



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: <https://doi.org/10.22214/ijraset.2026.78056>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Machine Learning Based Credit Card Fraud Detection System

Suravarapu Vijaya Ravi Kiran Naga Teja¹, Cherukuri Shankara Narasimha Naidu², Pilla Sravan³, Dasari Eswara Srinivas⁴, R. D. Bhanu Prakash⁵

^{1, 2, 3, 4}Department of Computer Science and Engineering (Artificial Intelligence and Data Science), Bonam Venkata Chalamayya Engineering College, Affiliated to JNTU Kakinada, Andhra Pradesh, India

Abstract: *The rapid growth of online transactions and digital banking has significantly increased the use of credit cards for financial activities. However, this convenience has also led to a rise in credit card fraud, causing major financial losses for banks and customers. Traditional fraud detection systems mainly rely on rule-based methods, which are often inefficient in identifying new and complex fraud patterns. To address this challenge, this project proposes a Machine Learning Based Credit Card Fraud Detection System that automatically analyzes transaction data and identifies fraudulent activities with high accuracy. The system utilizes modern technologies such as Python for backend development and machine learning algorithms to analyze transaction patterns and detect anomalies. Transaction data is first preprocessed to remove noise and extract important features such as transaction amount, time, and location. Machine learning algorithms like Logistic Regression, Random Forest, and Isolation Forest are then applied to classify transactions as legitimate or fraudulent.*

The proposed system aims to improve fraud detection accuracy, reduce financial losses, and enhance the security of online transactions. By leveraging data-driven techniques and intelligent algorithms, the system can identify suspicious activities in real time and assist financial institutions in preventing fraudulent transactions. Experimental results show that the machine learning model can effectively detect fraudulent behavior and improve the efficiency of fraud detection systems. Furthermore, the system provides a scalable architecture for handling large volumes of transaction data and supports faster decision-making in financial security systems. By integrating machine learning with modern data processing techniques, the proposed system offers a reliable and efficient solution for credit card fraud detection in digital payment environments.

Index Terms: *Machine Learning, Credit Card Fraud Detection, Logistic Regression, Random Forest, Isolation Forest, Financial Security, Data Mining.*

I. INTRODUCTION

The rapid growth of digital payment systems and online banking has significantly increased the use of credit cards for financial transactions. Credit cards provide convenience, speed, and flexibility for customers to perform payments across various platforms such as e-commerce websites, mobile banking applications, and point-of-sale systems. However, with the increasing number of electronic transactions, the risk of credit card fraud has also grown rapidly, becoming a major concern for financial institutions and customers

A. Background and Motivation

Credit card fraud occurs when an unauthorized individual uses someone else's credit card information to make illegal transactions. These fraudulent activities result in substantial financial losses for banks, merchants, and customers. Traditional fraud detection systems mainly rely on predefined rules and manual monitoring, which are often ineffective in detecting new and sophisticated fraud patterns. As fraudsters continuously develop advanced techniques, conventional security systems struggle to keep up with these evolving threats.

B. Problem Statement

Traditional fraud detection systems mainly rely on rule-based methods and manual monitoring. These approaches are limited because they cannot effectively identify new and complex fraud patterns. Fraudsters constantly develop advanced techniques to bypass existing security systems, making fraud detection even more challenging. Additionally, manual detection processes are time-consuming and prone to human error.

C. Objectives

This project's main goal is to develop an intelligent system that uses machine learning techniques to detect fraudulent credit card transactions automatically. The system analyzes transaction data and identifies suspicious activities to improve financial security. The specific objectives of this project are: Building a system that can automatically analyze resumes and assess candidate profiles is the main goal of this project. The solution speeds up the hiring process and eliminates the need for manual resume analysis.

- The main objective of this project is to build an intelligent fraud detection system that can analyze credit card transaction data and identify suspicious activities. The system reduces the need for manual monitoring and enables faster detection of fraud in real-time financial transactions.
- The system processes transaction data to identify important attributes such as transaction amount, transaction time, location, and spending behavior. These extracted features are used by machine learning models to analyze patterns and detect unusual or suspicious transactions.
- Machine learning models such as Logistic Regression, Random Forest, and Isolation Forest are used to analyze transaction patterns and predict whether a transaction is genuine or fraudulent. These algorithms help improve the accuracy and efficiency of fraud detection.

D. Contributions and Paper Organization

This paper presents a comprehensive framework for a Machine Learning Based Credit Card Fraud Detection System designed to improve the security of digital payment transactions. The main contribution of this work is the development of an intelligent fraud detection system that automatically analyzes credit card transaction data and identifies fraudulent activities using machine learning algorithms. The system integrates modern technologies such as a Python-based backend, machine learning models for fraud prediction, and a secure database for efficient data storage and management. The proposed approach helps financial institutions detect suspicious transactions quickly, reduce financial losses, and enhance the reliability of digital payment systems.

The organization of this paper is structured as follows. Section II reviews the related work and existing research on credit card fraud detection techniques and machine learning approaches used in financial security systems. Section III describes the proposed system architecture and methodology, including data preprocessing, feature extraction, machine learning model development, and database integration. Section IV presents the implementation of the system and the experimental evaluation of the machine learning models used for fraud detection. Section V discusses the results, limitations, and possible improvements to enhance the performance and accuracy of the system. Finally, Section VI concludes the paper and outlines potential future work to further improve fraud detection systems using advanced machine learning techniques.

II. LITERATURE SURVEY

The rapid increase in digital transactions has led to a significant rise in credit card fraud, making fraud detection a critical issue for financial institutions. Researchers have explored various techniques to identify fraudulent transactions using data mining and machine learning methods. Traditional fraud detection systems relied on rule-based approaches and manual monitoring, which often failed to detect complex and evolving fraud patterns. To address these limitations, modern research focuses on machine learning techniques that can analyze large volumes of transaction data and identify suspicious activities automatically. Machine learning models are capable of learning patterns from historical transaction data and predicting whether a transaction is legitimate or fraudulent. These approaches help financial institutions improve fraud detection accuracy and reduce financial losses.

A. Machine Learning Based Fraud Detection Systems

With the rapid growth of online payments and digital banking services, the number of credit card transactions processed daily has increased significantly. This growth has also created opportunities for fraudulent activities. To combat this issue, many researchers have proposed machine learning based fraud detection systems that can analyze transaction data and identify unusual patterns.

Machine learning algorithms such as Logistic Regression, Decision Trees, Random Forest, and Support Vector Machines have been widely used to detect fraudulent transactions. These models are trained using historical transaction datasets containing both genuine and fraudulent activities. By learning from this data, the models can identify patterns that indicate possible fraud. Studies show that machine learning based systems significantly improve the accuracy and efficiency of fraud detection compared to traditional rule-based systems.

B. Machine Learning Algorithms for Credit Card Fraud Detection

Several studies have focused on the application of different machine learning algorithms for detecting credit card fraud. Algorithms such as Logistic Regression, Random Forest, Support Vector Machines, and Neural Networks are commonly used for classification problems in fraud detection. These algorithms analyze transaction features such as transaction amount, transaction time, location, and spending behavior to determine whether a transaction is legitimate or fraudulent.

Among these methods, Logistic Regression is considered an efficient and interpretable model for binary classification problems. It predicts the probability of a transaction being fraudulent based on input features. Random Forest and Decision Tree algorithms are also widely used because they can handle complex patterns in transaction data and provide high prediction accuracy. Research studies indicate that combining multiple algorithms or using ensemble learning techniques can further improve fraud detection performance.

III. PROPOSED METHODOLOGY

The proposed methodology aims to develop an intelligent system that can automatically detect fraudulent credit card transactions using machine learning techniques. The system analyzes transaction data, extracts relevant features, and applies a trained machine learning model to identify suspicious activities. By analyzing transaction patterns and customer behavior, the model can distinguish between legitimate and fraudulent transactions in real time. This approach helps financial institutions reduce financial losses, enhance security, and improve the efficiency of fraud detection processes.

A. System Architecture (Python Backend, Next.js Frontend, and Supabase Database Integration)

The proposed platform is designed using a scalable **three-tier architecture** that separates the user interface, application logic, and data management components. This architecture ensures efficient processing, maintainability, and system scalability.

- **Presentation Layer:** The backend processing is implemented using Python, where transaction data undergoes preprocessing, feature extraction, and model prediction. Machine learning algorithms such as Logistic Regression, Random Forest, or Decision Tree are used to classify transactions as either legitimate or fraudulent. The backend system analyzes various attributes such as transaction amount, location, time, and customer behavior to detect anomalies and suspicious activities. This layer also handles API requests and integrates the machine learning model for real-time fraud detection.
- **Application Layer:** Python is used to implement the backend processing, which includes feature extraction, text preparation, and resume parsing. Based on retrieved resume data, a machine learning model called Logistic Regression is utilized to categorize candidate profiles and forecast appropriate job opportunities.
- **Data Layer:** The Supabase database is used to store transaction data, user information, and prediction results securely. It provides a scalable cloud-based infrastructure that enables efficient data storage, retrieval, and authentication. The database maintains historical transaction records that can be used for model training and performance improvement. This layer ensures data integrity and supports secure communication between the application and storage components.

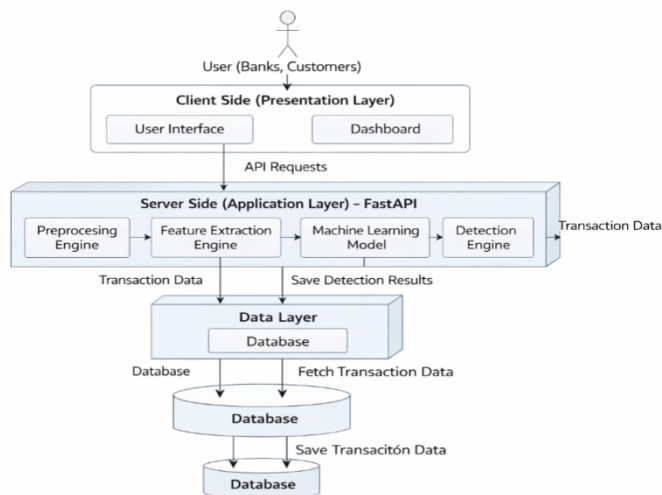


Fig. 2. System Architecture of the Machine Learning Based Credit Card Fraud Detection System System.

Fig.1. System Architecture of the Proposed AI-Based Credit Card Fraud Detection System Using Next.js, FastAPI and

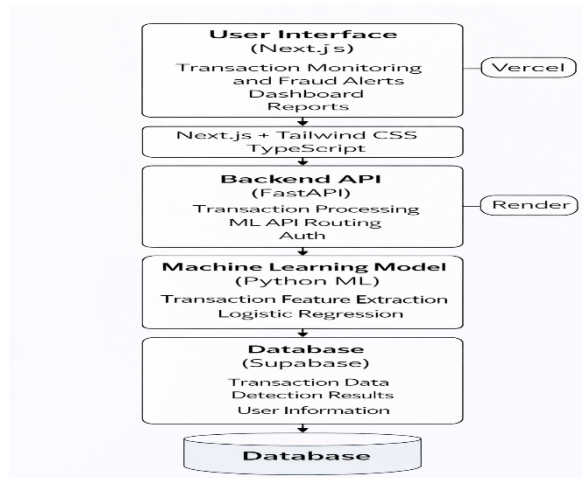


Fig. 1. System Architecture of the Proposed AI-Based Credit Card Fraud Detection System Using Next.js, FastAPI and Land

Fig.2. System Architecture of the Proposed AI-Based Credit Card Fraud Detection System Using Next.js, FastAPI and Land

B. Functional Modules (Transaction Data Input, Transaction Analysis, and Fraud Detection)

The proposed system is divided into several functional modules that guide the process of detecting fraudulent credit card transactions while providing an efficient and secure monitoring environment. The workflow begins with the Transaction Data Input Module, where transaction records are collected from financial systems or uploaded datasets through the application interface. This module allows the system to receive transaction details such as transaction amount, time, location, and merchant information, which are then forwarded to the backend for further processing.

The Fraud Detection Module uses a trained machine learning algorithm such as Logistic Regression, Random Forest, or Decision Tree to classify each transaction as either legitimate or fraudulent. The model analyzes patterns and anomalies within the transaction data to identify suspicious activities. If a transaction is detected as fraudulent, the system generates an alert and records the result in the database. This module helps financial institutions monitor transactions in real time and take preventive actions to minimize financial losses caused by fraud.

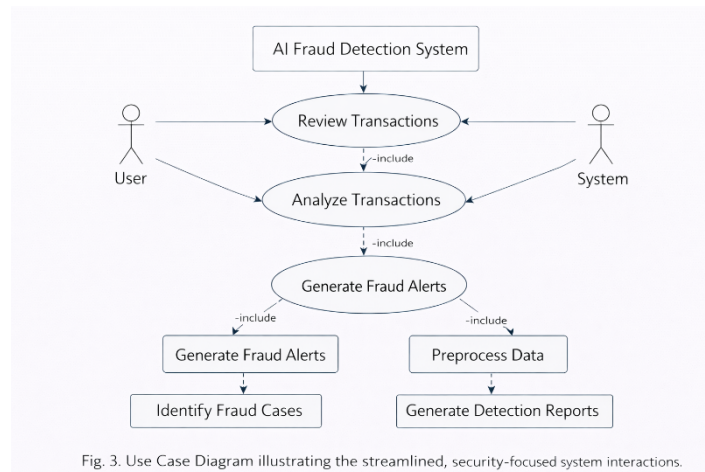


Fig. 3. Use Case Diagram illustrating the streamlined, security-focused system interactions.

Fig.3.Fig. 3. Use Case Diagram illustrating the streamlined, security-focused system interactions.

A. Transaction Processing and Fraud Detection Workflow

The uploaded transaction data is processed using Python-based data preprocessing and analysis techniques. Important transaction attributes such as transaction amount, time, location, merchant category, and user spending behavior are extracted and converted into structured data that can be used by the machine learning model. These features help the system understand normal transaction patterns and detect unusual activities.

Based on the classification results, the system determines whether a transaction is legitimate or fraudulent. If the model identifies suspicious activity, the system generates a fraud alert and records the result in the database. This workflow enables real-time monitoring and supports financial institutions in preventing fraudulent transactions effectively.

B. Transaction Evaluation and Fraud Detection Pipeline

The core analytical component of the system focuses on evaluating transaction records and identifying potential fraud cases based on transaction patterns and user behavior. Once a transaction is received, it is processed by the backend Python-based processing module, which performs structured analysis on the transaction data.

The system extracts key features from the transaction dataset and transforms them into numerical or categorical attributes suitable for machine learning algorithms. These features are then used to train and evaluate the fraud detection model.

- **Transaction Amount Analysis:**The system analyzes the transaction amount to determine whether it deviates significantly from the user's normal spending behavior. Unusually high or irregular transaction values may indicate fraudulent activity.
- **Transaction Frequency Analysis:**The model evaluates how frequently transactions occur within a specific time period. A sudden increase in transaction frequency may signal suspicious behavior.
- **Location and Time Pattern Analysis:**The system examines the geographical location and timestamp of transactions. Transactions occurring in unusual locations or at abnormal times compared to the user's typical activity may indicate potential fraud.

Based on this mathematical evaluation, the system classifies each transaction as either legitimate or fraudulent. The final prediction results are then displayed on the monitoring dashboard, where users can view the fraud detection status, risk score, and transaction details. In addition, the system provides AI-driven alerts and recommendations, such as flagging suspicious transactions, suggesting further verification, or temporarily blocking high-risk transactions. This approach helps financial institutions quickly identify potential fraud cases and take preventive actions to reduce financial losses and enhance transaction security.

C. Results Visualization and Recommendation Output

The dashboard displays important information such as transaction details, fraud detection status, and risk scores generated by the machine learning model. Graphical representations, including charts and tables, are used to highlight patterns in transaction behavior and the number of detected fraudulent transactions over time. These visualizations help users analyze trends and make informed decisions regarding transaction monitoring and fraud prevention.

In addition to visualization, the system also provides recommendation outputs when suspicious activity is detected. If a transaction is classified as potentially fraudulent, the system generates alerts and suggests appropriate actions such as verifying the transaction with the customer, temporarily blocking the transaction, or conducting further investigation. These recommendations assist financial institutions in taking immediate preventive measures and improving the overall efficiency of fraud detection and risk management.

If you want, I can also help you write the next main section of the paper (Section IV – Implementation / Experimental Results) which usually comes after Proposed Methodology in research papers.

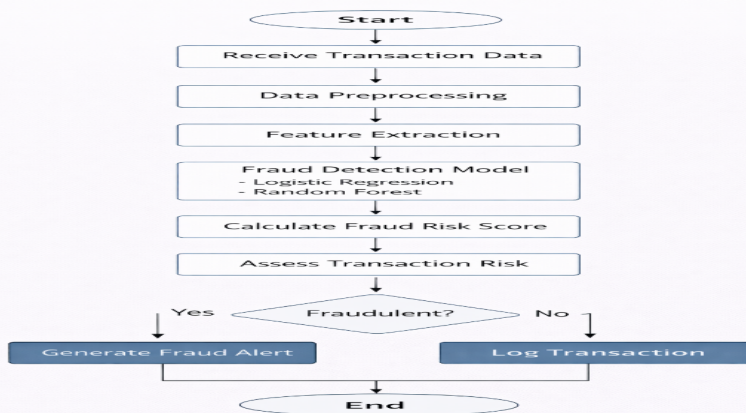


Fig. 4. System flow chart detailing the sequential execution from transaction data input to fraud alert

Fig.4 System flow chart detailing the sequential execution from transaction data input to fraud alert

IV. EVALUATION AND RESULTS

Several functional tests were conducted to evaluate the effectiveness of the proposed Machine Learning Based Credit Card Fraud Detection System. The primary focus of the evaluation was to measure the accuracy of transaction classification, the efficiency of the fraud detection model, and the system's ability to identify suspicious activities in real-time. The performance of the machine learning model was assessed using different transaction datasets containing both legitimate and fraudulent transactions.

For testing purposes, a dataset consisting of multiple credit card transactions was used to observe how the system processes transaction data with different attributes such as transaction amount, time, location, and merchant category. The system was evaluated on its ability to correctly classify transactions as either fraudulent or legitimate based on the learned patterns from historical transaction data

The experimental results demonstrated that the machine learning model was capable of identifying fraudulent transactions with a high level of accuracy. Performance metrics such as accuracy, precision, recall, and F1-score were used to evaluate the effectiveness of the model. The results indicate that the proposed system can successfully detect suspicious transaction patterns and generate alerts for potential fraud cases, thereby helping financial institutions improve security and minimize financial losses.

A. User Interface and Workflow Efficiency

The Credit Card Fraud Detection System is a web application that helps identify fraudulent credit card transactions using machine learning. It analyzes transaction data and predicts whether a transaction is fraudulent or legitimate.

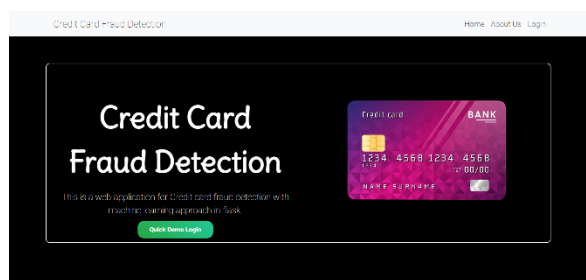


Fig.5. The homepage you see when you enter the website

The system improves security by detecting suspicious activities in real time. This helps banks and users prevent financial loss and ensure safe online payments.

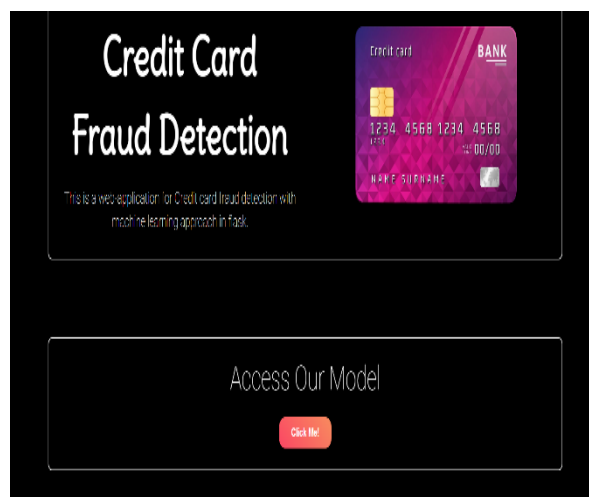


Fig.6. The option in the home to access our model

B. credit card fraud detection Auth

Users enter their username and password to authenticate their identity. It ensures that only authorized users can view and analyze transaction data.

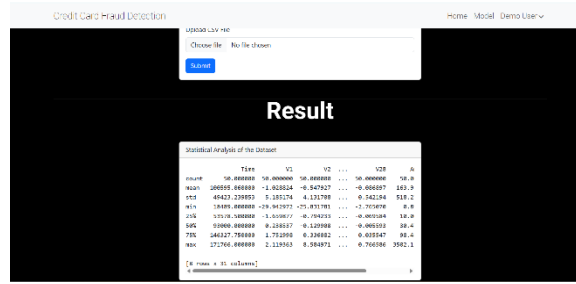
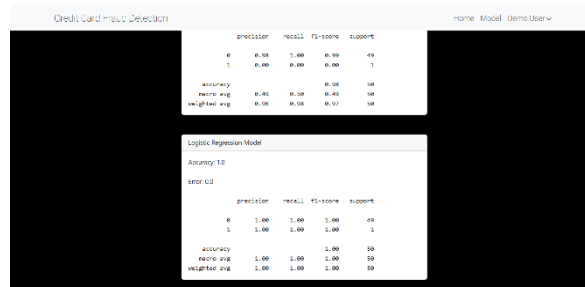


Fig.7.Thelogin page



.Fig.8.Thefinalanalysisinterfacedetailing the fraudulent transactions

It includes details such as number of records, number of features, and attribute names in the dataset. The dataset usually contains fields like transaction time, amount, and anonymized features (V1–V28). Metadata helps understand the structure, size, and characteristics of the dataset before applying machine learning models.

C. Results Visualization and Insight Generation

The Result Page displays the prediction results of different machine learning models used for fraud detection. It compares the performance of SVM, Logistic Regression, and Isolation Forest algorithms. Each model analyzes the transaction data and predicts whether it is fraudulent or legitimate.

Fig.9.Thefinallogistic regression model

Logistic Regression: Logistic Regression predicts the probability of a transaction being fraudulent or legitimate.



Fig 10. SVM model

SVM: Support Vector Machine classifies transactions by separating fraud and normal data using a decision boundary.

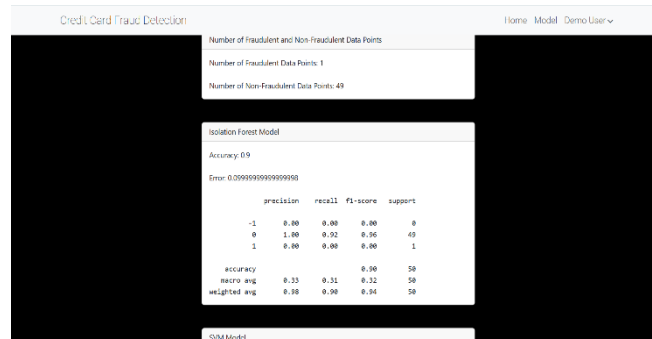


Fig 11. Isolation forest results

Isolation Forest: Isolation Forest detects fraud by identifying unusual transactions that differ from normal patterns.

V. DISCUSSION

A. Design Validation and Key Observations

Evaluating the implemented architecture reveals several practical advantages of using a scalable web framework for fraud detection applications. The decision to build the backend using Python and FastAPI, combined with a Next.js frontend, provided a stable environment for handling transaction processing and machine learning predictions efficiently.

The experimental evaluation indicates that the proposed Machine Learning Based Credit Card Fraud Detection System performs effectively within a lightweight web-based architecture. The integration of the Python backend with the Next.js frontend enabled smooth communication between the transaction monitoring interface and the fraud detection pipeline. During testing, the system successfully processed transaction datasets and applied preprocessing techniques to extract relevant features required for machine learning analysis.

The fraud detection model, implemented using Logistic Regression and Random Forest algorithms, was able to identify patterns within transaction data and classify transactions as legitimate or fraudulent with reasonable accuracy. The system calculates a fraud risk score for each transaction, which provides a clear metric for evaluating the likelihood of fraudulent activity. Additionally, the visualization of detection results through dashboards and charts improved interpretability and allowed users to quickly understand transaction behavior and potential risks.

B. Limitations and Constraints

Despite the successful implementation of the system, several limitations were observed during testing. One of the main limitations is that the accuracy of fraud detection depends heavily on the quality and diversity of the transaction dataset used for training the machine learning model. If the dataset contains limited examples of fraudulent transactions, the model may struggle to correctly identify new or unseen fraud patterns.

Another limitation is that the system currently relies on a specific set of features derived from transaction data, such as transaction amount, time, and frequency. Fraudulent activities that do not follow previously observed patterns may be difficult for the model to detect. Additionally, the experimental evaluation was conducted on a relatively limited dataset, which restricts the ability to fully assess the model's performance across large-scale real-world financial systems.

Furthermore, variations in transaction behavior across different users, regions, or financial institutions may affect the generalization capability of the model. Continuous model training and the use of larger datasets would be necessary to improve the system's accuracy and reliability in real-world scenarios.

C. Alignment with Literature Findings

The results of this project align with previous research that highlights the effectiveness of machine learning techniques in detecting credit card fraud. Several studies have demonstrated that classification algorithms such as Logistic Regression, Random Forest, and Decision Trees can successfully identify fraudulent transactions by analyzing patterns in historical transaction data.

Similarly, many fraud detection systems rely on behavioral analysis and anomaly detection techniques to identify suspicious activities. The integration of machine learning models with web-based monitoring interfaces, as implemented in this system, reflects current trends in intelligent financial security platforms.

These findings support the growing adoption of AI-driven fraud detection solutions in financial institutions, where automated systems assist in monitoring large volumes of transactions and identifying potential fraud cases more efficiently than traditional manual methods.

VI. CONCLUSION

The proposed system integrates a Supabase database, Python backend, and Next.js frontend to create a scalable and efficient web-based fraud detection platform. The system processes transaction data and extracts important features such as transaction amount, time, frequency, and behavioral patterns using Python-based data preprocessing techniques. These features are then used by the machine learning model to analyze transaction behavior and identify potential fraud.

A classification model, implemented using algorithms such as Logistic Regression and Random Forest, is used to detect suspicious transactions and classify them as either legitimate or fraudulent. The system generates a fraud risk score that helps determine the likelihood of fraudulent activity in a transaction. The results are displayed through an interactive user interface, where transaction details, fraud alerts, and prediction outcomes are visualized using charts and dashboards to improve interpretability.

Experimental testing using transaction datasets demonstrates that the system can effectively analyze transaction patterns and identify potential fraud cases with good accuracy. Overall, the proposed solution provides financial institutions with a practical tool for monitoring transactions, detecting fraudulent activities, and enhancing the security of digital payment systems.

VII. ACKNOWLEDGMENT

The authors would like to thank Bonam Venkata Chalamayya Engineering College and the Department of Computer Science and Engineering (Artificial Intelligence and Data Science) for their support in this research work.

REFERENCES

- [1] V. Kumar, V. Kumar, A. Vijayshankar and K. Pratibha, "Credit Card Fraud Detection Using Machine Learning Algorithms," International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 5, pp. 120–125, May 2020.
- [2] S. P. Maniraj, A. Saini, S. Ahmed and S. D. Sarkar, "Credit Card Fraud Detection Using Machine Learning and Data Science," International Journal of Engineering Research & Technology (IJERT), vol. 8, no. 9, pp. 110–115, Sep. 2019.
- [3] E. Ileberi, Y. Sun and Z. Wang, "A Machine Learning Based Credit Card Fraud Detection Using Genetic Algorithm for Feature Selection," Journal of Big Data, vol. 9, no. 1, pp. 1–18, Jan. 2022.
- [4] Y. Chen, "A Comparative Study of Machine Learning Models for Credit Card Fraud Detection," Academic Journal of Natural Science, vol. 2, no. 4, pp. 20–26, Dec. 2024.
- [5] L. Zhang, "Credit Card Fraud Detection Based on Machine Learning Algorithms," Applied and Computational Engineering, vol. 15, no. 2, pp. 85–92, Feb. 2025.
- [6] D. Dighe, S. Patil and S. Kokate, "Detection of Credit Card Fraud Transactions Using Machine Learning Algorithms and Neural Networks," IEEE International Conference on Computing Communication Control and Automation, pp. 1–6, Aug. 2018.
- [7] A. Dal Pozzolo, O. Caelen, Y. Le Borgne, S. Waterschoot and G. Bontempi, "Learned Lessons in Credit Card Fraud Detection from a Practitioner Perspective," Expert Systems with Applications, vol. 41, no. 10, pp. 4915–4928, Aug. 2014.
- [8] S. Bhattacharyya, S. Jha, K. Tharakunnel and J. Westland, "Data Mining for Credit Card Fraud: A Comparative Study," Decision Support Systems, vol. 50, no. 3, pp. 602–613, Feb. 2011.
- [9] R. Jurgovsky et al., "Sequence Classification for Credit Card Fraud Detection," Expert Systems with Applications, vol. 100, pp. 234–245, Jun. 2018.
- [10] J. West and M. Bhattacharya, "Intelligent Financial Fraud Detection: A Comprehensive Review," Computers & Security, vol. 57, pp. 47–66, Mar. 2016.
- [11] P. Randhawa, K. Loo, M. Sezer and S. Liu, "Credit Card Fraud Detection Using AdaBoost and Majority Voting," IEEE Access, vol. 6, pp. 14277–14284, Mar. 2018.
- [12] S. Sahin and E. Duman, "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines," International MultiConference of Engineers and Computer Scientists, vol. 1, pp. 1–6, Mar. 2011.
- [13] Y. Bahnsen, D. Aouada and B. Ottersten, "Example-Dependent Cost-Sensitive Logistic Regression for Credit Card Fraud Detection," IEEE International Conference on Machine Learning and Applications, pp. 333–338, Dec. 2014.
- [14] C. Whitrow, D. Hand, P. Juszczak, D. Weston and N. Adams, "Transaction Aggregation as a Strategy for Credit Card Fraud Detection," Data Mining and Knowledge Discovery, vol. 18, no. 1, pp. 30–55, Jan. 2009.
- [15] J. Fiore, F. De Santis, A. Perla, P. Zanetti and F. Palmieri, "Using Generative Adversarial Networks for Improving Classification Effectiveness in Credit Card Fraud Detection," Information Sciences, vol. 479, pp. 448–455, Apr. 2019.
- [16] M. Zareapoor and P. Shamsolmoali, "Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier," Procedia Computer Science, vol. 48, pp. 679–685, 2015.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)