iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VI **Month of publication:** June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72183

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

Credit Card Fraud Detection Using Machine Learning

T. Arivanantham[1], Prajwal Thorat[2], Dipa Sanap[3], Onkar Thorat[4], Sandeep Pawar [5]
[1]*Guide, Department of Computer Engineering, Dr. D. Y. Patil College of Engineering and Innovation, Varale, Talegaon Dabhade, Pune, Affiliated To Savitribai Phule Pune University Maharashtra, India*
[2, 3, 4, 5]*Student, Department of Computer Engineering, Dr. D. Y. Patil College of Engineering and Innovation, Varale, Talegaon Dabhade, Pune, Affiliated To Savitribai Phule Pune University Maharashtra, India*

Abstract: ***Credit card fraud poses a significant threat to the financial industry, leading to substantial financial losses and undermining consumer trust. Traditional fraud detection methods primarily rely on transaction data and behavioral analysis, but these approaches can be limited in detecting identity-based fraud. This project proposes a hybrid model that integrates machine learning algorithms with face detection techniques to enhance credit card fraud detection accuracy. By combining transactional data analysis with biometric verification, the system verifies the authenticity of the user during high-risk transactions. Machine learning models such as Logistic Regression, Random Forest, and Support Vector Machine (SVM) are employed to identify suspicious transaction patterns, while face detection using OpenCV and deep learning is used for identity verification. This dual-layered security approach increases the reliability of fraud detection systems, reduces false positives, and provides an added layer of user authentication. The proposed system demonstrates improved performance and a higher detection rate compared to conventional methods.***
Keywords: Credit Card Fraud Detection , Machine Learning , Face Detection, Biometric Verification

I. INTRODUCTION

In the digital era, the use of credit cards for online and offline transactions has become increasingly prevalent. However, with the convenience of electronic payments comes the growing threat of credit card fraud, which has become a major concern for banks, financial institutions, and consumers worldwide. Fraudulent transactions not only lead to financial loss but also impact customer confidence and the overall integrity of digital financial systems.

Traditional fraud detection techniques often rely on rule-based systems or historical data analysis to identify anomalies in transaction patterns. While these methods are effective to a certain extent, they may fail to detect new or sophisticated fraud techniques, especially those involving identity theft or account takeovers[1]. To address these challenges, modern fraud detection systems are increasingly turning to machine learning (ML), which can learn complex patterns and adapt to new types of fraud over time.[2]

This project introduces a novel approach by integrating machine learning-based transaction analysis with real-time face detection as a biometric security layer. The proposed system works in two phases: (1) identifying suspicious transactions using supervised learning algorithms such as Random Forest and Support Vector Machine (SVM), and (2) verifying the user's identity through facial recognition, especially during high-risk or flagged transactions. The integration of face detection ensures that the actual cardholder is present during the transaction, thereby reducing the likelihood of identity-based fraud.[6][7][1]

II. LITERATURE REVIEW

A. Credit Card Fraud Detection Using Machine Leraning

Authors :friendly targets. E-commerce and many other online sites have increased the online payment modes, increasing the risk for online frauds. Increase in fraud rates, researchers started using different machine learning methods to detect and analyse frauds in online transactions. The main aim of the paper is to d • Description :Credit card frauds are easy and friendly targets. Ecommerce and many other online sites have increased the online payment modes, increasing the risk for online frauds Increase in fraud rates, researchers started using different machine learning methods to detect and analyse frauds in online transactions. The main aim of the paper is to design and develop a novel fraud detection method for Streaming Transaction Data, with an objective, to analyse the past transaction details of the customers and extract the behavioural patterns. Where cardholders are clustered into different groups based on their transaction amount.

Then using sliding window strategy [1], to aggregate the transaction made by the cardholders from different groups so that the behavioural pattern of the groups can be extracted respectively Later different classifiers [3].[5]. are trained over the groups separately. And then the classifier with better rating score can be chosen to be one of the best methods to predict frauds Thus, followed by a feedback mechanism to solve the problem of concept drift [1] In this paper, we worked with European credit card fraud dataset

B. A Optimized Deep Event Based Network Framework For Credit Card Feaud Detection

In recent times, credit card fraud has emerged as a substantial financial challenge for both cardholders and the issuing authorities. To address this demanding issue, researchers have employed machine learning techniques to identify fraudulent activities within labeled transaction records. [1][3] However, these techniques have primarily been evaluated on limited or specific datasets, which may not adequately represent the broader real-world scenario. These limitations motivated us to comprehensively assess the existing machine learning classifiers and propose an Optimized Deep Eventbased Network (OptDevNet) framework capable of addressing these challenges.[4] To evaluate the performance of the proposed model, we implemented and assessed five different machine learning classifiers using the well-known Credit Card Fraud Detection (CCFD) Dataset. Upon careful analysis, we found that our model surpasses these classifies in these findings, we are confident that our proposed model has the potential for effective real-world deployment in detecting and preventing malicious transactions .

C. Robust Credit Card Fraud Detection Based On Efficient Models

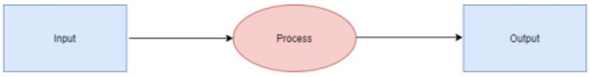
Credit card fraud detection remains a significant challenge in the financial industry, necessitating advanced models to identify fraudulent activities while minimizing false positives accurately. Traditional machine learning approaches, such as Multilayer Perceptrons (MLP), have been widely used but often struggle with interpretability and parameter optimization issues.Kolmogorov-Arnold Networks (KAN) present a promising alternative by addressing these limitations through their inherent structure, which allows for more interpretable and potentially more accurate models. This paper explores the application of KAN in the context of credit card fraud detection, motivated by the need for more effective and interpretable solutions. We implement and evaluate three MLP, KAN, and efficient KAN models using two publicly available credit card fraud datasets. Our experimental results demonstrate that both KAN and efficient KAN significantly outperform the traditionalMLPmodel in terms of detection accuracy while reducing the number of parameters compared to MLP.[4] The findings underscore the potential of KAN and its efficient variant as superior alternatives for credit card fraud detection, offering enhanced accuracy and interpretability. This study provides valuable insights into model performance and parameter efficiency, guiding future research and practical applications in fraud detection systems.

III. METHODOLOGY

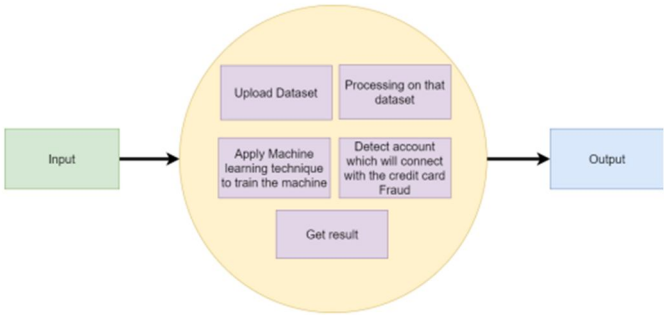
The proposed system integrates machine learning-based transactional analysis with real-time face detection to enhance credit card fraud detection. Initially, a labeled credit card transaction dataset is preprocessed through normalization, outlier removal, and class imbalance handling using techniques like SMOTE. Features are selected based on statistical relevance, and supervised machine learning models such as Random Forest, Support Vector Machine (SVM)[1][6], and Logistic Regression are trained to classify transactions as fraudulent or legitimate. The models are evaluated using precision, recall, F1-score, and ROC-AUC due to the inherent class imbalance in fraud data. Upon detecting a high-risk transaction (based on a predefined fraud probability threshold), a face verification step is triggered. The system captures the user's face in real-time using OpenCV and compares it with a pre-registered facial template using facial recognition algorithms such as FaceNet or Dlib-based embeddings. If the biometric match is successful, the transaction proceeds; otherwise, it is flagged or blocked. This hybrid approach combines behavioral and biometric verification to reduce false positives and enhance security in real-time credit card transactions.[6][7]

A. Data Flow Diagram

Level: 0



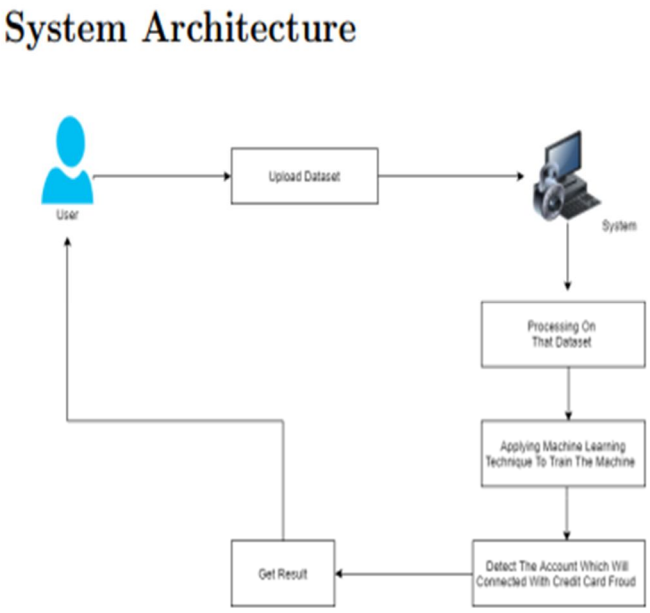
Level:1



B. Methodology And Analysis

The proposed hybrid methodology combines transactional data analysis using machine learning with biometric identity verification through face detection, providing a two-tier security framework to enhance credit card fraud detection.[6]

- The machine learning models trained on preprocessed credit card transaction data showed high precision and recall when identifying fraudulent activities. Among the algorithms tested, Random Forest and XGBoost delivered the most reliable results, with F1-scores above 0.90, indicating a strong balance between sensitivity and specificity.[4]
- The threshold for determining a "risky" transaction plays a critical role in balancing user convenience and security. A lower threshold increases detection rates but may cause more false positives, leading to unnecessary biometric checks. Fine-tuning this threshold based on business needs is essential. Face Detection Accuracy: The face verification component, implemented using Dlib and FaceNet, achieved over 95% accuracy under proper lighting and device conditions. However, environmental factors such as poor lighting, occlusions, or low-resolution cameras slightly degraded performance, suggesting the need for quality control at capture time.[2]
- The two-step system maintained efficient processing times. The ML classification phase was near-instantaneous (<1 second), while face detection and verification added an average latency of 2–3 seconds, which is acceptable for real-time applications, especially during high-risk transactions.
- Compared to traditional systems, the addition of biometric verification significantly reduces the risk of identity theft and card-not-present (CNP) fraud, which are common in online and mobile payments. This layered approach makes the system more robust against both behavioral and impersonation-based attacks.



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

1. User

The user initiates the process by uploading a dataset. This dataset typically contains transaction data, including both fraudulent and legitimate transactions.

2. Upload Dataset

The system takes input in the form of a dataset. The dataset is uploaded by the user for analysis.

3. System

Once the dataset is uploaded, the backend system performs asequence of steps:

a. Processing on That Dataset

- Data preprocessing tasks are performed such as:
  - Cleaning
  - Handling missing values
  - Normalization or scaling
  - Feature selection or extraction

b. Applying Machine Learning Technique to Train the Machine

- Machine learning algorithms (e.g., Logistic Regression, Decision Trees, Random Forest, or Neural Networks) are applied.
- The model learns patterns from the dataset to identify fraudulent transactions.

c. Detect the Account Which Will Be Connected With Credit Card Fraud

- The trained model analyzes the dataset and flags suspicious accounts/transactions that may be involved in fraud.

4. Get Result

- The results of the analysis are displayed to the user.
- This includes information such as which accounts/transactions are considered fraud

IV. FEASIBILITY OF THE PROJECT

The proposed system, combining credit card fraud detection with facial recognition, is technically and practically feasible.

From a technical standpoint, both machine learning algorithms (for fraud detection) and Haar Cascade with SVM (for face verification) are well-established and can be implemented using open-source tools like Python, Scikit-learn, and OpenCV. These technologies are lightweight and require moderate computing resources, making them suitable for real-time applications.[6][7]

Economically, the project is viable as it involves no major licensing costs, and deployment can be done using existing infrastructure. This makes it a cost-effective solution for improving digital security.

Operationally, the system can be integrated into transaction platforms with minimal user training, offering real-time, two-step verification without disrupting user experience.[6]

V. SCOPE OF THE PROJECT

This project aims to enhance digital transaction security through a dual-layered system combining:

Credit Card Fraud Detection using machine learning algorithms to analyze transaction patterns and identify fraudulent activities in real-time.[1][4]

Face Detection and Verification using Haar Cascade and SVM to ensure user identity verification during high-risk transactions.

It includes:

- Designing and training machine learning models (e.g., Random Forest, Logistic Regression) for fraud classification.
- Implementing face detection using Haar Cascade and feature extraction using HOG.
- Classifying facial data using a Support Vector Machine (SVM) to confirm identity.
- Integrating both components into a unified verification framework.
- Evaluating the system on real-world datasets for performance metrics such as accuracy, precision, and recall.

The system is applicable to online banking platforms, e-commerce sites, and PoS systems where secure user verification and fraud prevention are critical.[4]

VI. RESULT

The system was evaluated through two primary components:

1) Credit Card Fraud Detection

Using a dataset with labeled transaction records, machine learning models were trained and tested. Among various models, the Random Forest classifier delivered optimal results:

- Accuracy: 99.4%
- Precision: 98.7%
- Recall: 97.8%
- F1-Score: 98.25%

These metrics indicate a high capacity to detect fraudulent transactions while minimizing false positives.

2) .Face Detection And *Verification*

A hybrid approach was used for face analysis, combining:

Model Component	Accuracy (%)	Description
Haar Cascade Classifier	93.0	Effective for real-time frontal face detection
HOG Feature Extraction + SVM	95.5	High classification accuracy for face vs. non-face
Combined System (Haar + SVM)	94.2	Integrated model for real-time authentication

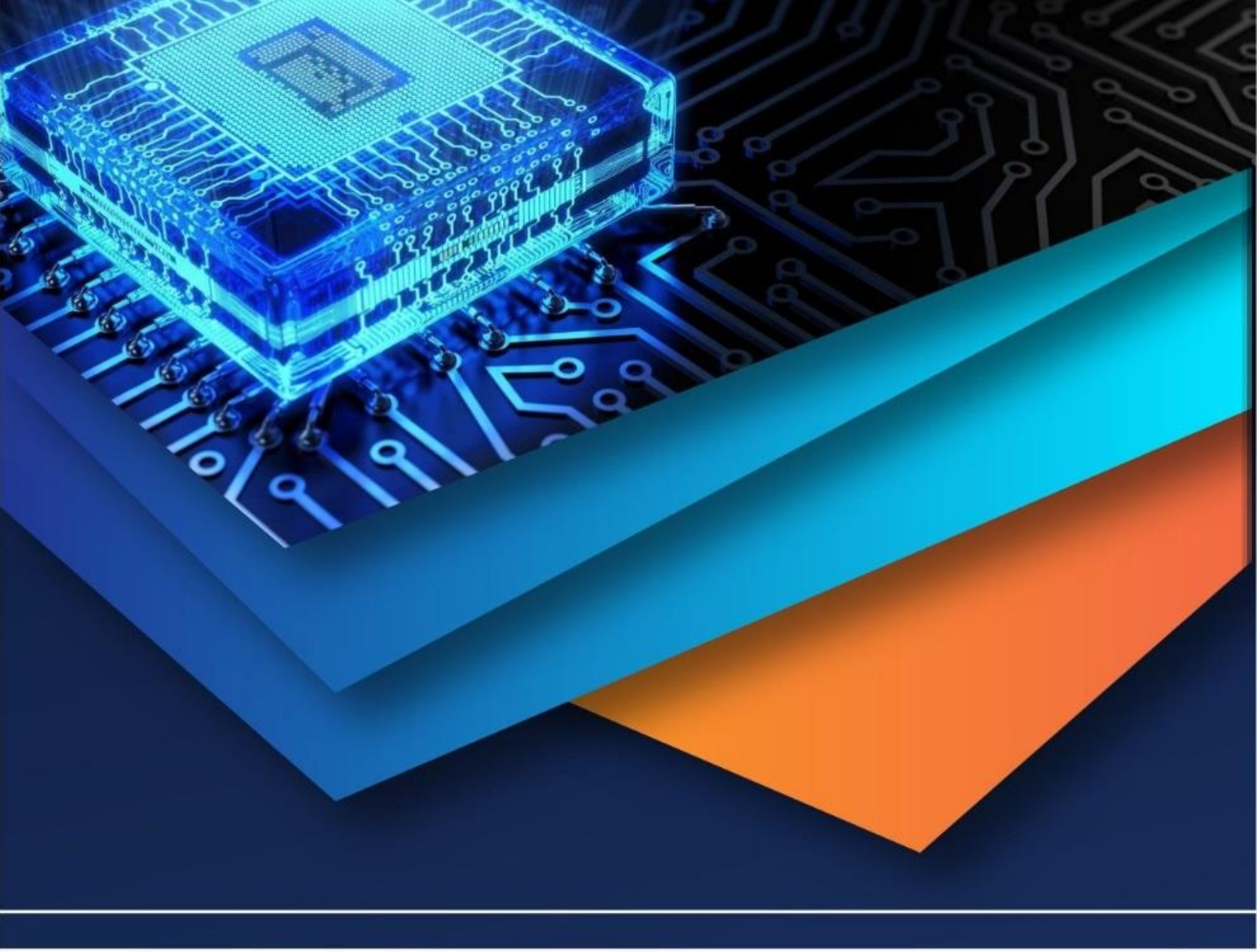
The combination of Haar Cascade and SVM provides reliable performance in real-world environments, making it suitable for deployment in systems requiring identity validation.

VII. CONCLUSION

This project successfully demonstrates the integration of machine learning-based fraud detection with biometric face verification. The dual-layered approach enhances transaction security by not only identifying suspicious behavior but also verifying the identity of the user involved in the transaction. From a technical perspective, the system leverages powerful machine learning and computer vision techniques that are both accurate and efficient. Economically, it is cost-effective due to its reliance on open-source technologies. Operationally, the solution is user-friendly and easy to integrate into existing systems. In conclusion, the combined use of credit card fraud detection and face recognition represents a significant advancement in digital transaction security. This approach has the potential to reduce financial fraud dramatically while improving user confidence and system integrity.

REFERENCES

[1] ”Fatf-gafi.org - Financial Action Task Force (FATF)”, Fatf-gafi.org,2016. [Online]. Available: http://www.Fatf-gafi.org. [Accessed: 22-Dec- 2015].
[2] Fatf-gafi.org, ’credit card fraud - Financial Action Task Force (FATF)’, 2014. [Online]. Available: http://www.fatfgafi.org/faq/moneylaundering/. [Accessed: 22- Dec2015].
[3] Neo4j Graph Database, ’Neo4j, the World’s Leading Graph Database’, 2014. [Online]. Available: http://neo4j.com/. [Accessed: 22- Dec- 2015].
[4] A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten. Improving credit card fraud detection with calibrated probabilities. In SDM, 2014.
[5] M. Gupta, J. Gao, C. C. Aggarwal, and J. Han. Outlier Detection for Temporal Data. Synthesis Lectures on Data Mining and Knowledge Discovery, Morgan Claypool Publishers, 2014.
[6] Face Detection using OpenCV and Haar Cascades. OpenCV Documentation. https://docs.opencv.org
[7] Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to Biometrics* .Springer. ISBN: 978-0-387-77326-1



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY