International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Hybrid AI Model for Online Payment Fraud Detection Using Machine Learning

Under the guidance of
Mrs. Bhagyashree Wakde
Assistant Professor
Department of Computer Science and Engineering
Rajiv Gandhi Institute of Technology
Bangalore, India

Mahesh
Department of Computer Science and Engineering
Rajiv Gandhi Institute of Technology
Bangalore, India
maheshbj42@gmail.com

Sudharshan R
Department of Computer Science and Engineering
Rajiv Gandhi Institute of Technology
Bangalore, India
sidhurpns2004@gmail.com

Mahesha J A
Department of Computer Science and Engineering
Rajiv Gandhi Institute of Technology
Bangalore, India
maheshmahesh08008@gmail.com

Gurubasava
Department of Computer Science and Engineering
Rajiv Gandhi Institute of Technology
Bangalore, India
guruvpatil5555@gmail.com

Abstract- The rapid growth of digital payment systems has significantly increased the convenience of financial transactions while simultaneously exposing users and institutions to rising risks of fraudulent activities. Traditional rule-based fraud detection systems are inadequate in identifying complex and evolving fraud patterns due to their static nature and high false-positive rates.

This paper proposes a Hybrid Artificial Intelligence (AI) Model for online payment fraud detection that integrates rule-based systems, supervised machine learning classification, and unsupervised anomaly detection techniques into a unified framework. The model leverages historical transaction data and behavioral patterns to accurately detect fraudulent activities in real time.

Experimental analysis demonstrates improved accuracy, reduced false positives, and enhanced adaptability compared to conventional methods. The proposed system offers a scalable and efficient solution suitable for modern financial ecosystems.

Index Terms— Anomaly Detection, Fraud Detection, Machine Learning, Online Payments, Supervised Learning

I. INTRODUCTION

The evolution of digital payment technologies, including mobile banking, e-commerce platforms, and real-time transaction systems, has revolutionized financial operations worldwide. However, this rapid advancement has also introduced significant security challenges, particularly in detecting and preventing fraudulent transactions.

Fraudulent activities such as identity theft, account takeover, card-not-present (CNP) fraud, and automated bot attacks are

increasingly sophisticated. Traditional fraud detection mechanisms rely heavily on predefined rules and manual verification, which are insufficient in handling dynamic and large-scale data environments.

To address these limitations, this paper introduces a **hybrid AI-based fraud detection model** that combines:

- Rule-based expert systems for initial filtering
- Supervised learning models for classification
- Unsupervised learning models for anomaly detection

This integrated approach enhances detection capability while maintaining scalability and real-time performance.

II. EXISTING SYSTEM

Current fraud detection systems primarily rely on the following approaches:

- Rule-based systems using predefined conditions
- Supervised machine learning models trained on labeled datasets
- Single-model anomaly detection techniques
- Human reviewer-based verification systems

While these methods provide baseline protection, they fail to address evolving fraud patterns effectively.

III. DISADVANTAGES OF EXISTING SYSTEM

Existing systems suffer from several limitations:

- High false positive rates affecting user experience
- Lack of adaptability to new fraud techniques
- Dependence on labeled datasets
- Limited scalability with increasing transaction volume
- Inefficient real-time detection capabilities
- Poor handling of unknown or zero-day fraud patterns

IV. PROPOSED SYSTEM

The proposed system introduces a **Hybrid AI Model** that integrates multiple detection techniques into a layered architecture.

IV.I **System Architecture :**

The system consists of three main components:

1. **Rule-Based Engine**
   - Applies predefined rules (e.g., transaction limit, location mismatch)
2. **Supervised Learning Model**
   - Algorithms such as Random Forest and XGBoost
   - Classifies transactions as fraudulent or legitimate
3. **Unsupervised Anomaly Detection**
   - Uses techniques like Isolation Forest
   - Detects unusual transaction patterns

IV.II **Workflow :**

1. Transaction data is collected
2. Feature extraction is performed
3. Rule-based filtering is applied
4. ML model predicts fraud probability
5. Anomaly detection evaluates unusual behavior
6. Final decision is made using ensemble scoring

V. ADVANTAGES OF PROPOSED SYSTEM

The proposed model offers the following benefits:

- Improved accuracy through hybrid learning

- Reduced false positives using ensemble techniques
- Real-time fraud detection capability
- Adaptability to evolving fraud patterns
- Reduced dependence on labeled data
- High scalability for large datasets
- Enhanced explainability via rule-based decisions

VI. METHODOLOGY

6.1 Dataset

The system can utilize publicly available datasets such as:

- Kaggle Credit Card Fraud Dataset

6.2 Features Used

- Transaction amount
- Transaction time
- Location/IP address
- Device information
- User behavior patterns

6.3 Algorithms

- Random Forest
- XGBoost
- Isolation Forest

6.4 Evaluation Metrics

- Accuracy
- Precision
- Recall
- F1-Score

VII. LITERATURE SURVEY

Several studies have explored fraud detection using machine learning:

- Diana T. Mosa et al. (2024) proposed hybrid ML models with meta-heuristic optimization for improved accuracy.
- Abdulwahab Ali Almazroi et al. (2023) compared various ML techniques for fraud detection.
- J.G.K.P (2022) demonstrated that XGBoost performs better than Random Forest in imbalanced datasets.
- Ritam Maity et al. (2025) analyzed multiple ML algorithms but lacked hybrid approaches and real-time implementation.

These studies highlight the need for integrated and scalable hybrid systems.

VIII. RESULTS AND DISCUSSION

The hybrid model improves fraud detection performance by combining strengths of multiple techniques. Compared to traditional systems, it:

- Achieves higher detection accuracy
- Reduces false positive rates
- Enhances detection of unknown fraud patterns

The ensemble approach ensures balanced decision-making and improved reliability.

IX. CONCLUSION

This paper presents a hybrid AI-based fraud detection system that integrates rule-based logic, supervised learning, and anomaly detection. The proposed system effectively identifies fraudulent transactions while maintaining scalability and real-time performance.

Future work includes:

- Integration of deep learning models
- Deployment in real-time financial systems
- Use of streaming data processing frameworks

REFERENCES

1. J. G. K. P., “Fraud Detection in Banking Transactions using Random Forest and XGBoost,” 2022.

2. A. Almazroi, “Online Payment Fraud Detection Using Machine Learning Techniques,” 2023.
3. M. Rukhsar et al., “Automating Machine Learning Algorithms for Financial Transactions,” 2023.
4. K. R. Dileep et al., “Efficient Credit Card Fraud Detection using Machine Learning,” 2023.
5. V. V. Ganesh et al., “Credit Card Fraud Detection using Ensemble Methods,” 2022.
6. A. Hafeez et al., “Enhanced AI-based Model for Financial Fraud Detection,” 2023.