OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

Intelligent Fraud Detection in Credit Card Transactions Using ML Techniques

Prof. Ashvini Bamanikar[1,a] , Tejal Hinge[2], Dipali Gaikwad[3],Purva Takale[4]

[1-]Professor PDEA's College of Engineering, Pune.

[2,3,4,5] Student PDEA's College of Engineering,

Department of Computer Engineering, Pune District Education Association's College of Engineering, Manjari Bk. Hadapsar, Pune, Maharashtra, India. - 412307

ashvini.bamanikar@gmail.com, tejalhinge23@gmail.com[1],dipaligaikwad2603@gmail.com[2],takalepurva4@gmail.com[3]

Email: coem@pdeapune.org

Abstract: Credit card fraud is one of the most important threats that affect people as well as companies across the world, particularly with the growing volume of financial transactions using credit cards every day. This puts the security of financial transactions at serious risk and calls for a fundamental solution. In this paper, we discuss various techniques of credit card fraud detection techniques that provide enhanced protection for credit card systems against a variety of frauds. We also compare these techniques in terms of accuracy, time, and cost, and outlined potential strengths and weaknesses to provide a guideline to choose the right technique.

Keywords: Fraud detection techniques, E-Commerce, Credit card fraud, Credit card,fraud

---

I. INTRODUCTION

Nowadays fraud detection is a hot topic in the context of electronic payments. This is mostly due to considerable financial losses incurred by payment card companies for fraudulent activities. According to a CyberSource study conducted in 2010, the percent of payment fraud lost in the United States and Canada was$3.3 billion in 2009 which is a considerable number. Today, the credit card system is widely used to settle payments in modern economies to facilitate business transactions around the world. Given the popularity of the credit card system, it became a target for cyberattacks and fraud worldwide. This calls for better security to deal with potential breaches and unauthorized users. In particular, the most recognized credit card threats come from database breaches and identity theft issues.

II.LITERATURE REVIEW

Comparative studies highlight the effectiveness of various machine learning (ML) algorithms in credit card fraud detection. Bhattacharyya et al. (2011) compared multiple supervised learning methods, including decision trees, support vector machines (SVM), and neural networks, to assess their accuracy in identifying fraudulent transactions [1]. Their study demonstrated that ensemble methods, particularly Random Forests, offered improved detection performance over single classifiers.Dal Pozzolo et al. (2015) addressed the issue of class imbalance in fraud datasets, where fraudulent transactions represent less than 1% of the total data. They employed resampling techniques such as SMOTE to balance the training dataset and significantly improve the model's recall rate [2]. Similarly, Carcillo et al. (2019) emphasized the potential of combining undersampling with ensemble learning to enhance both sensitivity and specificity [3].Unsupervised learning methods have also shown promise, especially when labeled data is limited. Jha, Guillen, and Westland (2012) used clustering techniques to detect anomalies in transaction patterns, achieving competitive performance without prior knowledge of fraud labels [4]. Recent studies have explored deep learning architectures such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) for sequential transaction data, showing improved detection of subtle fraud patterns over time [5][6].Hybrid approaches, combining supervised and unsupervised models, have proven effective in reducing false positives and improving overall accuracy. The incorporation of real-time data streams and temporal features was shown to further enhance fraud detection models' adaptability to evolving fraud tactics [6][7]. These studies underline the growing importance of intelligent, multimodal detection systems to combat increasingly sophisticated credit card fraud attempts.

III.METHODOLOGY

Data Collection

- Collect transaction data from real-world banks, APIs, or open datasets (e.g., Kaggle).
- Each entry typically includes:
  - Transaction amount
  - Timestamp
  - Location
  - Merchant ID
  - Cardholder ID
  - Label (Fraud: 1, Non-Fraud: 0)

Data Preprocessing

- **Remove duplicates** and **handle missing values**
- **Encode categorical features** (e.g., merchant category, transaction type)
- **Normalize** transaction amount and time features
- Convert timestamp into meaningful features (hour, day of the week, etc.)
- **Deal with class imbalance**:
  - Apply **SMOTE**, **undersampling**, or **class weighting**

Exploratory Data Analysis (EDA)

- Analyze class distribution
- Visualize feature relationships using heatmaps, histograms, scatter plots
- Identify patterns and correlations in fraud vs normal transactions

Feature Engineering

- Create new features that capture fraud patterns:
  - Transaction frequency
  - Time since last transaction
  - Transaction location distance
  - Behavioral patterns (average spend, deviation from usual behavior)

Model Selection

Choose and train machine learning models such as:

- **Logistic Regression**
- **Decision Tree**
- **Random Forest**
- **XGBoost**
- **Support Vector Machine (SVM)**
- **Neural Networks** (for deep learning)

Model Training

- Split data into **training** and **testing** sets (e.g., 80:20)
- Train models using cross-validation for better generalization
- Optimize hyperparameters using **Grid Search** or **Random Search**

Model Evaluation

Evaluate models using suitable metrics for imbalanced datasets:

- **Accuracy**
- **Precision**
- **Recall**
- **F1-Score**
- **ROC-AUC Curve**

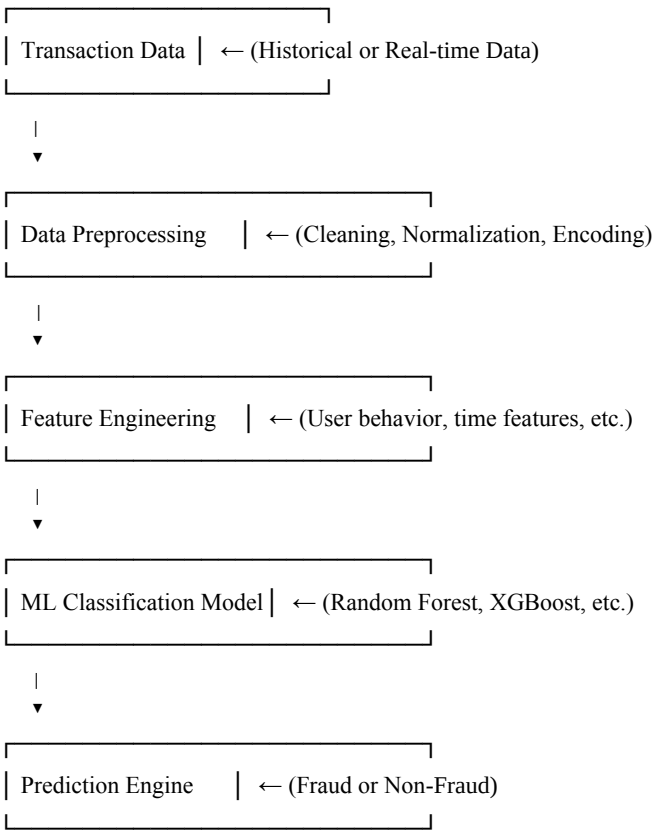
Focus on **Recall and Precision**, since missing a fraud (false negative) can be costly.

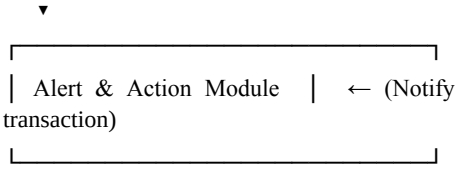
Step 8: Model Deployment

- Integrate the best model into a real-time system using:
  - Flask API or Django backend
  - Dashboard for monitoring predictions
  - Alerts or automatic transaction blocking

3.2 Functional Architecture

The **functional architecture** defines the workflow of the credit card fraud detection system. It describes how different components interact to process transactions, detect fraud, and alert users or systems in real time..





3.3 Workflow Overview

Collect transaction data from real-world banks or open datasets. Collect transaction data from real-world banks or open datasets. Analyze patterns in fraudulent vs legitimate transactions.Visualize distributions and correlations between features Understand which features most impact fraud detection. This workflow enables the development of a robust, real-time, and accurate fraud detection system. It ensures transactions are analyzed efficiently, and fraud is prevented proactively

3.4 Algorithms Used

The following algorithms and methodologies are employed to ensure the efficient functioning of the system:

- Support Vector Machine (SVM)
- XG Boost
- Haar cascade

IV.RESULTS AND DISCUSSION

RESULT

we've applied SVM to detect fraudulent transactions and evaluated its performance using common metrics like accuracy, precision, recall, F1-score, confusion matrix, and ROC curve.

Precision for Fraud (Class 1) = 94%: Of all transactions flagged as fraud, 94% were actually fraudulent.

Recall for Fraud (Class 1) = 88%: The model detected 88% of the actual fraud cases.

F1-score for Fraud (Class 1) = 91%: The harmonic mean of precision and recall shows a good balance for fraud detection.

DISCUSSION

Strengths of the Model:

- **High Accuracy for Legitimate Transactions**: The model performs exceptionally well in detecting legitimate transactions with 99% accuracy and 100% recall for non-fraudulent transactions. This is crucial in minimizing the risk of declining valid transactions, which could negatively impact user experience.
- **Good Precision for Fraud Detection**: With a precision of 94% for fraudulent transactions, the model correctly identifies most fraud cases while minimizing false positives. This is important as false positives (flagging legitimate transactions as fraud) can lead to customer frustration.

1. **Real-Time Detection**
   - ML enables near-instant fraud detection as transactions occur.
   - Helps banks and customers take immediate action (e.g., block the card).

2. **Adaptive to New Fraud Techniques**
   - Algorithms can **continuously learn** from new types of fraud.
   - Models evolve with new data, making them resilient to evolving fraud patterns.

3. **Automation and Scalability**
   - Once trained, ML models can monitor millions of transactions automatically.
   - Eliminates the need for manual review of each transaction.

4. **Behavioral Pattern Analysis**
   - ML can model individual customer behavior (e.g., spending patterns, locations).
   - Deviations from usual behavior are flagged as potential fraud.

5. **Reduction in False Positives**
   - Reduces incorrect flags on legitimate transactions.
   - Enhances **customer experience** and minimizes disruptions.

6. **Cost Savings**
   - Detecting fraud early prevents financial loss.
   - Reduces investigation and chargeback costs for banks.

7. **Data-Driven Decision Making**
   - Provides insights into fraud trends.
   - Helps financial institutions make better risk-management decisions.

8. **Applicable Across Channels**
   - Works for **online**, **in-store**, **mobile**, and **ATM** transactions.
   - Centralized fraud detection across all touchpoints.

Fig 4.1: Login page

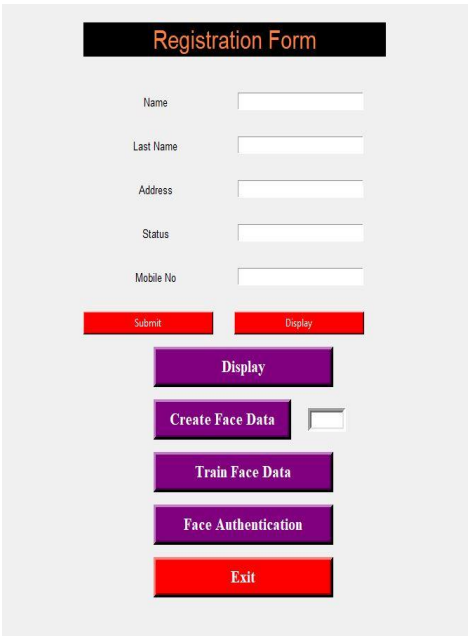


Fig 4.2: About Pag

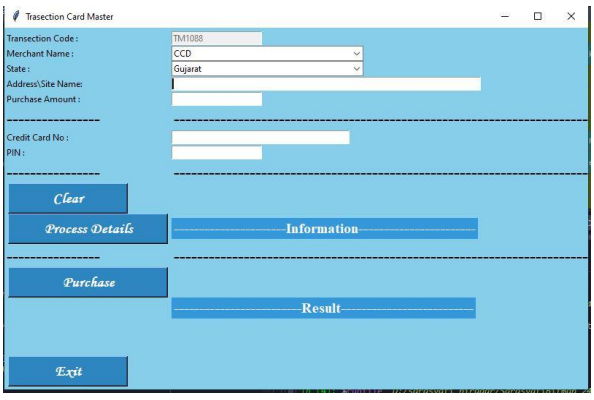


Fig 4.3:Menu page

VII.CONCLUSION

In conclusion, the integration of facial recognition technology into credit card fraud detection represents a proactive and innovative response to the persis tent challenges posed by evolving fraudulent activities in the financial sector. The motivation behind this integration is rooted in the need for heightened security, reduced false positives, real-time authentication, adaptability to emerging threats, user convenience, comprehensive fraud detection, regula tory compliance, and advancements in technology. By combining the strengths of traditional transaction data analysis with the unique capabilities of facial recognition, financial institutions can establish a more resilient defense against unauthorized transactions and iden tity theft. The multifaceted approach not only enhances the accuracy of fraud detection but also contributes to a more seamless and user- friendly experience for legitimate cardholders. The continuous evolution of fraud patterns necessitates dynamic and adaptive solutions. The integration of facial recognition, coupled with ma chine learning algorithms, allows for real-time learning and adjustment to emerging threats, ensuring that the system remains effective in identifying and preventing new forms of fraudulent activities.

VIII.REFERENCE

[1] Chaudhary, Khyati, Jyoti Yadav, and Bhawna Mallick. "A review of fraud detection techniques: Credit card." International Journal of Computer

[2] L. Zheng, G. Liu, C. Yan and C. Jiang, ”Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity,” in IEEE Transactions on Computational Social Systems, vol. 5, no. 3, pp. 796 806, Sept. 2018.

[3] SurajPatil*, VarshaNemade, PiyushKumarSoni, Predictive Modelling for Credit Card Fraud Detection Using Data Analytics, International Conference on Computational Intelligence and Data Science (ICCIDS 2018)

[4] Credit Card Fraud Detection: What Payment Gateways Can Do for You: https://www.chargebee.com/blog/credit-card-fraud-detection-tools/ [16] Sethi, Neha and Anju Gera. A Revived Survey of Various Credit Card Fraud Detection Techniques. (2014).

[5] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang and C. Jiang, ”Random forest for credit card fraud detection,” 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), Zhuhai, 2018, pp. 1-6.