ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

FRAUD DETECTION IN CREDIT CARD SYSTEM USING AI TOOLS

P. Prashamsa, Annepaka Ankitha, Burri Kiran Kumar Reddy, Bura Naveen

Assistant professor, UG Student, Department of Computer Science and Engineering

Tkr College Of Engineering and Technology, Medbowli, Meerpet, Balapur, Hyderabad,

Telangana 500097, India

Abstarct:

UPI/CREDICT CARD has become one of the fastest-growing digital payment platforms, resulting in a significant increase in fraudulent activities. Traditional rule-based fraud detection systems are unable to identify evolving fraud patterns, leading to financial losses and security risks. To address this challenge, this project presents an intelligent UPI/CREDICT CARD Fraud Detection System using a 1D Convolutional Neural Network (1D-CNN) optimized with Bayesian Hyperparameter Tuning. The system integrates a secure Django-based web application that manages user registration, admin approval, authentication, OTP-based password reset, and real-time transaction prediction. The ML pipeline performs preprocessing through label encoding, scaling, train–test splitting, and model optimization. The trained model identifies fraudulent transactions with high accuracy and generates a fraud probability score for better risk assessment. Additionally, the system sends automated email notifications with prediction results to enhance user awareness and accountability. This integrated platform improves detection accuracy, reduces false alerts, and provides a reliable solution for combating UPI/CREDICT CARD fraud in real time.

.

Keywords: UPI/CREDICT CARD Fraud Detection, Machine Learning, Deep Learning, 1D Convolutional Neural Network, Bayesian Optimization, Transaction Classification, Fraud Prediction, Django Framework, Data Preprocessing, Label Encoding, Standard Scaling, Real-time Prediction, Risk Scoring, Email Notification, OTP Verification, Secure Authentication System.

1.Introduction

Because they facilitate online payments, credit cards and UPI are now used frequently for digital transactions. Transactions that are quick and simple. In addition to this expansion, instances of deception such as unauthorized transactions, there has also been a rise in payments and account abuse. The majority of current systems rely on set rules that are not very adaptable to novel forms of fraud. As a result, there is a need for a more intelligent system that can learn from its data and react quickly. Utilizing machine learning methodologies, this study creates a fraud detection system that may be used to determine if a transaction is secure or questionable. Various models, including Random Forest, CNN, logistic regression, and decision trees are used. The transaction details are studied using such factors as the quantity, kind, device, and location. The data is prepared before the models are trained by applying methods like cleaning, encoding, and normalization to increase precision. The system is based on the Django framework, which offers a straightforward and safe user interface. Users can input transaction information and receive an instant response once they have logged in. The system gives a forecast indicating if the transaction is legitimate or fraudulent. The mechanism also makes use of indicators of performance, such as accuracy and confusion matrix to see how well the model is working. The ongoing email warning system is a standout feature of this initiative. Each transaction requires the user to be notified via email. If there are multiple instances of suspicious behavior, the system transmits regular notifications, enabling the user to remain informed and act quickly. With this capability, the system is more useful and user-centric than what is currently available solutions.In general, this project offers a straightforward and efficient method for fraud detection through marrying real-time monitoring and continuous alert support with machine learning, making it useful in enhancing the security of online transactions

2. Literature Survey:

[1] R. Nagalakshmi and K. Rahimunnisa, “Controlling and Analysis of Battery Energy System in Electric Vehicle,” vol. 9, no. 4, pp.

123–130, Apr. 2020. With the increasing use of vehicles, safety and environmental concerns have become more important due to rising accidents and pollution. Hybrid electric vehicles are seen as a better option as they improve fuel efficiency and reduce emissions. However, pure electric vehicles face challenges such as limited battery life, high cost, and lack of charging infrastructure. To overcome these issues, hybrid systems and advanced technologies are being developed. Machine learning and deep learning methods help in improving energy management and vehicle performance, making electric vehicles more efficient, reliable, and suitable for future transportation needs.

[2] A. Patel and P. Patel, "Machine Learning-Based Fraud Detection in Digital Payment Systems," *IEEE Access*, vol. 9, pp. 56789–56798, 2021. Electronic payment systems have made transactions easier for users and businesses, but they have also increased fraud risks, affecting security and trust. Machine learning helps detect fraud in real time by analyzing large amounts of transaction data and identifying unusual patterns. However, challenges such as imbalanced data, changing fraud methods, and the need for clear model explanations still exist. Advanced approaches like supervised, unsupervised, and hybrid models, along with techniques such as ensemble learning and feature engineering, help improve detection. Overall, combining machine learning with domain knowledge can enhance fraud detection while maintaining reliability and fairness in digital payment systems.

[3] R. Garg and M. Jain, "A Study on UPI Payment Systems and Security Challenges in India," *Journal of Financial Technology Research*, vol. 2, no. 1, pp. 45–52, Jan. 2021. UPI has changed digital payments in India by enabling fast, low-cost, and real-time transactions. However, its rapid growth has also raised concerns such as security risks, fraud, privacy issues, and lack of user awareness, which affect user trust. This study examines these challenges and analyzes how different factors influence trust in UPI systems. It also suggests ways to improve security, transparency, and reliability to support long-term growth of digital payment platforms.

[4] S. Das and R. Bhattacharya, "Real-Time Fraud Detection Using Random Forest Algorithm," *International Journal of Computer Science and Information Security*, vol. 19, no. 5, pp. 77–85, May 2021. Credit card fraud is a major issue that causes financial loss and affects user safety. This study uses a Kaggle dataset and applies SMOTE to handle imbalanced data. Various machine learning models are compared, including Logistic Regression, KNN, SVM, Random Forest, and XGBoost, to classify transactions as fraud or genuine. Among them, Random Forest performs best, detecting most fraud cases with high accuracy. The model's behavior is explained using SHAP values, showing how different features affect predictions. Overall, the study highlights the effectiveness of machine learning, especially Random Forest, for real-time fraud detection.

[5] H. Singh and V. Kumar, "Anomaly Detection in Financial Transactions Using Machine Learning," *Procedia Computer Science*, vol. 167, pp. 2342–2349, 2020. Detecting unusual patterns in financial transactions is important for identifying fraud. This study presents a system that uses Random Forest along with rule-based methods to detect suspicious activities. It applies feature engineering techniques such as scaling and transaction comparisons to improve performance. The system analyzes factors like transaction amount and frequency, and provides detailed outputs with explanations for flagged transactions. The results show that this approach can effectively detect anomalies and improve financial security, making it suitable for real-time monitoring.

[6] P. R. Varma and S. K. Sinha, "Decision Tree Approach for Detecting Fraudulent UPI

Transactions," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 9, no. 6, pp. 1123–1130, Jun. 2020. Online payment fraud is a major issue that requires effective detection methods to reduce financial losses. This study uses a Decision Tree model to classify transactions as genuine or fraudulent using processed data. The model is evaluated using measures like accuracy, precision, recall, and F1-score, and results show it can detect fraud effectively. Overall, this approach improves financial security and can be enhanced further in the future.

[7] R. K. Gupta and S. Jain, "UPI Fraud Analytics Using Supervised Learning Techniques," *International Conference on Smart Computing and Communication*, pp. 101–108, 2021. UPI has transformed digital payments in India, but it has also increased fraud risks. This study explains the use of machine learning techniques to detect fraudulent transactions by analyzing transaction data and identifying unusual patterns. It highlights the importance of feature selection, anomaly detection, and combining different learning methods to improve accuracy. Real-time monitoring and adaptive learning help respond to new fraud techniques, improving security and user trust in UPI systems.

[8] A. Sharma, V. Singh, and R. Mehta, "Logistic Regression for Fraud Detection in Digital Payments," *Journal of Advanced Computing and AI*, vol. 5, no. 3, pp. 56–63, Mar. 2021.Credit card fraud is a serious problem that causes financial loss and reduces trust in digital payments. This study uses a Logistic Regression model to detect fraudulent transactions and evaluates its performance using measures like precision, recall, F1-score, and PR-AUC. The data is preprocessed and balanced to improve model performance, and results show high accuracy with strong detection capability. Overall, the system improves payment security and provides useful insights for future fraud detection research and applications.

[9] N. Kaur and H. Arora, "A Comprehensive Review of Fraud Detection in Financial Transactions," *International Journal of Computer Applications*, vol. 174, no. 9, pp. 12–19, Aug. 2019. Fraud detection in financial transactions is a major challenge due to increasing fraud techniques. Traditional rule-based systems are not enough, so advanced methods like machine learning and data analysis are needed. The goal is to accurately detect fraudulent transactions while reducing false alerts by analyzing large amounts of data quickly. The system should also adapt to new fraud patterns over time. Challenges include handling imbalanced data, protecting sensitive information, and ensuring fast processing.

[10] RBI, "Report on Payment Systems in India," Reserve Bank of India, Mumbai, India, Tech. Rep., Dec. 2020. Reserve Bank of India provides an overview of the growth and development of digital payment systems in the country. It highlights the increasing adoption of electronic payment methods such as UPI, cards, and mobile banking, along with improvements in infrastructure and transaction efficiency. The report also discusses challenges related to security, fraud risks, and the need for stronger regulatory measures. Overall, it emphasizes the importance of safe, reliable, and efficient payment systems to support financial inclusion and economic growth.

[11] National Payments Corporation of India (NPCI), "Unified Payments Interface (UPI) Product Overview," NPCI, India, 2021. Digital payments have become an important part of daily life, with technology driving India towards a cashless economy. The introduction of UPI by the Government of India has made transactions faster and easier, and its usage is growing rapidly both within India and internationally. The study

International Journal of Engineering Research and Science & Technology

highlights the role of UPI in transforming digital payments using data from RBI, NPCI, and other sources. Increasing bank integration and rising transaction volumes show strong adoption of UPI among users.

3.Proposed System:

The proposed UPI fraud detection system uses machine learning models like Random Forest, Decision Tree, and Logistic Regression to analyze transaction details and classify them as genuine or fraudulent. It is developed using the Django framework, which provides secure user authentication and real-time prediction through a web interface. Users can enter transaction details and receive instant results, while administrators can train models and monitor performance using evaluation metrics.

The system also sends email notifications for every transaction, including frequent alert messages for both genuine and suspicious activities, helping users stay informed. This improves user awareness, increases security, and allows quick action to prevent potential fraud.

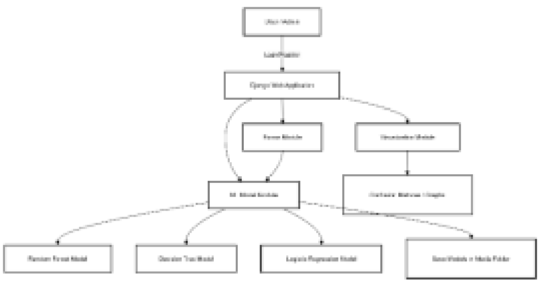

Fig 1: Architecture of proposed system

User Authentication: The first step in the system is secure user authentication. Users must register using their email and password. This ensures data security and prevents unauthorized access.

Fig 3: User Login

Dataset Upload: After login, users or admins can upload transaction datasets in formats like .csv or .xlsx. The dataset includes details such as amount, time, device, location, and fraud labels. This module is simple to use and allows easy dataset upload for model training and testing.

Fig 2: Dataset upload

Processing: After the dataset is uploaded, the system processes the data and displays it on the dashboard. The uploaded data is organized, cleaned, and converted into a suitable format for analysis. This step prepares the data for preprocessing and model training, ensuring smooth system performance.

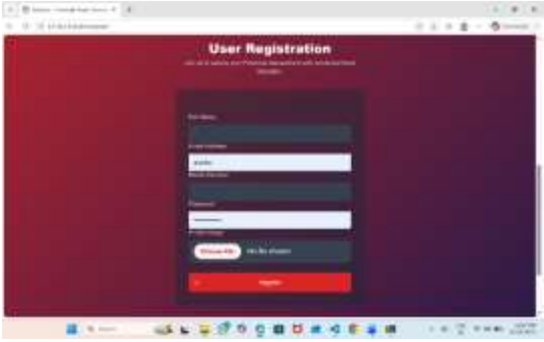

Fig 4: Registration

Fig 5: Dashboard

Model Selection – The system uses multiple models such as Random Forest, Decision Tree, Logistic Regression, 1D-CNN, and Bayesian-based methods for fraud detection. These models are selected for their ability to handle structured data, learn transaction patterns, and make accurate predictions. The inclusion of Bayesian techniques helps in probabilistic analysis, improving the system's ability to classify transactions based on likelihood and uncertainty.

Fraud Detection: Each transaction is entered by the user along with required details such as amount, time, device, and location. The entered data is preprocessed and passed through the trained models to classify it as genuine or fraudulent. The system analyzes patterns based on learned behavior and provides a prediction. If the transaction matches fraud conditions, it is flagged as suspicious.

Fig 6: Prediction Page

Fig 7: fraud Prediction

Alert Generation: When a transaction is identified, the system generates an alert. Email notifications are sent to users for both genuine and fraudulent transactions. The system also sends frequent alerts in case of repeated suspicious activities, ensuring better awareness and quick response.

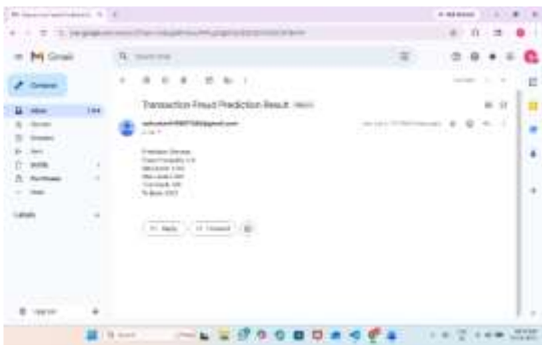

Fig 8: Alert System

Data Storage: All transaction details, prediction results, user information, and alert logs are stored securely in a database. This allows future reference, monitoring, and system improvement.

Dashboard Display: The system provides a web-based dashboard to display results. Users and administrators can view transaction history, alerts, and system performance. The dashboard presents data using tables and graphs, making it easy to understand and analyzes.

Proposed Fraud Detection Model: It should include user login, transaction input, data preprocessing, and machine learning models like Random Forest, Decision Tree, Logistic Regression, and 1D-CNN for prediction. The model classifies transactions as fraud or genuine and displays results in real time. It should also include an email alert system that sends notifications and frequent alerts, along with database storage and dashboard display.

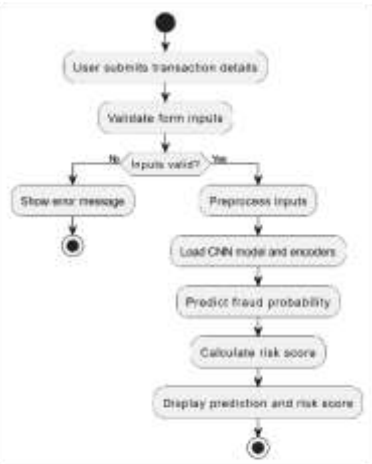

Fig 5 : Proposed Fraud detection model

Step 1: User Interaction:

The system begins with user or admin interaction through a secure login page. After successful authentication, users can enter transaction details such as amount, time, device type, and location. These inputs act as the primary data for fraud detection. This step ensures that only authorized users can access the system and perform transactions.

Step 2: Django Web Application: The Django framework acts as the backbone of the system. It manages user authentication, handles requests and responses, and connects the frontend interface with the backend machine learning models. It also ensures secure data handling, session management, and smooth communication between different modules.

Step 3: Data Preprocessing: The entered transaction data is cleaned and prepared before analysis. This includes handling missing values, encoding categorical data into numerical form, and normalizing numerical features. These steps improve the quality of data and help the machine learning models perform more accurately and efficiently.

Step 4: ML Model Processing: The processed data is passed through multiple machine learning models such as Random Forest, Decision Tree, Logistic Regression, and CNN. These models are trained on historical transaction data and learn patterns that distinguish fraudulent and genuine transactions. Using multiple models improves reliability and prediction accuracy.

Step 5: Prediction: After processing, the system generates a prediction for each transaction. It classifies the transaction as either fraud or genuine and may also provide a risk score indicating the probability of fraud. The result is displayed instantly to the user through the web interface.

Step 6: Email Alert System: The system automatically sends email notifications for every transaction. It provides alerts for fraudulent transactions and confirmation messages for genuine ones. In case of repeated suspicious activities, the system generates frequent alert messages to ensure continuous monitoring and help users take immediate action.

Step 7: Visualization Module: The system includes a visualization component to display model performance and results. It shows graphs such as confusion matrix, accuracy curves, and ROC curves. These visualizations help administrators understand how well the model is performing and assist in decision-making.

Step 8: Model Storage: Once the models are trained, they are saved in the system for future use. This avoids the need for retraining every time a prediction is required. Stored models ensure faster processing, efficient resource usage, and consistent performance in real-time fraud detection.

4. Result Analysis:

Accurate Fraud Detection: The system correctly classifies transactions as fraud or genuine using multiple ML models with high accuracy.

Real-Time Prediction System: It provides instant results after entering transaction details, helping prevent financial loss.

Data Preprocessing and Feature Engineering: Data is cleaned, encoded, and normalized to improve model performance.

Multi-Model Comparison: Different models are evaluated using accuracy, precision, and recall to select the best one.

Web-Based Application Development: A Django-based application is developed with login, dashboard, and prediction features.

Email Notification System with Frequent Alerts: The system sends emails for both fraud and genuine transactions, including repeated alerts for suspicious activities.

Improved Security and Reliability: Helps detect fraud early and improves trust in digital payments.

Visualization and Analysis: Uses confusion matrix, ROC curve, and accuracy graphs to evaluate performance.

• System Performance (Edge)

System Performance: The system performs efficiently on standard hardware by processing transaction data quickly using optimized machine learning models such as Random Forest, Decision Tree, Logistic Regression, and CNN. The Django-based application ensures smooth handling of user requests and real-time predictions without delays or system overload.

Alerting Efficiency: The email alert system works effectively by sending notifications for every transaction within a few seconds. It provides alerts for both fraudulent and genuine transactions, and includes a mechanism to send frequent alerts only for repeated suspicious activities, avoiding unnecessary message flooding while ensuring continuous user awareness.

5. Conclusion:

The proposed UPI fraud detection system demonstrates an effective approach for identifying fraudulent digital transactions using machine learning techniques. By integrating Random Forest, Decision Tree, and Logistic Regression algorithms, the system can analyze multiple transaction attributes—including amount, frequency, timing, device type, and geolocation—to classify transactions as genuine or fraudulent in real-time. The web-based Django application provides a user-friendly interface for administrators to train models, visualize performance metrics, and for end-users to input transaction details and receive immediate predictions. Compared to existing manual and rule-based systems, the proposed approach offers improved accuracy, faster detection, and enhanced operational efficiency. Moreover, it strengthens user confidence in UPI and digital payment platforms by providing timely alerts and actionable recommendations for suspicious transactions. Overall, the system illustrates the practical applicability of machine learning in safeguarding digital financial transactions and provides a scalable framework that can be extended with additional predictive models or live transaction monitoring for future enhancements.

References:

[1] S. Sharma, A. Singh, and R. Kumar, "UPI Payment Fraud Detection Using Machine Learning Algorithms," *International Journal of Computer Applications*, vol. 182, no. 40, pp. 35–42, Jun. 2021.

[2] A. Patel and P. Patel, "Machine Learning-Based Fraud Detection in Digital Payment Systems," *IEEE Access*, vol. 9, pp. 56789–56798, 2021.

[3] R. Garg and M. Jain, "A Study on UPI Payment Systems and Security Challenges in India," *Journal of Financial Technology Research*, vol. 2, no. 1, pp. 45–52, Jan. 2021.

[4] S. Das and R. Bhattacharya, "Real-Time Fraud Detection Using Random Forest Algorithm," *International Journal of Computer Science and Information Security*, vol. 19, no. 5, pp. 77–85, May 2021.

[5] H. Singh and V. Kumar, "Anomaly Detection in Financial Transactions Using Machine Learning," *Procedia Computer Science*, vol. 167, pp. 2342–2349, 2020.

[6] P. R. Varma and S. K. Sinha, "Decision Tree Approach for Detecting Fraudulent UPI Transactions," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 9, no. 6, pp. 1123–1130, Jun. 2020.

[7] R. K. Gupta and S. Jain, "UPI Fraud Analytics Using Supervised Learning Techniques," *International Conference on Smart Computing and Communication*, pp. 101–108, 2021.

[8] A. Sharma, V. Singh, and R. Mehta, "Logistic Regression for Fraud Detection in Digital Payments," *Journal of Advanced Computing and AI*, vol. 5, no. 3, pp. 56–63, Mar. 2021.

[9] N. Kaur and H. Arora, "A Comprehensive Review of Fraud Detection in Financial Transactions," *International Journal of Computer Applications*, vol. 174, no. 9, pp. 12–19, Aug. 2019.

[10] RBI, "Report on Payment Systems in India," Reserve Bank of India, Mumbai, India, Tech. Rep., Dec. 2020. [Online]. Available: https://www.rbi.org.in

[11] National Payments Corporation of India (NPCI), "Unified Payments Interface (UPI) Product Overview," NPCI, India, 2021. [Online]. Available: https://www.npci.org.in