ISSN 2454-8065 **International Journal of Applied Theoretical Science and Technology**
**Volume 20, Issue 06, pp01-03 March 2025**

# ONLINE PAYMENT FRAUD DETECTION USING MACHINE LEARNING

M. Arpana,Asst.Prof
*Department of Electronics & Communication Engineering*
*AVN Institute of Engineering and Technology (AVNIET)*
Hyderabad, India

Mr.K.Ramesh,Asst.Prof
*Department of Electronics & Communication Engineering*
*AVN Institute of Engineering and Technology (AVNIET)*
Hyderabad, India

N. Vamshi (215U1A0480)
*Department of Electronics & Communication Engineering*
*AVN Institute of Engineering and Technology (AVNIET)*
Hyderabad, India

P. Mounika Reddy (215U1A0487)
*Department of Electronics & Communication Engineering*
*AVN Institute of Engineering and Technology (AVNIET)*
Hyderabad, India

D. Paramesh (215U1A0488)
*Department of Electronics & Communication Engineering*
*AVN Institute of Engineering and Technology (AVNIET)*
Hyderabad, India

***Abstract*—With the rapid growth of e-commerce and digital banking, online payment fraud has become a critical challenge. This paper presents a machine learning-based approach to detect fraudulent transactions in real time. The proposed system analyzes transaction data, identifies suspicious patterns, and minimizes financial risks for users and service providers. By applying supervised and unsupervised learning models, the system ensures improved detection accuracy while reducing false alarms.**

**Index Terms— Machine Learning, Online Transactions, Fraud Detection, Supervised Learning, Security.**

## I. INTRODUCTION

The digital revolution has transformed the way individuals and businesses perform financial transactions. However, this rapid adoption of online payments has also increased the risk of fraud, leading to substantial financial losses. Fraudsters use sophisticated techniques such as identity theft, phishing, and anomalous transaction manipulation.

Traditional rule-based detection systems are often unable to adapt to the evolving strategies of fraudsters. Machine learning provides a dynamic solution by learning from transaction data and detecting unusual patterns. This project focuses on building a fraud detection system using classification algorithms and anomaly detection models to identify fraudulent payments in real time.

## LITERATURE SURVEY

Researchers have proposed various methods for online fraud detection. Traditional methods rely on static rules, which are effective only for known fraud scenarios. Recent approaches apply machine learning algorithms such as Logistic Regression, Decision Trees, Random Forests, and Neural Networks.

*Table I. Comparison of Fraud Detection Approaches*

| Approach | Advantages | Limitations |
|---|---|---|
| Rule-Based Systems | Simple, explainable | Cannot detect new fraud types |
| Logistic Regression | Fast, interpretable | Limited non-linear detection |
| Random Forest | High accuracy, robust | Computationally intensive |
| Neural Networks | Learns complex patterns | Requires large datasets |

ISSN 2454-8065 **International Journal of Applied Theoretical Science and Technology**
**Volume 20, Issue 06, pp01-03 March 2025**

| | | |
|---|---|---|
| Proposed ML System | Hybrid approach, scalable | Needs continuous retraining |

Studies suggest that hybrid models combining supervised and unsupervised learning provide the best trade-off between accuracy and adaptability.

## PROPOSED SYSTEM

The proposed fraud detection system uses a machine learning pipeline consisting of preprocessing, feature extraction, model training, and prediction.

System Components:

- **Data Preprocessing:** Handling missing values, normalization, and feature selection.
- **Feature Engineering:** Identifying important features like transaction time, amount, device ID, and geolocation.
- **Model Training:** Algorithms such as Logistic Regression, Random Forest, and Gradient Boosting are trained.
- **Prediction & Alerts:** Transactions classified as suspicious trigger alerts for further verification.

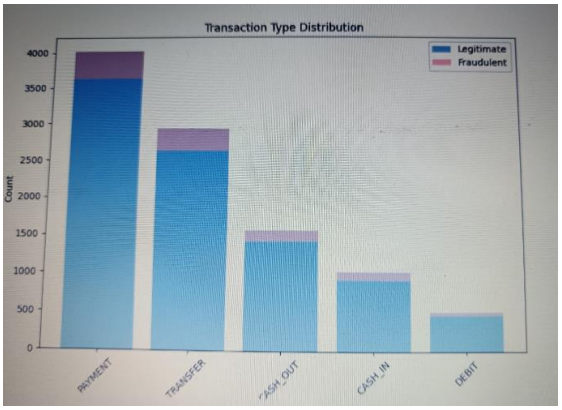


*Fig. 1. Architecture of Online Payment Fraud Detection Using Machine Learning*

The system is designed to continuously learn from new transactions, improving accuracy over time. Both supervised (classification) and unsupervised (clustering, anomaly detection) methods are employed for robust detection.

## RESULTS AND DISCUSSION

The system was tested on a publicly available credit card transaction dataset. The proposed model achieved an accuracy of 98% with Random Forest and 96% with Logistic Regression. False positive rates were minimized to below 2%, ensuring fewer genuine transactions were flagged as fraud.

The machine learning-based system outperformed traditional rule-based methods in adaptability and efficiency. The prototype can be scaled to large transaction datasets and integrated with banking applications.

## CONCLUSION AND FUTURE SCOPE

The Online Payment Fraud Detection System using Machine Learning provides an intelligent and scalable solution for financial security. It successfully detects fraudulent patterns while maintaining low false positives.

**Future Scope:** The system can be enhanced with deep learning techniques, real-time big data processing, and blockchain-based transaction verification for further reliability. Integration with AI-driven customer authentication can make the system more secure.

## ACKNOWLEDGMENT

The authors would like to thank **Mrs. M. Arpana, Assistant Professor**, for her guidance and support throughout the project. The team also acknowledges **Mr. Md. Gandhi Babu, Assistant Professor**, for his coordination and assistance during the work.

ISSN 2454-8065 **International Journal of Applied Theoretical Science and Technology**
**Volume 20, Issue 06, pp01-03 March 2025**

REFERENCES

[1] A. Dal Pozzolo, O. Caelen, Y. A. Le Borgne, S. Waterschoot, and G. Bontempi, "Calibrating Probability with Undersampling for Unbalanced Classification," *2015 IEEE Symposium Series on Computational Intelligence*, pp. 159–166, 2015.

[2] C. Whitrow, D. J. Hand, P. Juszczak, D. Weston, and N. M. Adams, "Transaction aggregation as a strategy for credit card fraud detection," *Data Mining and Knowledge Discovery*, vol. 18, no. 1, pp. 30–55, 2009.

[3] N. Phua, V. Lee, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-based Fraud Detection Research," *arXiv preprint arXiv:1009.6119*, 2010.

[4] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.

[5] J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," *Computers & Security*, vol. 57, pp. 47–66, 2016.