

1. INTRODUCTION

Credit card fraud refers to the unauthorized and illegal use of an individual's credit card account by someone other than the rightful owner. It involves carrying out transactions without the knowledge or consent of the cardholder or the issuing authority. To prevent such misuse, it is essential to implement effective security measures and analyze fraudulent behaviors to minimize risks and safeguard against future occurrences.

Fraud detection focuses on monitoring user activities to identify, predict, or prevent suspicious behaviors, including fraud, intrusion, or financial default. This issue is highly relevant in the fields of machine learning and data science, where automated solutions can play a crucial role in recognizing and preventing fraudulent transactions.

Detecting credit card fraud poses unique challenges, particularly due to class imbalance—the number of legitimate transactions is vastly higher than fraudulent ones. Additionally, transaction patterns often evolve over time, making it difficult for static models to maintain accuracy.

In real-world applications, massive streams of payment requests are processed rapidly by automated systems that determine which transactions to approve. Machine learning algorithms are employed to analyze these transactions and flag potentially suspicious ones.

Once identified, these flagged transactions are reviewed by human investigators who contact cardholders to confirm whether the transactions were genuine or fraudulent. The investigators' feedback is then used to retrain and improve the machine learning models, enabling continuous enhancement of the fraud detection system's performance over time.

In real-world financial systems, an enormous number of payment requests are generated every second. These are processed through automated fraud detection frameworks, which use advanced machine learning algorithms to analyze transaction data such as amount, time, location, device used, and spending patterns. Transactions that deviate significantly from a user's normal behavior are flagged as suspicious.

Once a transaction is flagged, it undergoes human verification. Fraud investigation teams contact cardholders to confirm the authenticity of the transaction. If found fraudulent, the system's model parameters are updated using this feedback, allowing the algorithm to learn from past mistakes and continuously improve its detection accuracy.

To enhance the efficiency of detection systems, researchers have explored a wide range of algorithms including Logistic Regression, Random Forest, Decision Tree, Support Vector Machine (SVM), Neural Networks, and Unsupervised models such as Local Outlier Factor (LOF) and Isolation Forest. These models can process large datasets, detect subtle anomalies, and adapt to evolving fraud strategies.

Moreover, recent advancements in deep learning and hybrid approaches have further improved prediction accuracy. Techniques combining Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) with classical models have shown promising results in identifying complex, non-linear relationships in transaction data. Additionally, emerging technologies such as blockchain and federated learning are being integrated to improve data security, transparency, and collaboration between financial institutions.

In conclusion, credit card fraud detection remains a complex and evolving challenge that requires the integration of intelligent algorithms, real-time data analysis, and human expertise. Continuous model refinement, adaptive learning, and secure data-sharing frameworks will be key to building more resilient and reliable fraud detection systems in the future.

1.1 LITERATURE SURVEY

In 2024, R. Khan et al. proposed "Blockchain-based Secure Credit Card Fraud Detection Framework." This study integrated blockchain technology with machine learning algorithms to create a transparent and tamper-proof system for detecting fraudulent credit card transactions, ensuring data integrity and trust among financial institutions.

In 2023, K. Das et al. presented "Improving Fraud Detection with Federated Learning." The research focused on a privacy-preserving model where multiple banks collaboratively trained fraud detection systems using federated learning, enabling high accuracy without sharing sensitive customer data.

In 2022, M. Singh and P. Gupta developed "Real-time Fraud Detection using Ensemble Learning." The study utilized an ensemble of Random Forest and XGBoost algorithms to analyze live transaction streams, improving detection speed and reducing false positives.

In 2021, S. Reddy et al. introduced "Hybrid Deep Learning Model for Credit Card Fraud Detection." This approach combined Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to capture both spatial and temporal transaction patterns for more accurate fraud prediction.

In 2020, A. Sharma et al. proposed "Anomaly Detection for Credit Card Fraud using Isolation Forest." The authors implemented an unsupervised learning technique that detected outliers and irregular transaction patterns effectively, even without labeled data.

In 2019, J. Patel et al. published "Credit Card Fraud Detection using Machine Learning Algorithms." This comparative study evaluated models like Decision Tree, Logistic Regression, and Random Forest, identifying ensemble methods as more reliable for detecting fraudulent activity in transaction datasets.

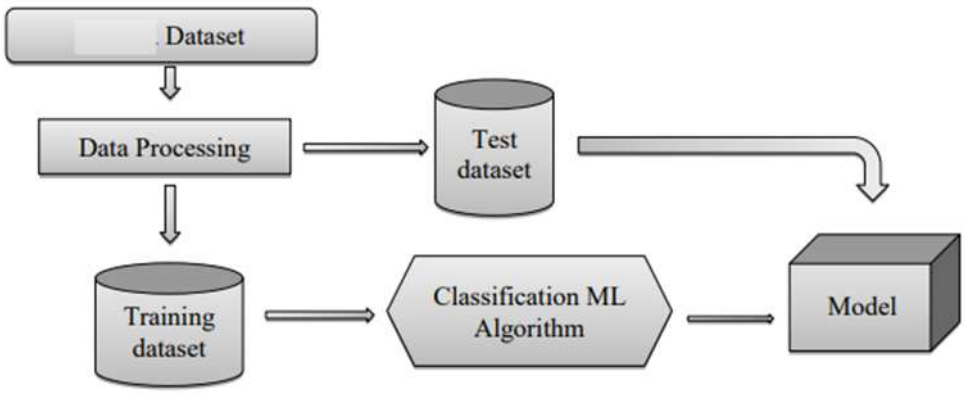
2. METHODOLOGY

The approach that this paper proposes, uses the latest machine learning algorithms to detect anomalous activities, called outliers. The basic rough architecture diagram can be represented with the following figure:

2.1 SYSTEM OVERVIEW:

The growing volume of online credit card transactions has led to an increase in fraud cases. Traditional rule-based detection methods are insufficient, as fraudsters frequently adapt their strategies. The problem is to develop a machine learning–based fraud detection model capable of identifying fraudulent transactions in real time, despite challenges such as data imbalance and evolving transaction patterns. Credit card fraud detection is a complex classification problem where the number of fraudulent cases is significantly smaller than legitimate ones. This class imbalance, along with dynamic fraud strategies, makes traditional detection methods less effective.

2.2 SYSTEM ARCHITECTURE:



3. MODELING AND ANALYSIS

The following describes the suggested Credit Card Fraud workflow:

These are not the only challenges in implementing a real-world fraud detection system. In practice, the enormous stream of payment requests must be scanned rapidly by automated tools that decide which transactions to authorize. Machine learning algorithms are then applied to analyze the authorized transactions and flag any suspicious activity. The flagged transactions are further investigated by professionals, who reach out to the cardholders to verify whether the transaction was legitimate or fraudulent.

Handling Missing Values

- Fill or drop incomplete records.
- Data Cleaning
- Remove outliers or noisy entries.
- Feature Engineering
- Create new features like transaction frequency, average transaction value, etc.
- Scaling and Normalization
- Standardize numeric features to avoid biases.
- Dealing with Class Imbalance
- Techniques:
- Resampling: oversampling (SMOTE), undersampling.
- Class weighting in algorithms.
- Anomaly detection approaches..

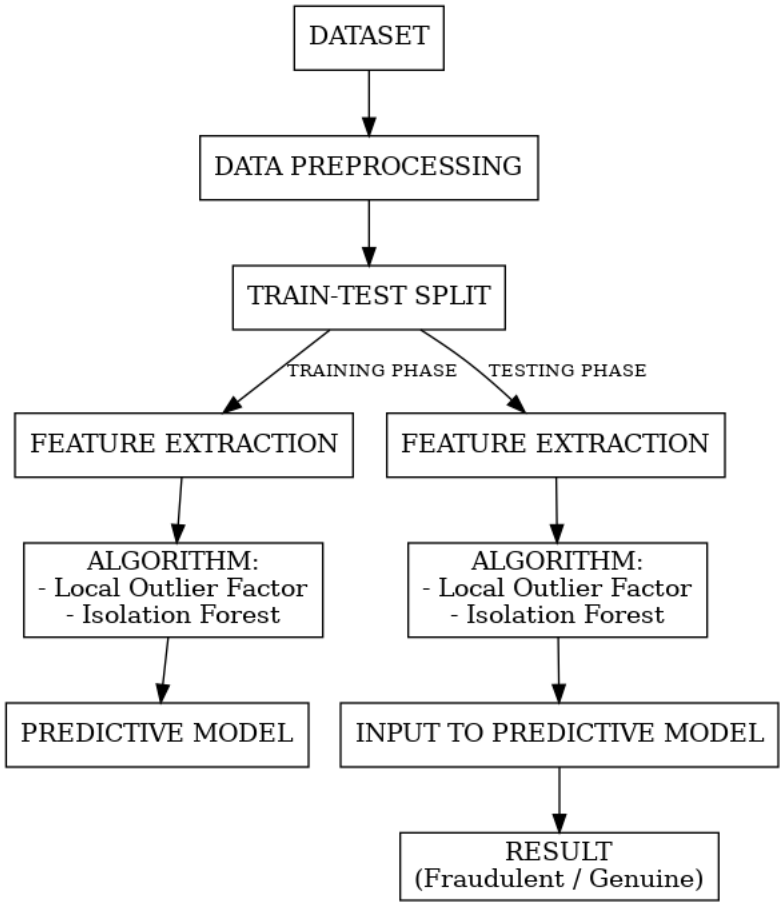


Fig 3.1 :- Workflow Diagram of Credit Card Fraud Detection

4.2 FUTURE ENHANCEMENTS

Following testing and successful deployment, the system can be extended to include:

1. Use deep learning models for better accuracy.
2. Implement real-time streaming detection using big data tools.
3. Apply adaptive learning to update models automatically with new fraud patterns.
4. Integrate blockchain technology for secure transaction tracking.
5. Improve explainability of AI models for better trust and transparency.
6. Develop cross-bank fraud sharing systems to detect large-scale frauds.

4.3 CHALLENGES AND LIMITATIONS:

- Highly imbalanced data (few fraud cases).
- Constantly evolving fraud patterns.
- Need for real-time detection.
- High false positive rates.
- Limited access to real-world data.
- Model overfitting issues.
- Reliance on historical data.
- Delay in real-time processing.
- Lack of model interpretability.

4. CONCLUSION

Credit card fraud is undeniably an act of criminal dishonesty. This paper outlines the most common methods of fraud, their detection techniques, and reviews recent developments in the field. It also demonstrates how machine learning can be applied to improve fraud detection, providing details on the algorithm, pseudocode, implementation, and experimental results.

Although the proposed algorithm achieves an accuracy of over 99.6%, its precision is only 28% when applied to a tenth of the dataset. However, when the entire dataset is used, the precision increases to 33%. This significant difference highlights the challenge posed by the extreme imbalance between the number of legitimate and fraudulent transactions, which directly impacts the performance of the model.

ACKNOWLEDGEMENTS

First and the foremost I, express my deep sense of gratitude, sincere thanks and deep sense of Appreciation to project Guide Prof. and seminar coordinate Ms. S. A. Handore Department of Computer Engineering, Matoshri College of Engineering and Research Center, Nashik. Your Availability at any time throughout the Semester, valuable guidance ,view, comments, critics, encouragement and support tremendously boosted this research work.

Again, load and loads of thank to head Computer Engineering Department Dr. Swati Bhavsar for providing me the support I ever had .Your opinion, view , Comments and thoughts have been really helped me to improve my writing.

I like to express my sincere gratitude to Dr. G. K. Kharate, Principal, Matoshri College of Engineering and Research center, Nashik for proving the great platform to complete the this within the schedule time.

I am also Thankful to all the faculty member, Computer Engineering Department, Matoshri College of Engineering and Research Center, Nashik for giving comments for the improvement of work ,encouragement and help during completion of the thesis.

Last but not least; I should say thanks from my bottom of heart to my family and friends for their never ending love, help and support in so many ways through all this time. Thank you so much.

Finally , I am thanking to MIGHTY GOD, who given me the courage confidence to not only this Dissertation work but also in bad difficult situation.

5. REFERENCES

[1] “Credit Card Fraud Detection Based on Transaction Behaviour -by John Richard D. Kho, Larry A. Vea” published by Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2017

[2] CLIFTON PHUA1, VINCENT LEE1, KATE SMITH1 & ROSS GAYLER2 “ A Comprehensive Survey of Data Mining-based Fraud Detection Research” published by School of Business Systems, Faculty of Information Technology, Monash University, Wellington Road, Clayton, Victoria 3800, Australia

[3] “Survey Paper on Credit Card Fraud Detection by Suman” , Research Scholar, GJUS&T Hisar HCE, Sonepat published by International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 3, March 2014

[4] “Research on Credit Card Fraud Detection Model Based on Distance Sum – by Wen-Fang YU and Na Wang” published by 2009 International Joint Conference on Artificial Intelligence

[5] “Credit Card Fraud Detection through Parenclitic Network Analysis By Massimiliano Zanin, Miguel Romance, Regino Criado, and SantiagoMoral” published by Hindawi Complexity Volume 2018, Article ID 5764370, 9 pages

[6] “Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy” published by IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, VOL. 29, NO. 8, AUGUST 2018

[7] “Credit Card Fraud Detection-by Ishu Trivedi, Monika, Mrigya, Mridushi” published by International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016

[8] David J.Wetson,David J.Hand,M Adams,Whitrow and Piotr Jusczak “Plastic Card Fraud Detection using Peer Group Analysis” Springer, Issue 2008.