IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

Machine Learning-Based Fraud Detection : A Predictive Approach for Identifying Fraudulent Financial Transactions

Pritam Pathare, Santosh Pawar, Snehal Phapale
Department of Master of Computer Applications (MCA)
Vidya Niketan Institute of Management and Computer Application, Bota

Abstract: *Fraud detection is an important challenge in digital banking, online shopping, and electronic payment systems. Traditional methods rely on predefined rules and may fail to identify new fraud patterns. Machine Learning (ML) helps detect suspicious activities by analyzing transaction data and identifying unusual behavior. This review paper discusses machine learning techniques, including Logistic Regression, Decision Trees, Random Forest, and Neural Networks. It also examines applications, challenges, and future developments in fraud detection. Machine learning can improve fraud detection accuracy and efficiency when supported by reliable data and continuous monitoring*

Keywords: Machine Learning, Fraud Detection, Artificial Intelligence, Credit Card Fraud, Cybersecurity, Anomaly Detection.

I. INTRODUCTION

The growth of digital transactions has increased the risk of financial fraud. Fraudsters use stolen card details, unauthorized account access, and fake transactions to cause financial losses.

Traditional fraud detection systems use predefined rules, which may not identify complex or new fraud patterns. Machine learning provides an advanced approach by learning from historical data and identifying suspicious transactions.

This paper reviews machine learning techniques, their applications, challenges, and future scope in fraud detection.

II. KEY FEATURES OF MACHINE LEARNING-BASED FRAUD DETECTION

2.1 Supervised Learning

Supervised learning uses labeled transaction data to classify transactions as fraudulent or legitimate. Common algorithms include Logistic Regression, Decision Trees, and Random Forest.

2.2 Unsupervised Learning

Unsupervised learning identifies unusual transaction patterns without requiring labeled fraud data. It is useful for detecting previously unknown suspicious activities.

2.3 Random Forest

Random Forest combines multiple decision trees to improve classification performance. It can identify complex patterns in transaction data.

2.4 Neural Networks

Neural networks learn complex relationships in large datasets and can help detect suspicious financial activities.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/568
ISSN 2581-9429 IJARSCT

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

III. APPLICATIONS OF FRAUD DETECTION

3.1 Credit Card Fraud

Machine learning analyzes transaction amounts, locations, and spending habits to identify potentially unauthorized transactions.

3.2 Banking and Digital Payments

Banks use machine learning to identify suspicious transfers and unusual account activities.

3.3 E-Commerce

Online shopping platforms use machine learning to detect payment fraud, account takeovers, and suspicious refund requests.

3.4 Insurance

Machine learning analyzes insurance claims and identifies unusual patterns that may require investigation.

IV. COMPARISON OF MACHINE LEARNING TECHNIQUES

Algorithm	Main Advantage	Limitation
Logistic Regression	Simple and efficient	Limited for complex patterns
Decision Tree	Easy to understand	Can overfit
Random Forest	Handles complex patterns	Requires more resources
Neural Networks	Learns complex relationships	Difficult to interpret

The choice of algorithm depends on the dataset, computational resources, and fraud detection requirements.

V. CHALLENGES AND LIMITATIONS

• Imbalanced Data: Fraudulent transactions are much less common than legitimate transactions, making detection difficult.
• False Predictions: Legitimate transactions may be incorrectly flagged, while some fraudulent transactions may go undetected.
• Changing Fraud Patterns: Fraudsters continuously develop new methods, requiring regular model updates.
• Data Privacy: Financial information must be protected through appropriate security measures.
• Computational Cost: Complex models may require significant processing power for real-time detection.

VI. FUTURE TRENDS

Machine learning-based fraud detection is expected to improve through real-time transaction monitoring, explainable AI, deep learning, and hybrid models. These technologies may help identify new fraud patterns and improve system transparency.

Future systems may also use adaptive learning to respond to changing fraudulent activities while maintaining customer privacy and security.

VII. CONCLUSION

Machine learning is an effective approach to identifying suspicious financial transactions. Algorithms such as Logistic Regression, Random Forest, and Neural Networks can help detect fraud in banking, e-commerce, credit card transactions, and insurance.

Although challenges such as imbalanced data, false positives, and privacy concerns remain, continuous monitoring and improved algorithms can strengthen fraud detection systems. Machine learning is expected to play an increasingly important role in financial security.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

REFERENCES

1. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235–255.
2. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119.
3. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15.
4. Breiman, L. (2001). Random forests. Machine Learning, 45, 5–32.