International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2(1) (2026)

ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com

Peer Reviewed,Referred & Indexed Journal

Research Paper

REAL-TIME FINANCIAL TRANSACTION FRAUD DETECTION USING BEHAVIORAL PATTERN ANOMALIES

[1]K.Srikanth,[2]M.Laxmi prasanna,[3]D.Varshith,[4]G.Abhinay

[1]Assistant Professor, [234]Students

Department of Computer Science and Engineering

Siddhartha institute of technology & sciences,narapally

srikanthk@siddhartha.org.in,23TQ1A05A9@siddhartha.co.in,23TQ1A05C6@siddhartha.co.in, ,23TQ1A05B2@siddhartha.co.in

ABSTRACT

Financial fraud has become a major challenge for financial institutions due to the rapid growth of digital payment systems and online banking. Detecting fraudulent transactions in real time is essential to prevent financial losses and protect user accounts. This project presents a machine learning-based system for detecting fraudulent financial transactions using behavioral pattern anomalies. The system analyzes transaction attributes such as time, transaction amount, and behavioral features that represent user activity patterns. In this approach, machine learning algorithms including Logistic Regression, Decision Tree, and Random Forest are used to classify transactions as legitimate or fraudulent.

The behavioral features capture patterns such as transaction frequency, spending deviation, device usage, and merchant interaction. These patterns help the system identify unusual activities that may indicate fraud. The model is trained using historical transaction data and then deployed through a web-based interface developed using Streamlit, allowing users to input transaction details and obtain instant fraud predictions. The proposed system demonstrates effective fraud detection with high accuracy and provides a simple, interactive platform for real-time analysis of financial transactions. This project highlights the importance of machine learning techniques in improving the efficiency and reliability of fraud detection systems in modern financial environments.

Financial fraud has become a major challenge with the rapid growth of digital transactions. Traditional fraud detection systems based on static rules are no longer sufficient to detect complex and evolving fraudulent activities. This project proposes a real-time financial transaction fraud detection system using behavioral pattern anomalies and machine learning techniques.

The system analyzes user transaction behavior such as spending patterns, transaction frequency, location, and time to build a behavioral profile. Any deviation from the normal behavior is identified as a potential fraud. Advanced machine learning algorithms like Random Forest and Isolation Forest are used to improve detection accuracy and reduce false positives.

The proposed system processes transactions in real time, enabling immediate identification and prevention of fraudulent activities.

I INTRODUCTION

In recent years, the rapid advancement of digital technology has significantly transformed the financial sector. Online banking, mobile payments, digital wallets, and electronic transactions have become widely used due to their convenience, speed, and accessibility. Millions of financial transactions occur every day through credit cards, debit cards, and online payment platforms. While these technological developments have improved the efficiency of financial services, they have also increased the risk of fraudulent activities.

Financial fraud refers to illegal transactions carried out by individuals or groups with the intention of gaining unauthorized financial benefits. Common types of financial fraud include credit card fraud, identity theft, online payment fraud, and account takeover attacks. Fraudulent transactions often occur when attackers gain access to sensitive financial information such as card details, account credentials, or personal identification data. These activities can result in significant financial losses for both customers and financial institutions.

The rapid growth of digital banking, online shopping, mobile payments, and electronic transactions has significantly transformed the financial industry. People increasingly rely on digital platforms to perform daily financial activities such as transferring money, paying bills, and making purchases. Although these technologies provide convenience and efficiency, they have also increased the opportunities for cybercriminals to exploit vulnerabilities in financial systems. As a result, financial fraud has become a major concern for both financial institutions and customers. One of the key challenges in fraud detection is the large volume of financial transactions that occur every second. Manually monitoring and verifying each transaction is practically impossible for banks and financial organizations. Traditional fraud detection systems based on fixed rules are often insufficient because fraudsters continuously adapt their strategies to bypass security mechanisms. These systems may either fail to detect sophisticated fraudulent transactions or generate a large number of false alarms, which can inconvenience legitimate users. The motivation for this project arises from the need to develop an intelligent and automated system capable of identifying fraudulent transactions effectively. Machine learning techniques provide an efficient way to analyze large datasets and recognize patterns in transaction behavior. By learning from historical transaction data, machine learning models can distinguish between normal and suspicious activities. Algorithms such as Logistic Regression, Decision Tree, and Random Forest are widely used to detect fraud by classifying transactions based on their characteristics.

II LITERATURE SURVEY

Paper 1: U. Dornadula and S. Geetha (2019)

Title: Credit Card Fraud Detection Using Machine Learning Algorithms.

Approach: The authors used machine learning techniques to analyze transaction data and identify fraudulent activities. The study applied classification models to detect fraud based on transaction behavior patterns. Accuracy: The model achieved approximately 97–98%

accuracy in fraud detection. Limitations: Dataset imbalance affected the detection of rare fraud cases.

Paper 2: A. Dal Pozzolo, O. Caelen (2015)

Title: Calibrating Probability with Under sampling for Unbalanced Classification in Credit Card Fraud Detection.

Approach: The study applied several machine learning algorithms including Random Forest, Logistic Regression, and Gradient Boosting to detect fraud in highly imbalanced transaction datasets. Accuracy: The Random Forest model achieved nearly 99% detection accuracy with a high AUC score. Limitations: High computational complexity for large datasets.

Paper 3: S. Afriyie, S. A. Yeboah, and J. K. Panford(2023)

Title: A Supervised Machine Learning Alhorithm for Detecting Credit Card Fraud.

Approach: The study compared multiple supervised learning algorithms including Logistic Regression, Decision Tree, and Random Forest to classify fraudulent transactions. Accuracy: Random Forest achieved approximately 96% accuracy with high precision and recall. Limitations: Performance depends on proper datasets balancing.

Paper 4: P. K. Chan and S. J. Stolfo (1998)

Title: Toward Scalable Learning with Non-Uniform Class and Cost Distribution.

Approach: The research applied machine learning algorithms including K-Nearest Neighbor, Logistic Regression, and Random Forest to detect fraudulent transactions in large datasets.

III SYSTEM ANALYSIS

Financial fraud detection systems aim to identify suspicious transactions by analyzing user behavior patterns in real time. Traditional rule-based systems rely on predefined thresholds such as transaction limits, location mismatches, or unusual spending amounts. However, modern fraud techniques are adaptive and often bypass static rules, making traditional systems less effective.

The proposed system focuses on behavioral anomaly detection, where each user's normal transaction pattern is learned using machine learning models. Features such as transaction frequency, time of purchase, device information, geolocation, and spending habits are analyzed. Any deviation from the learned behavior is flagged as a potential fraud.

Real-time processing is a critical component of this system. Streaming frameworks process incoming transactions instantly, ensuring immediate detection and response. The system integrates data preprocessing, feature extraction, model training, and anomaly detection into a unified pipeline

Existing system

Existing fraud detection systems mainly depend on rule-based techniques and simple statistical methods. These systems use predefined conditions such as transaction amount limits, unusual locations, or frequency thresholds. Banks and financial institutions implement these rules to detect suspicious activities. However, these systems are static and require continuous manual updates. They struggle to adapt to new fraud patterns and often fail in real-time detection. As a result, fraudsters can exploit loopholes in these systems.

DisAdavantages of Existing system

- Static rules cannot detect evolving fraud patterns
- High false positive rate
- Requires frequent manual updates
- Limited real-time detection capability
- Inefficient for large-scale transaction data

Proposed system

The proposed system uses machine learning and behavioral analytics to detect fraud in real time. It builds user profiles based on historical transaction data and identifies anomalies in behavior. Advanced algorithms such as Random Forest, Isolation Forest, and Neural Networks are used for prediction. The system processes streaming data to detect fraud instantly. It continuously learns and updates patterns to improve accuracy. This makes the system adaptive, scalable, and efficient for modern financial environments.

Advantages of Proposed System

- Real-time fraud detection
- Adaptive learning from new data
- Reduced false positives
- Handles large-scale data efficiently
- Detects complex behavioral anomalies

IV METHODOLOGY

The methodology begins with data collection from financial transaction datasets, including attributes like transaction ID, timestamp, amount, location, and user details. The collected data undergoes preprocessing, where missing values are handled, and noise is removed. Feature engineering is then applied to extract behavioral patterns such as average spending, transaction intervals, and location consistency.

Next, the dataset is divided into training and testing sets. Machine learning models such as Logistic Regression, Random Forest, and Isolation Forest are trained to identify fraudulent transactions. Supervised learning is used when labeled data is available, while unsupervised techniques help detect unknown fraud patterns.

The trained model is deployed in a real-time environment where incoming transactions are continuously monitored. Each transaction is analyzed against learned behavioral patterns, and

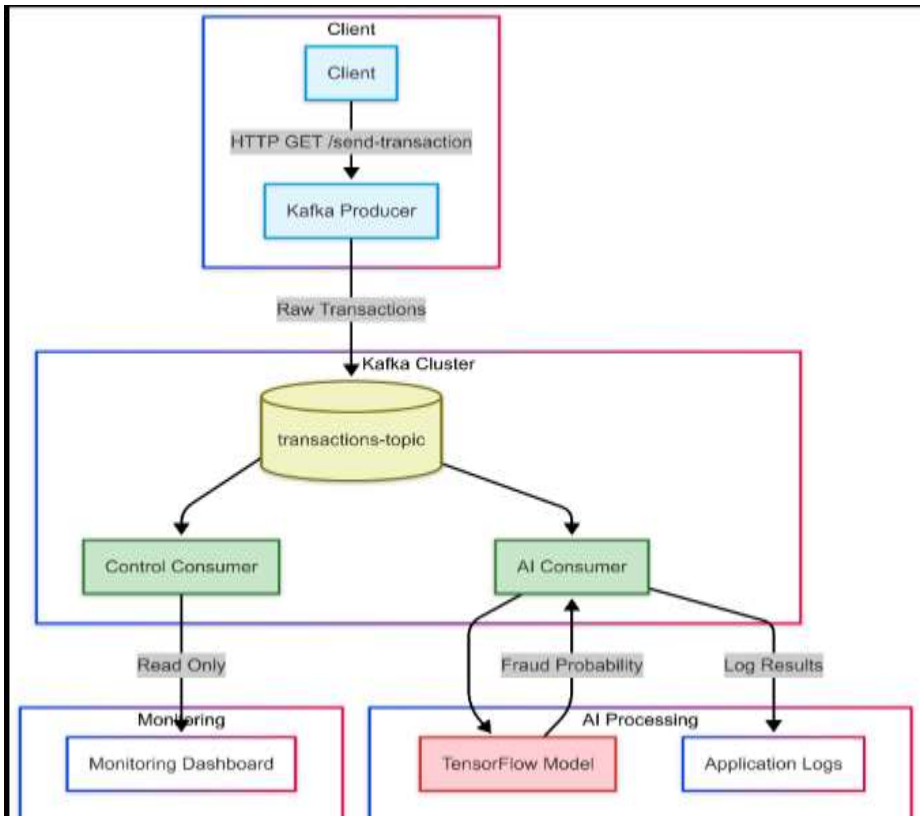
anomalies are flagged instantly. Performance metrics like accuracy, precision, recall, and F1-score are used to evaluate the system.

Finally, a feedback mechanism is incorporated to update the model based on new fraud cases, ensuring continuous improvement and adaptability to emerging threats.

System Architecture

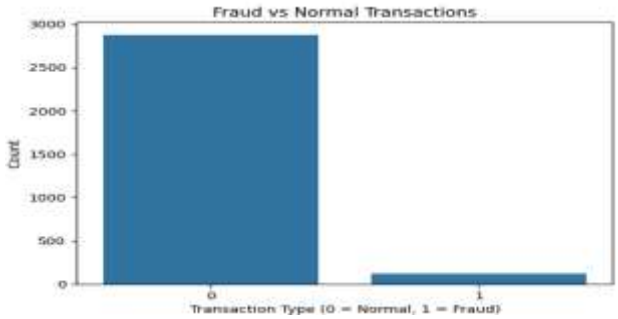
The system architecture consists of multiple layers working together for real-time fraud detection. The data collection layer gathers transaction data from banking systems. The preprocessing layer cleans and transforms data into usable formats. Feature engineering extracts meaningful attributes such as transaction frequency, amount patterns, and location.

The model layer applies machine learning algorithms to classify transactions as normal or fraudulent. A real-time processing engine (like streaming systems) ensures instant analysis. The alert system notifies users or banks when suspicious activity is detected. Finally, a feedback loop updates the model with new data to improve accuracy continuously.

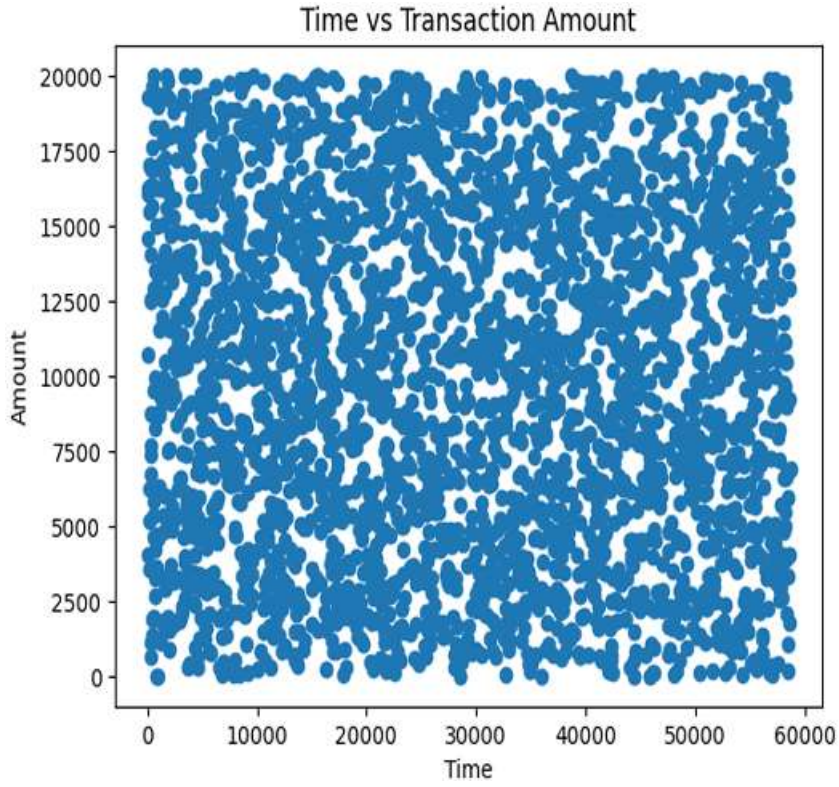


V RESULTS &OUTPUT

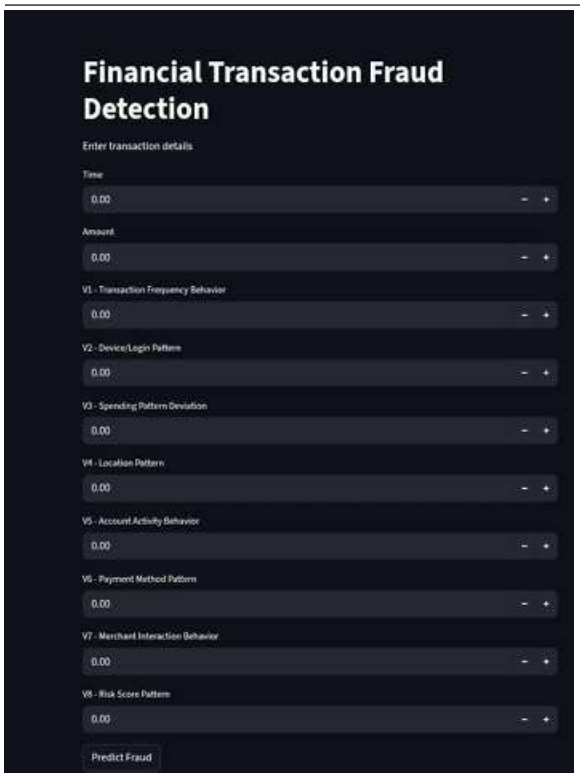
Fraud vs Normal Transaction



Time vs Transaction Amount



Transaction Application



VI CONCLUSION

The Financial Transaction Fraud Detection System developed in this project demonstrates the effective use of machine learning techniques to identify fraudulent activities in financial transactions. With the increasing use of digital payment systems and online banking, financial fraud has become a significant challenge for financial institutions. Therefore, developing intelligent systems capable of detecting suspicious transactions is essential for ensuring financial security. In this project, machine learning algorithms were applied to analyze transaction data and identify patterns associated with fraudulent behavior. The system uses important transaction attributes such as transaction time, transaction amount, and behavioral pattern features to classify transactions as legitimate or fraudulent. By learning from historical transaction data, the model can detect anomalies and unusual transaction patterns that may indicate fraud. One of the key strengths of this system is its ability to automate the fraud detection process. Instead of relying solely on manual monitoring or traditional rule-based methods, the system uses intelligent algorithms to analyze large volumes of transaction data efficiently. This enables faster detection of fraudulent activities and reduces the workload for financial analysts. The system also integrates a user-friendly interface that allows users to enter transaction details and obtain prediction results easily. This makes the system practical and accessible for analyzing financial transactions and detecting fraud in a simplified manner. Although the system has some limitations such as dataset imbalance and dependence on training data, it demonstrates that machine learning-based approaches can

significantly improve fraud detection accuracy compared to traditional rule-based systems. The experimental results show that the model achieves high accuracy and consistent performance, indicating its effectiveness in identifying fraudulent transactions.

REFERENCE

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.

[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.

[3] Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm

[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.

[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, “Real-Time Object Detection in Drone Surveillance Using YOLOv5,” in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.

[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, “Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks,” in Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.

[7] R. D. Kumar, V. N. S.Manaswini, “Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology,” in Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.

[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, “An advanced movie recommender using collaborative filtering and sentiment analysis,” International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.

[9] Ravi Kumar Banoth, Ramana Murthy B V, “Automatic crop recommendation system using LightGBM and decision tree machine learning models,” Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.

[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.

[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.