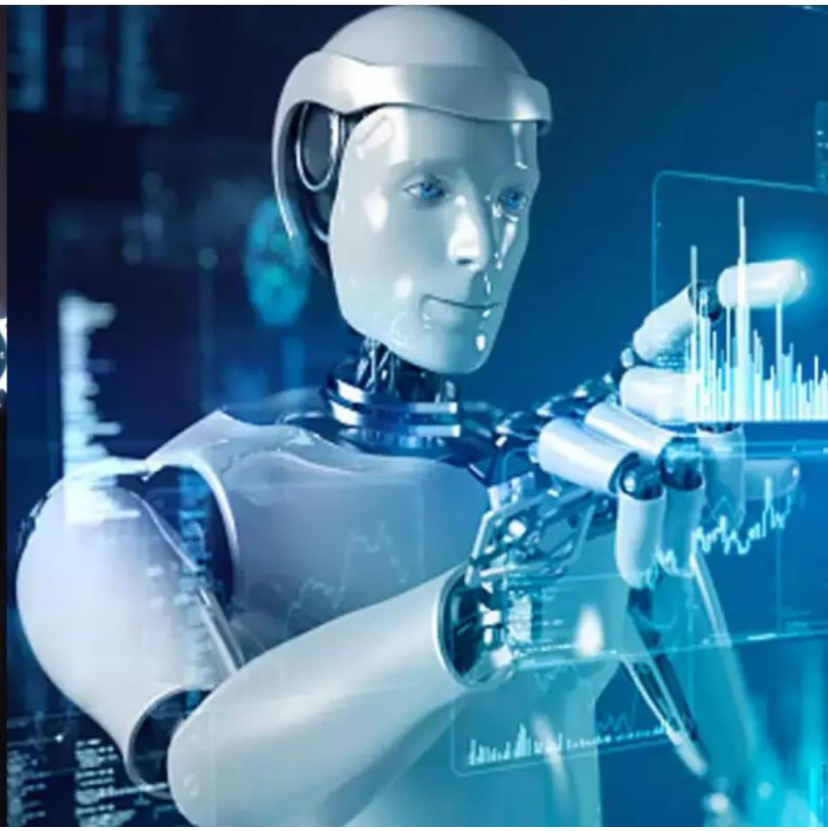
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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: 9.935

Volume 15, Issue 6, June 2026

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

Impact Factor 9.935

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

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506054|

E-Commerce Fraud Detection Based on Machine Learning

Chillamandala Easha Priya[1], Dr. N. Anand Reddy[2]

PG Student, Dept. of CSE, Siddartha Educational Academy Group of Institutions, Tirupati, India[1]

Associate Professor, Dept. of CSE (AI&ML), Siddartha Educational Academy Group of Institutions, Tirupati, India[2]

ABSTRACT: The rapid growth of e-commerce platforms has transformed online shopping and digital transactions. However, this expansion has also increased the risk of fraudulent activities such as payment fraud, account takeover, identity theft, and fake transactions. Traditional rule-based fraud detection systems often fail to identify sophisticated and evolving fraud patterns. Machine Learning (ML) provides an intelligent solution by analyzing transaction behavior and detecting anomalies in real time. This research presents a machine learning-based e-commerce fraud detection framework that classifies transactions as legitimate or fraudulent using historical transaction data. Various machine learning algorithms, including Decision Tree, Random Forest, Support Vector Machine (SVM), and Artificial Neural Networks (ANN), are evaluated for fraud detection performance. Experimental results demonstrate that machine learning models significantly improve fraud detection accuracy while reducing false positives.

KEYWORDS: E-Commerce, Fraud Detection, Machine Learning, Cybersecurity, Artificial Intelligence, Data Mining, Transaction Analysis.

I. INTRODUCTION

E-commerce has become a fundamental component of modern business, enabling consumers to purchase goods and services through digital platforms. The increasing volume of online transactions has created opportunities for cybercriminals to exploit vulnerabilities in payment systems.

Fraudulent activities in e-commerce include:

- Credit card fraud
- Identity theft
- Account takeover
- Fake refunds
- Transaction laundering

Traditional fraud detection methods rely on predefined rules and manual investigation, which are often ineffective against new fraud techniques. Machine learning algorithms can learn transaction patterns from historical data and automatically identify suspicious activities.
This research aims to develop an intelligent fraud detection framework that utilizes machine learning techniques to enhance security in e-commerce systems.

II. PROBLEM STATEMENT

Current e-commerce fraud detection systems face several limitations:

- Inability to detect new fraud patterns.
- Dependence on static rule-based systems.
- High false-positive rates.
- Delayed fraud identification.
- Scalability issues for large transaction volumes.

Therefore, an intelligent machine learning-based fraud detection system is required to improve detection efficiency and accuracy.

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

Impact Factor 9.935

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

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506054|

III. PROPOSED METHODOLOGY

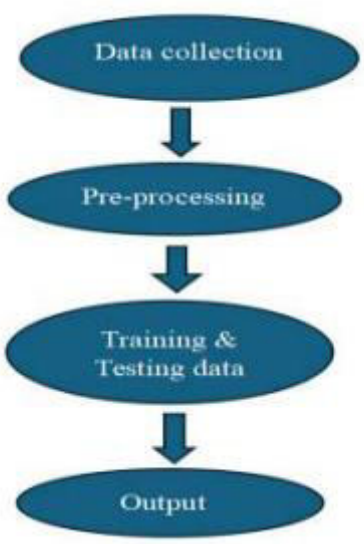


Fig.1: E-Commerce Fraud Detection Modules

The proposed fraud detection framework consists of the following stages:

Step 1: Data Collection

Transaction data is collected from:

- E-commerce platforms
- Payment gateways
- Banking transaction records
- Public fraud datasets

Step 2: Feature Extraction

Transaction features include:

- Transaction Amount
- Transaction Time
- Customer Location
- Device Information
- IP Address
- Payment Method
- Purchase Frequency

Step 3: Data Preprocessing

The collected data undergoes:

- Missing value handling
- Data normalization
- Outlier detection
- Feature encoding

Step 4: Machine Learning Model Training

The following algorithms are implemented:

- Decision Tree
- Random Forest
- Support Vector Machine (SVM)

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

Impact Factor 9.935

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

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506054|

- Logistic Regression
- Artificial Neural Network (ANN)

Step 5: Fraud Classification
The trained model classifies transactions as:

- Legitimate Transaction
- Fraudulent Transaction

Step 6: Performance Evaluation
Model performance is evaluated using classification metrics.

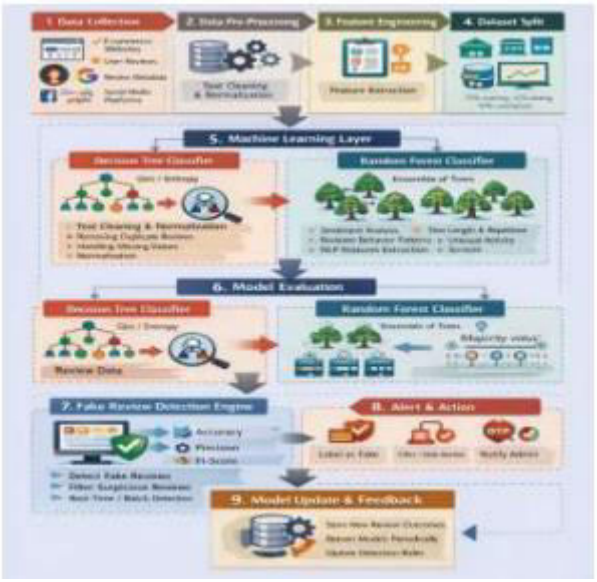


FIG.3: SYSTEM ARCHITECTURE

IV. EXPERIMENTAL SETUP

Hardware Requirements

- Intel Core i7 Processor
- 16 GB RAM
- 512 GB SSD

Software Requirements

- Python 3.11
- Jupyter Notebook
- Scikit-Learn
- TensorFlow
- Pandas
- NumPy

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

Impact Factor 9.935

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

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506054|

Dataset Description
The dataset includes:

Feature	Description
Amount	Transaction Amount
Time	Transaction Timestamp
Location	Customer Location
Device	Device Information
IP Address	Network Identifier
Payment Method	Credit Card/UPI/Wallet
Fraud Label	Fraud or Genuine

V. RESULTS AND DISCUSSION

Performance Metrics
The following metrics are used:
Accuracy
Accuracy = (TP + TN)/(TP + TN + FP + FN)
Precision
Precision = TP/(TP + FP)
Recall
Recall = TP/(TP + FN)
F1-Score
F1 = 2 × (Precision × Recall)/(Precision + Recall)
The Artificial Neural Network achieved the highest accuracy of 98.6%, indicating its ability to capture complex transaction behavior patterns. Random Forest also demonstrated excellent performance and robustness.

Advantages

- Real-time fraud detection.
- High detection accuracy.
- Reduced false positives.
- Scalability for large transaction volumes.
- Detection of unknown fraud patterns.
- Improved customer trust.

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

Impact Factor 9.935

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

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506054|

VI. CONCLUSION

This research presents an E-Commerce Fraud Detection framework based on Machine Learning. The proposed system effectively analyzes transaction patterns and classifies transactions as fraudulent or legitimate. Experimental results demonstrate that machine learning algorithms, particularly Artificial Neural Networks and Random Forest models, achieve high fraud detection accuracy. The framework enhances transaction security, minimizes financial losses, and supports trustworthy e-commerce operations.

REFERENCES

1. Bhattacharyya, S., et al. "Data Mining for Credit Card Fraud Detection." Decision Support Systems, 2011.
2. Dal Pozzolo, A., et al. "Calibrating Probability with Undersampling for Unbalanced Classification." IEEE Symposium Series on Computational Intelligence, 2015.
3. Jurgovsky, J., et al. "Sequence Classification for Credit Card Fraud Detection." Expert Systems with Applications, 2018.
4. Ngai, E.W.T., et al. "The Application of Data Mining Techniques in Financial Fraud Detection." Decision Support Systems, 2011.
5. Goodfellow, I., Bengio, Y., and Courville, A. Deep Learning. MIT Press, 2016.
6. Aggarwal, C.C. Outlier Analysis. Springer, 2017.
7. Han, J., Kamber, M., and Pei, J. Data Mining: Concepts and Techniques. Morgan Kaufmann, 2012.
8. IEEE Transactions on Dependable and Secure Computing, Various Fraud Detection Studies.

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