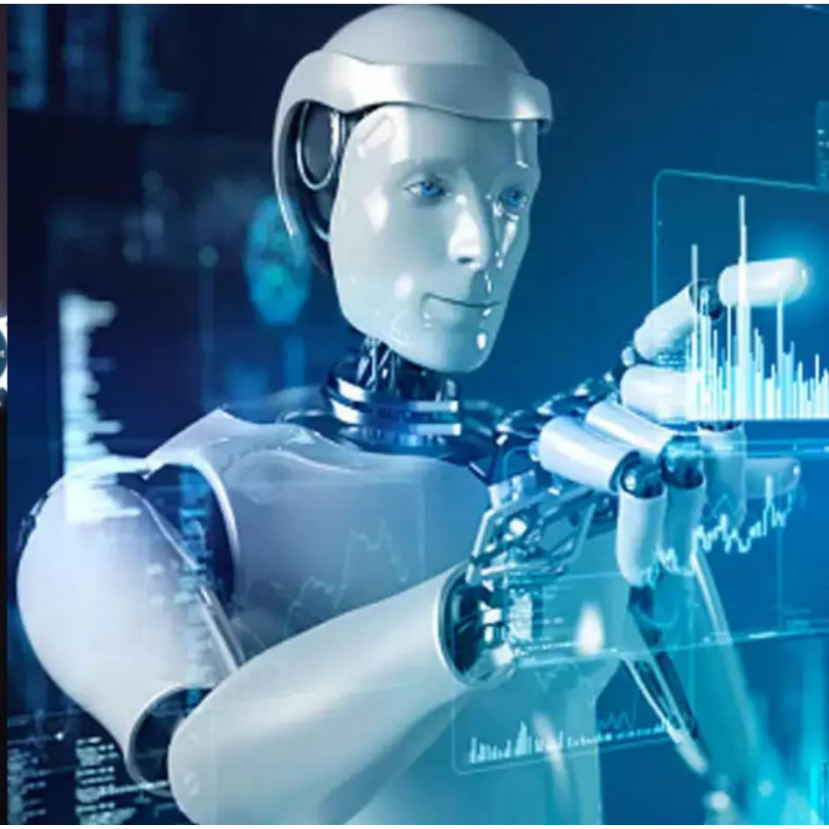
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 12, December 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412026|

A Machine Learning and Dual-Authentication Framework for Secure Credit Card Fraud Detection

Karthik S. D[1], Priya S. Banakar[2], Shrinivas K. Jadar[3], Paravathi S. Neelagunda[4], Dr. Murgesh V. Jambigi[5]

Department of Computer Science and Engineering, STJ Institute of Technology, Ranebennur, India[1-4]

Guide, Department of Computer Science and Engineering STJ Institute of Technology, Ranebennur, India[5]

ABSTRACT: Credit card fraud has increased significantly with rapid digitalization, causing financial losses worldwide. Traditional rule-based systems struggle to detect evolving attack patterns. This paper presents a hybrid machine learning and dual-authentication framework that enhances fraud detection accuracy and strengthens transaction security. Multiple supervised learning models—including Logistic Regression, Decision Tree, Random Forest, and CNN—are trained on preprocessed transaction data. Suspicious transactions undergo OTP verification and facial recognition using LBPH. Experimental results demonstrate improved classification accuracy, reduced false positives, and enhanced user verification. The system is suitable for real-time financial applications requiring high security.

I. INTRODUCTION

The growth of e-commerce and digital payments has resulted in a proportional increase in credit card fraud. Fraudsters use stolen credentials, phishing, and identity theft to perform unauthorized transactions. Traditional rule-based systems lack adaptability and fail to detect new fraud behaviors. Machine Learning (ML) models, trained on large datasets, can identify unusual transaction patterns effectively.

While ML detects suspicious actions, verifying the user's identity is also crucial. Hence, this system integrates ML-based fraud detection with dual authentication (OTP and biometric verification). This provides stronger security and minimizes unauthorized transactions.

II. RELATED WORK

Researchers have applied ML to fraud detection with promising results. Sharma et al. used Logistic Regression and Random Forest to evaluate fraud datasets. Thennakoon et al. implemented real-time API-based fraud detection. Najadat et al. improved DL performance by balancing datasets using SMOTE. However, existing studies rarely integrate strong authentication mechanisms. This work fills that gap by combining ML and biometric-based authentication.

III. PROPOSED SYSTEM

The proposed model consists of:

- Machine Learning-based transaction classification
- OTP verification through Telegram Bot API
- Facial recognition authentication using LBPH
- ML Fraud Detection

The dataset includes 28 anonymized features (V1–V28) and Amount. Preprocessing includes:

- Removal of noise and missing values
- Standardization and normalization
- SMOTE-based class balancing
- Feature selection via correlation heatmap

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412026|

Models used: Logistic Regression, Decision Tree, Random Forest, CNN. Random Forest showed the highest accuracy and robustness.

Dual Authentication
OTP Verification: A 4-digit OTP is generated and sent via Telegram. This ensures the user has access to the registered device.

Facial Recognition: The LBPH model compares captured facial features with stored training images. Unauthorized and mismatched faces result in transaction rejection.

IV. SYSTEM ARCHITECTURE

The workflow consists of:
1. User enters transaction details.
2. ML model predicts “normal” or “suspicious.”3. Suspicious transactions trigger OTP verification.
3. Successful OTP leads to facial recognition.
4. Only verified users can complete the transaction.

V. IMPLEMENTATION

Python Flask is used for backend logic, with HTML/CSS for the UI. Libraries used: NumPy, Pandas, Scikit-learn, TensorFlow, OpenCV, Telepot API, SMOTE.

Data Flow
Transactions → Preprocessing → ML Prediction → Authentication → Decision.

Execution Flow
- User enters details (Amount, V-values).
- Backend processes values and passes them to the trained ML model.
- If suspicious, OTP is sent.
- Face recognition confirms user identity.
- Result displayed (Approved / Declined).

VI. RESULTS AND DISCUSSION

A feature correlation heatmap identifies key attributes contributing to fraud. Random Forest outperformed other ML models. OTP failures block unauthorized attempts. Face recognition prevents misuse even when OTP is compromised.

Key outcomes:
- Reduced false positives
- Strong biometric verification
- High model reliability
- Fast prediction suitable for real-time use

VII. CONCLUSION

This paper presents a secure credit card fraud detection system combining ML models with OTP and facial recognition. The integrated approach enhances security, reduces fraud risk, and provides stronger identity validation. The model is scalable and can be deployed in banks and e-commerce platforms.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412026|

VIII. FUTURE WORK

- LSTM models for sequence-based prediction
- Blockchain-based transaction verification
- Voice biometrics for user authentication
- Cloud deployment for large-scale processing

REFERENCES

1. I. Sharma et al., “Credit Card Fraud Detection Using ML,” IRJET, 2022.
2. A. Thennakoon et al., “Real-Time Fraud Detection,” IEEE Confluence, 2019.
3. H. Najadat et al., “Deep Learning for Fraud Detection,” ICICS, 2020.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details