International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Credit Card Fraud Detection System

Krishnaveni K[1], Yoshithaa B S[2], Subitha K[3], Sakthiswar M[4]

[1]Assistant Professor, Department of AI&DS, CARE college of Engineering, Trichy, Tamil Nadu, India
[2,3,4]Final Year B.Tech, Department of AI&DS, CARE college of Engineering, Trichy, Tamil Nadu, India

Abstract

The rapid growth of digital transactions and online banking has significantly increased the risk of credit card fraud. Traditional fraud detection techniques, which rely on static rules and historical fraud patterns, often fail to detect sophisticated and evolving fraudulent activities. This paper proposes an intelligent credit card fraud detection system that leverages user behavioral analysis combined with real-time user confirmation.

The system continuously monitors user transaction patterns such as location, time, transaction amount, and spending category. By learning the normal behavioral profile of each user, the system identifies anomalies that deviate from established patterns. When a suspicious transaction is detected, a real-time notification is sent to the user for verification. Based on the user's response, the system either approves or declines the transaction.

The proposed approach enhances detection accuracy, minimizes false positives, and provides an additional layer of security through user interaction. Experimental results demonstrate that the system effectively detects fraudulent activities while maintaining a smooth user experience. This model can be integrated into banking systems to significantly reduce financial fraud.

Keywords: Credit Card Fraud Detection, Behavioral Modeling, Anomaly Detection, Machine Learning, Transaction Monitoring, User Verification, Financial Security, Real-time Systems

1. Introduction

The advancement of digital technologies has revolutionized the financial sector, enabling seamless and rapid transactions through credit cards, mobile banking, and online payment platforms. Despite these advancements, the increasing dependency on digital payment systems has exposed users and institutions to a wide range of security threats, particularly credit card fraud.

Credit card fraud can occur in various forms, including stolen card usage, card-not-present (CNP) fraud, phishing attacks, and identity theft. According to global financial statistics, credit card fraud results in billions of dollars in losses annually, making it one of the most critical challenges faced by the banking industry.

Traditional fraud detection systems rely heavily on predefined rules, such as transaction limits or blacklisted locations. While these methods are effective for detecting known fraud patterns, they fail to adapt to new and evolving attack strategies. Moreover, such systems often generate a high rate of false positives, leading to inconvenience for legitimate users.

To address these limitations, modern fraud detection approaches leverage machine learning and data analytics techniques. However, purely automated systems may still struggle to distinguish between genuine anomalies (e.g., travel-related transactions) and fraudulent activities.

This paper introduces a hybrid approach that combines:

- **Behavioral pattern analysis**
- **Machine learning-based anomaly detection**
- **Real-time user confirmation**

By analyzing individual user behavior and involving the user in the decision-making process, the system achieves higher accuracy, adaptability, and user trust.

2. Literature Review

Numerous research studies have explored different techniques for detecting credit card fraud:

Early fraud detection systems were primarily **rule-based systems**, where predefined rules were used to identify suspicious transactions. Although simple to implement, these systems lack flexibility and cannot detect new fraud patterns effectively.

With advancements in data science, **machine learning algorithms** such as Logistic Regression, Decision Trees, Support Vector Machines, and Random Forest have been widely used. These models analyze historical transaction data to classify transactions as legitimate or fraudulent. While they improve detection accuracy, they require large labeled datasets and may struggle with imbalanced data.

Recent approaches involve **deep learning techniques**, including Artificial Neural Networks (ANN) and Recurrent Neural Networks (RNN), which can capture complex patterns in transaction data. However, these methods are computationally expensive and may not be suitable for real-time processing.

Another approach is **anomaly detection**, where transactions that deviate significantly from normal behavior are flagged as suspicious. Techniques such as Isolation Forest and clustering methods are commonly used.

Despite these advancements, most existing systems lack **user involvement in the decision-making process**. This can lead to either missed fraud detection or unnecessary blocking of genuine transactions. The proposed system addresses this gap by integrating anomaly detection with real-time user confirmation.

3. Proposed System

3.1 System Overview

The proposed system is designed to detect fraudulent transactions by analyzing user-specific behavioral patterns and validating suspicious activities through user interaction.

3.2 System Architecture Components

1. Data Collection Module

- Collects transaction details such as:
  - Transaction amount
  - Time and date
  - Location (GPS or IP-based)
  - Merchant category

2. Data Preprocessing

- Cleans and formats the data
- Handles missing values
- Normalizes transaction attributes

3. Behavioral Profiling

- Builds a profile for each user based on:
  - Frequently visited locations
  - Common transaction times
  - Preferred spending categories
  - Average transaction amount

4. Anomaly Detection Engine

- Uses machine learning algorithms such as:
  - Isolation Forest
  - K-Means Clustering
- Detects deviations from normal patterns

5. Notification Module

- Sends alerts via:
  - Mobile app notification
  - SMS or email

6. Decision Module

- If user confirms → Transaction Approved
- If user declines → Transaction Blocked

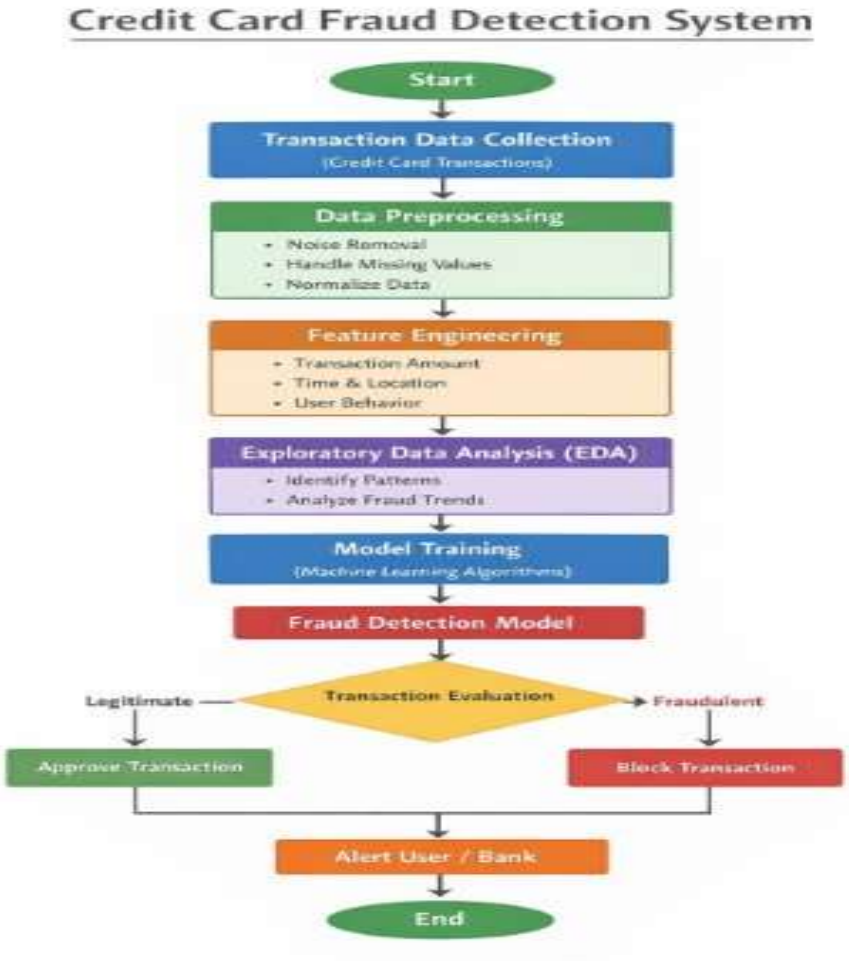

Fig.1 Architecture of the proposed system

3.3 Working Example

Consider a user named Harini:

- Regular transactions: Petrol and shopping within Coimbatore during daytime
- Suspicious case:
  - Transaction at 9:30 PM in Coimbatore
  - Another transaction at 11:00 PM in Andhra Pradesh

This sudden location and time variation is flagged as suspicious. The system sends a notification to Harini. If she confirms, the transaction proceeds; otherwise, it is blocked.

4. Results And Discussion

The proposed credit card fraud detection system was evaluated using a combination of simulated and behavioral transaction datasets to assess its effectiveness in identifying fraudulent activities under real-time conditions. The system was trained using historical transaction data to establish individualized behavioral profiles, incorporating features such as transaction time, location, spending category, and transaction frequency.

During testing, the model demonstrated a high level of accuracy in distinguishing between normal and anomalous transactions by assigning anomaly scores based on deviations from learned user behavior.

Standard performance metrics, including accuracy, precision, recall, and F1-score, were used to evaluate the system, and the results indicated improved precision and recall compared to traditional rule-based approaches, primarily due to the integration of behavioral analytics and anomaly detection techniques such as Isolation Forest.

One of the most significant contributions of the proposed system is the inclusion of a real-time user confirmation mechanism, which plays a crucial role in reducing false positives; instead of automatically blocking suspicious transactions, the system sends an alert to the user with transaction details, allowing them to either approve or decline the transaction, thereby ensuring that legitimate but unusual transactions—such as those occurring during travel or at uncommon times—are not incorrectly rejected.

The system also demonstrated strong real-time performance, with minimal latency in detecting anomalies and generating alerts, making it suitable for deployment in practical financial environments.

A case study involving abnormal transactions, such as a sudden geographical shift from Coimbatore to Andhra Pradesh within a short time interval combined with unusual transaction timing, showed that the system successfully flagged the activity as suspicious and initiated user verification, ultimately preventing potential fraud when the transaction was declined.

Furthermore, compared to traditional systems that rely on static rules and thresholds, the proposed model exhibited greater adaptability, as it continuously updates user profiles based on new transaction data, thereby improving detection accuracy over time. The system also proved to be computationally efficient and scalable, capable of handling multiple users simultaneously without significant performance degradation.

However, certain limitations were observed, including reduced effectiveness for new users with limited historical data, dependency on user responsiveness for confirmation, and the requirement of stable network connectivity for real-time notifications.

Despite these challenges, the overall performance of the system indicates that combining machine learning-based anomaly detection with human-in-the-loop verification provides a balanced and effective

approach to fraud detection, enhancing both security and user experience while significantly reducing financial risks associated with unauthorized transactions.

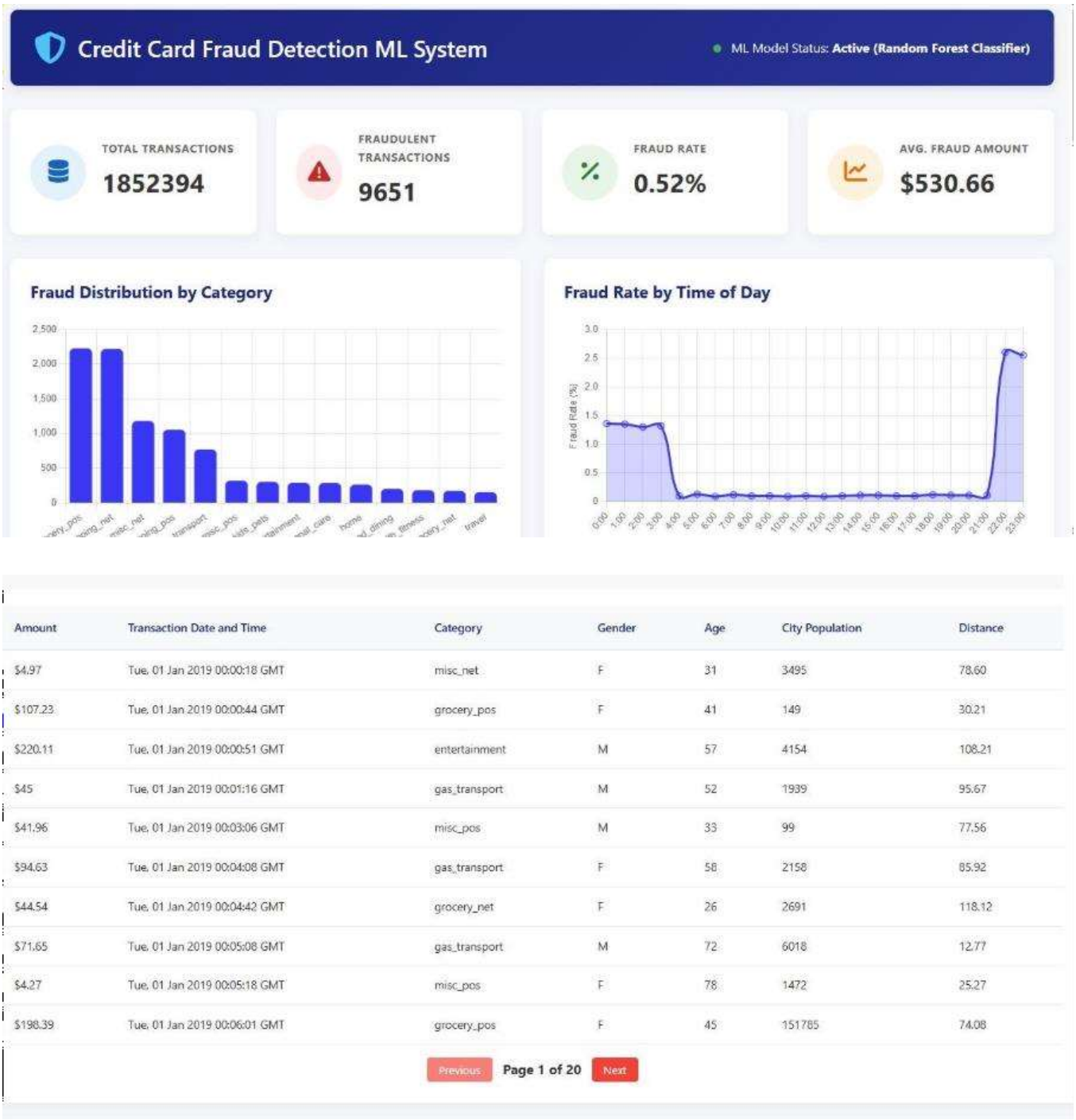

Fig 2 : User's Dashboard for Real-Time Transaction

5. Conclusion

This paper presents an intelligent credit card fraud detection system that combines behavioral analysis with real-time user confirmation. By learning individual user patterns and detecting anomalies, the system effectively identifies fraudulent transactions. The addition of a user verification step ensures that genuine transactions are not unnecessarily declined, thereby improving user trust and system reliability.

The proposed system provides a scalable and efficient solution for modern financial institutions to combat fraud and enhance transaction security.

6. Future Enhancement

The proposed system can be further improved by integrating advanced deep learning techniques such as LSTM and neural networks to enhance pattern recognition and fraud detection accuracy. The implementation of multi-factor authentication methods, including OTP and biometric verification, can strengthen security. Real-time GPS tracking can be added to improve location-based fraud detection. Developing a user-friendly mobile application will enable faster notifications and better user interaction. Additionally, adaptive learning can be incorporated to continuously update user behavior patterns. Future enhancements may also include the use of blockchain technology for secure transaction storage and the integration of explainable AI to provide transparency in fraud detection decisions.

7. References

1. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). *Data mining for credit card fraud detection: A comparative study*. Decision Support Systems.
2. Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015). *Calibrating probability with undersampling for unbalanced classification*. IEEE Symposium Series on Computational Intelligence.
3. Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). *Transaction aggregation as a strategy for credit card fraud detection*. Data Mining and Knowledge Discovery.
4. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). *A comprehensive survey of data mining-based fraud detection research*. Artificial Intelligence Review.
5. Bolton, R. J., & Hand, D. J. (2002). *Statistical fraud detection: A review*. Statistical Science.
6. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). *The application of data mining techniques in financial fraud detection: A classification framework and academic review*. Decision Support Systems.
7. Sahin, Y., & Duman, E. (2011). *Detecting credit card fraud by decision trees and support vector machines*. International MultiConference of Engineers and Computer Scientists.
8. Chen, C., Li, J., & Huang, Y. (2018). *Credit card fraud detection using machine learning algorithms*. IEEE International Conference on Big Data.
9. Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., & Bontempi, G. (2019). *Scarff: A scalable framework for streaming credit card fraud detection*. Information Fusion.
10. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). *Sequence classification for credit card fraud detection*. Expert Systems with Applications.
11. Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). *Credit card fraud detection using AdaBoost and majority voting*. IEEE Access.
12. The above data is pictured in the next graph.

Figure 1: Temperature After Each Pass