International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

Real-Time Online Transaction Fraud Detection Using Machine Learning

[1] SK. MOHAMMAD BASHA, [2] VAJRALA SAI KUMAR REDDY, [3] MITTA SAI KUMAR REDDY,

[4] SYED SHAMSHEER, [5] DOGIPARTHI SAI DEEPAK, [6] ARAVEETI LEELA VENKATA BUGGALAKSHMIPRASAD

[1] ASST., PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY & SCIENCES, DEVARAJUGATTU, MARKAPUR

[2,3,4,5,6] STUDENT, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY & SCIENCES, DEVARAJUGATTU, MARKAPUR

ABSTRACT

The rapid growth of digital payment platforms has significantly increased the risk of online financial fraud, posing serious challenges to individuals, financial institutions, and regulatory bodies. This project presents an intelligent Online Fraud Payment Detection and Blocking System using Machine Learning (ML) that aims to identify and prevent fraudulent transactions in real time. The system leverages advanced ML algorithms such as Logistic Regression, Random Forest, and Gradient Boosting to analyze transaction patterns and detect anomalies based on features like transaction amount, location, time, device information, and user behavior.

A large dataset of historical transactions is preprocessed and used to train the model, ensuring accurate classification of legitimate and fraudulent activities. Feature engineering techniques are applied to improve prediction performance, while imbalance handling methods such as SMOTE are used to address skewed datasets. The trained model is integrated into a real-time processing system that evaluates each incoming transaction and assigns a fraud probability score.

Keywords: Online Fraud Detection, Machine Learning, Payment Security, Anomaly Detection, Transaction Monitoring, Fraud Prevention, Random Forest, Logistic Regression, Real-Time Detection, SMOTE, Cybersecurity, Financial Technology (FinTech)

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

I. INTRODUCTION

The rapid advancement of digital technologies and the widespread adoption of online payment systems have transformed the way financial transactions are conducted. With the increasing use of mobile banking, e-commerce platforms, digital wallets, and contactless payments, users can perform transactions anytime and anywhere with convenience and speed. However, this digital transformation has also led to a significant rise in online payment fraud, making security a major concern for both users and financial institutions.

Online fraud involves unauthorized transactions carried out by malicious actors using stolen credentials, phishing attacks, identity theft, or compromised devices. Traditional rule-based fraud detection systems are no longer sufficient to handle the evolving and sophisticated nature of these attacks. Fraudsters continuously develop new techniques to bypass static security rules, leading to increased financial losses and reduced user trust in digital payment systems.

To address these challenges, machine learning (ML) has emerged as a powerful solution for detecting and preventing fraudulent transactions. ML models can analyze large volumes of transaction data, identify hidden patterns, and distinguish between legitimate and suspicious activities with high accuracy. Unlike traditional systems, ML-based approaches can adapt to new fraud patterns over time, making them more effective in dynamic environments.

II. LITERATURE REVIEW

The problem of online payment fraud detection has been widely studied in the fields of machine learning, data mining, and cybersecurity. Researchers have proposed various techniques to identify fraudulent transactions efficiently and accurately. Early systems primarily relied on rule-based approaches, where predefined conditions were used to detect suspicious activities. However, these systems lacked adaptability and failed to detect new and evolving fraud patterns.

A study by Vesta Corporation Research Team focused on rule-based fraud detection mechanisms and highlighted their limitations in handling large-scale and dynamic transaction data. These systems were effective only for known fraud patterns and required continuous manual updates, making them inefficient in modern digital environments.

Later, researchers such as Pedro Domingos emphasized the use of machine learning techniques for fraud detection. Supervised learning algorithms like Logistic Regression

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

and Decision Trees were introduced to classify transactions based on historical data. These models improved detection accuracy but were still limited by imbalanced datasets, where fraudulent transactions are much fewer than legitimate ones.

EXISTING SYSTEM

The existing systems for online fraud payment detection are primarily based on traditional rule-based methods and basic statistical analysis techniques. These systems rely on predefined rules and thresholds to identify suspicious transactions. For example, a transaction may be flagged as fraudulent if it exceeds a certain amount, originates from an unusual location, or occurs at an abnormal time. While such systems were effective in earlier stages of digital banking, they are no longer sufficient to handle the complexity and scale of modern online transactions.

Most financial institutions currently use rule engines combined with simple machine learning models to detect fraud. These systems analyze transaction data such as user behavior, transaction frequency, and device information. However, they often depend heavily on historical fraud patterns and require continuous manual updates by experts to remain effective. As fraud techniques evolve rapidly, these static systems struggle to adapt in real time.

Another limitation of existing systems is their inability to handle highly imbalanced datasets, where fraudulent transactions represent only a small fraction of the total data. This leads to biased predictions, where the system may classify most transactions as legitimate, resulting in missed fraud cases. Additionally, traditional systems often generate a high number of false positives, incorrectly flagging genuine transactions as fraudulent, which negatively impacts user experience and trust.

PROPOSED SYSTEM

The proposed **Online Fraud Payment Detection and Blocking System using Machine Learning** is designed to overcome the limitations of traditional fraud detection methods by providing a real-time, intelligent, and adaptive solution. This system leverages advanced machine learning algorithms to analyze transaction data, identify suspicious patterns, and take immediate action to prevent fraudulent activities before they are completed.

The system is built on a data-driven approach, where a large volume of historical transaction data is collected and preprocessed. Data preprocessing includes cleaning,

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

normalization, and feature engineering to extract meaningful attributes such as transaction amount, time, location, device information, frequency of transactions, and user behavior patterns. To handle class imbalance, techniques like SMOTE are applied to ensure that fraudulent transactions are adequately represented during model training.

Multiple machine learning models such as Random Forest, Logistic Regression, and Gradient Boosting are trained and evaluated to select the most accurate and efficient model. Ensemble learning techniques are used to improve prediction performance and reduce overfitting. The trained model is then deployed into a real-time transaction processing system.

METHODOLOGY

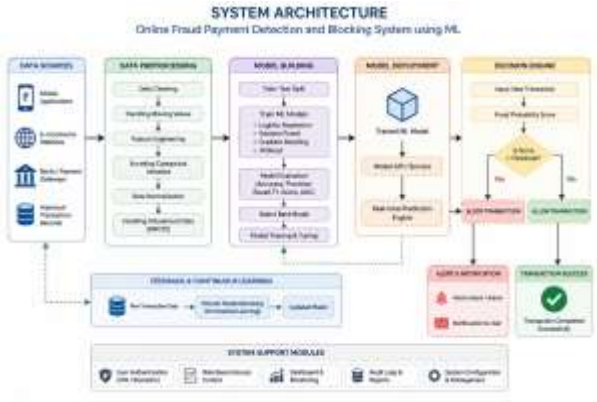
The proposed system follows a systematic and data-driven methodology to detect and prevent online payment fraud using machine learning techniques. The process begins with data collection, where historical transaction data is gathered from financial systems, including both legitimate and fraudulent transactions. This dataset typically contains features such as transaction amount, timestamp, location, device details, and user behavior patterns.

In the next step, data preprocessing is performed to clean and prepare the dataset for model training. This includes handling missing values, removing duplicates, normalizing numerical features, and encoding categorical variables. Since fraud datasets are highly imbalanced, techniques like Synthetic Minority Over-sampling Technique (SMOTE) are applied to balance the data and improve model performance.

Feature engineering is then carried out to extract meaningful insights from raw data. New features such as transaction frequency, average spending behavior, and location deviation are derived to enhance the model's ability to distinguish between normal and suspicious activities. After preprocessing, the dataset is split into training and testing sets.

VI. SYSTEM MODEL

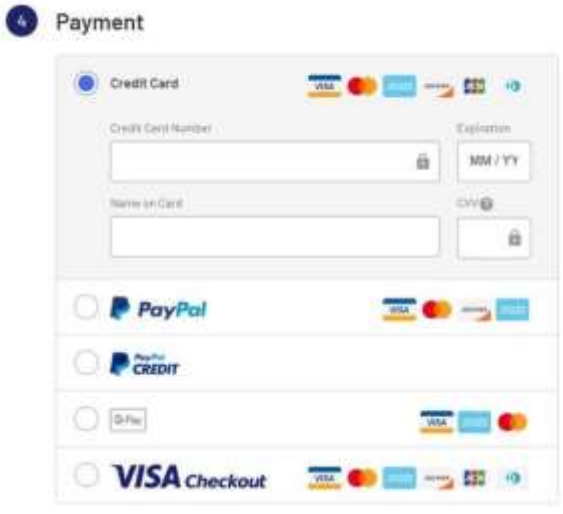
SystemArchitecture



2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

III. RESULTS AND DISCUSSIONS



International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

VIII. CONCLUSION

The **Online Fraud Payment Detection and Blocking System using Machine Learning** provides an effective and intelligent solution to address the growing challenges of digital payment fraud. With the increasing reliance on online transactions, ensuring security and trust has become a critical requirement for financial systems. The proposed system successfully leverages machine learning techniques to analyze transaction data, identify suspicious patterns, and take real-time action to prevent fraudulent activities.

By utilizing advanced algorithms such as Random Forest, Logistic Regression, and Gradient Boosting, the system achieves high accuracy in distinguishing between legitimate and fraudulent transactions. The integration of data preprocessing, feature engineering, and imbalance handling techniques further enhances the model's performance. Unlike traditional rule-based systems, the proposed solution adapts to new fraud patterns, making it more robust and reliable in dynamic environments.

One of the key strengths of the system is its real-time detection and automatic blocking capability, which minimizes financial losses and protects users from unauthorized transactions. Additionally, the system improves user confidence in digital payment platforms by reducing false positives and ensuring smooth transaction experiences.

Overall, the proposed system demonstrates how machine learning can be effectively applied to enhance cybersecurity in financial applications. It offers a scalable, efficient, and future-ready approach to fraud detection, making it highly suitable for modern banking and e-commerce systems.

IX. FUTURE WORK: Future work for this

The proposed Online Fraud Payment Detection and Blocking System can be further enhanced by incorporating advanced technologies and expanding its capabilities to handle more complex fraud scenarios. Future improvements can focus on increasing accuracy, scalability, and adaptability to evolving cyber threats.

One important direction is the integration of deep learning models such as Artificial Neural

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

Networks (ANNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks. These models can better capture sequential transaction patterns and user behavior over time, leading to improved detection of sophisticated fraud activities.

Another enhancement is the use of real-time big data processing frameworks like Apache Kafka and Apache Spark. These technologies can enable faster processing of large volumes of transaction data and support high-throughput, low-latency fraud detection in large-scale financial systems.

The system can also be improved by incorporating behavioral biometrics, such as keystroke dynamics, touch patterns, and mouse movements, to provide an additional layer of security. This helps in identifying users based on their unique interaction patterns, making fraud detection more precise.

Integration with blockchain technology can be explored to ensure secure, transparent, and tamper-proof transaction records. This can enhance trust and reduce the risk of data manipulation in financial systems.

XI. REFERENCES

➤ Leo Breiman, "Random Forests," *Machine Learning Journal*, 2001.

➤ Jerome H. Friedman, "Greedy Function Approximation: A Gradient Boosting Machine," *Annals of Statistics*, 2001.

➤ IEEE, "Credit Card Fraud Detection Using Machine Learning," IEEE Conference Papers, 2018.

➤ Elsevier, "Fraud Detection in Financial Transactions Using Machine Learning Techniques," *Procedia Computer Science*, 2019.

➤ Springer, "An Efficient Approach for Online Payment Fraud Detection," *Springer Journal of Big Data*, 2020.

➢ J.V. Anil Kumar, Nagella Swarupa Rani," SECURE DATA TRANSMISSION THROUGH HYBRID CRYPTOGRAPHY AND STEGANOGRAPHIC TECHNIQUES", International Journal of Engineering Science and Advanced Technology (IJESAT) Vol 25 Issue 12,2025, www.ijesat.com, https://doi.org/10.64771/ijesat.2025.046, Page 373 to 383, ISSN:2250-3676, 2025.

➢ J.V.ANIL KUMAR, ALLU MAHALAKSHMI, "SMART NETWORKING APPROACH FOR

Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

AUTOMATED INCIDENT MANAGEMENT", International Journal of Engineering Science and Advanced Technology (IJESAT) Vol 25 Issue 12,2025, www.ijesat.com, https://doi.org/10.64771/ijesat.2025.047, Page 384 to 392, ISSN:2250-3676, 2025.