International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 2, Mar-Apr 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Machine Learning-Based Real-Time E-Commerce Fraud Detection

K Naresh[1], Kuntrapakam Dhananjayulu[2]

[1]Assistant Professor, Department of MCA, Annamacharya Institute of Technology and Sciences, Tirupati, Andhra Pradesh, India.
[2]Postgraduate, Department of MCA, Annamacharya Institute of Technology and Sciences, Tirupati, Andhra Pradesh, India.

Abstract

The volume of online transactions has expanded dramatically due to the e-commerce platforms' rapid expansion, making them an ideal target for fraudulent activity. Because traditional rule-based systems frequently fall short in identifying intricate and dynamic fraud patterns, detecting fraudulent transactions in real time has become a crucial challenge for enterprises. In order to detect e-commerce fraud in real time, this study suggests a machine learning-based method that examines transaction data to spot questionable activity. To differentiate between legal and fraudulent transactions, the system trains classification models using data preprocessing techniques. A web-based application framework is created to effectively monitor transactions and forecast fraud. The suggested approach assesses transaction characteristics and looks for irregularities that might point to fraud.

According to experimental data, the system can detect possible fraud more accurately and quickly than traditional approaches. This strategy can help e-commerce companies increase consumer trust, decrease financial losses, and improve transaction security. The study emphasises how machine learning techniques can be used to create scalable and sophisticated fraud detection systems for contemporary digital commerce environments.

Keywords

E-commerce Fraud Detection, Machine Learning, Transaction Analysis, Fraudulent Transactions, Data Preprocessing, Real-Time Monitoring, Artificial Intelligence.

I. Introduction

E-commerce platforms' explosive growth has completely changed how consumers buy and sell goods worldwide. E-commerce has grown to be a crucial component of contemporary commerce due to the rise in the usage of digital payment methods, mobile transactions, and online purchasing. But this quick expansion has also resulted in a sharp increase in fraudulent activity, such as identity theft, payment fraud, fraudulent transactions, and unauthorised access to user accounts. Businesses suffer financial losses as a result of these fraudulent operations, and consumers lose faith in internet platforms.

Conventional fraud detection systems mostly rely on manual monitoring techniques and rule-based approaches. These algorithms are capable of identifying some forms of fraud, but they frequently fall short in spotting intricate and dynamic fraudulent patterns. Static rule-based systems find it challenging to identify suspicious activity in real time since fraudsters are always coming up with new ways to get around established security measures.

Machine learning algorithms have become an efficient way to identify fraudulent transactions in order to overcome these difficulties. Large amounts of transaction data may be analysed by machine

learning algorithms, which can also find hidden patterns and abnormalities that might point to fraud. These models can more accurately identify transactions as fraudulent or lawful by learning from past transaction information.

A framework based on machine learning is suggested in this study to identify fraudulent transactions in e-commerce systems. To find suspicious activity, the system preprocesses data, analyses transaction data, and uses classification algorithms. The detection model is combined with a web-based interface to track transactions and offer recommendations in real time. The suggested approach seeks to lower financial risks, strengthen e-commerce platform dependability, and increase online transaction security.

II. Literature Survey

The rise in online financial transactions has made e-commerce fraud detection a significant field of study. To efficiently identify fraudulent activity, researchers have developed a number of machine learning and data mining techniques.

The application of machine learning algorithms for online transaction fraud detection has been the subject of several studies. To examine transaction patterns and spot questionable activity, researchers have used classification models including Random Forest, Decision Trees, Logistic Regression, and Support Vector Machines. These models are able to identify anomalous patterns that can point to fraud by learning from past transaction data.

Deep learning techniques have also been employed by some researchers to enhance the effectiveness of fraud detection. Deep learning algorithms and neural networks may find intricate patterns in big datasets. By examining several transaction characteristics at once, these methods aid in increasing the precision of fraud detection systems. However, big datasets and a lot of processing power are frequently needed for deep learning models.

Anomaly detection is a crucial strategy in fraud detection. In this method, the system identifies transactions that significantly deviate from normal user behavior. Unusual transaction patterns that can point to fraud are found using methods like statistical analysis and clustering.

Real-time fraud detection systems that can quickly monitor transactions have also been the subject of recent research. These solutions identify fraud as soon as a transaction takes place by integrating machine learning models with web-based platforms. Real-time monitoring enhances the security of e-commerce platforms and helps avoid financial losses.

Many current systems still struggle with issues including high false positive rates, limited scalability, and trouble identifying novel forms of fraud, despite the fact that numerous fraud detection techniques have been put out. As a result, more effective and sophisticated fraud detection systems that can evaluate enormous transaction databases and offer precise real-time forecasts are required.

III. Problem Statement

E-commerce platforms are dealing with an increasing number of fraudulent transactions due to the fast growth of online shopping and digital payment methods. Fraudsters carry out operations including identity theft, fraudulent transactions, and unauthorised payments by taking advantage of flaws in online systems. Businesses suffer large financial losses as a result of these fraudulent operations, which also erode consumer confidence in online platforms.

Conventional fraud detection systems mostly use manual monitoring techniques and pre-established regulations. Nevertheless, these algorithms are unable to identify novel forms of attacks or intricate fraud patterns. Because fraudsters constantly alter

their tactics, it is challenging for static rule-based systems to successfully detect suspicious activity.

The enormous number of transactions that are produced daily on e-commerce platforms is another significant obstacle. It takes a lot of time and is ineffective to manually analyse such massive volumes. An intelligent system that can automatically evaluate transaction data, spot suspicious activity, and quickly identify fraudulent transactions is therefore required.

The goal of this research is to create a machine learning-based fraud detection system that can identify fraudulent or valid transactions by analysing transaction patterns. The suggested solution seeks to decrease response times and manual labour while increasing the accuracy of fraud detection.

IV. Workflow Explanation

The suggested e-commerce fraud detection system's workflow outlines the steps taken to process transaction data and use machine learning algorithms to identify fraudulent activity. The e-commerce platform's transaction data is first gathered by the system. A variety of characteristics, including transaction amount, payment method, user behaviour, location data, and other pertinent transaction aspects that aid in spotting suspicious activity, may be included in this data.

Data preparation is the next stage after data collection. The dataset is cleaned at this stage by eliminating missing values, fixing inconsistent data, and, if required, transforming categorical features into numerical form. Data preparation guarantees that the machine learning model can analyse the information efficiently and enhances the dataset's quality.

Feature extraction and selection are carried out following preprocessing. Key transaction characteristics that play a major role in identifying fraud are chosen. These characteristics aid in the model's comprehension of trends connected to both legal and fraudulent transactions.

After processing, the data is utilised to train a machine learning algorithm on past transaction data. The model discovers correlations and similarities between various transaction attributes and the fraud label. The program can recognise suspicious behaviour in subsequent transactions thanks to this learning process.

After training, the model is included into the fraud detection system, where it performs real-time analysis of incoming transaction data. The system processes the incoming data and transmits it to the trained model for prediction whenever a new transaction takes place.

Lastly, the system uses the prediction findings to determine whether the transaction is fraudulent or legitimate. The output is shown via the web interface, which enables system users or administrators to keep an eye on transaction activity and take appropriate action when questionable transactions are found. The solution can offer effective and automated fraud detection for e-commerce platforms thanks to this methodology.

V. Dataset

Information on e-commerce transactions that aids in spotting fraudulent activity can be found in the dataset utilised in this study. A user's single transaction on an e-commerce platform is represented by each record in the dataset. The dataset contains a number of crucial characteristics that characterise the specifics of the transaction, including the transaction amount, payment type, IP address, location, and fraud status.

The user's transaction's monetary value is represented by the amount attribute. Because abnormally high or irregular transaction amounts could point to suspect activity, this functionality is crucial. The method used to finish the transaction—such as net banking, debit card, credit card, wallet,

or UPI—is specified by the payment_method attribute.

This feature is helpful for detecting fraud because different payment methods may have varying fraud risk levels.

The country or region from which the transaction was conducted is indicated by the location attribute. Transactions coming from strange or unexpected places could be a symptom of fraud. The IP address linked to the transaction is represented via the ip attribute, which aids in locating the activity's network source. Monitoring IP addresses can assist in identifying suspicious access patterns or multiple fraudulent transactions from the same source.

The machine learning model's goal variable, is_fraud, is the last attribute in the dataset. The legitimacy or fraudulence of a transaction is indicated in this column.

A transaction with a value of 0 is considered valid, but a transaction with a value of 1 is considered fraudulent.

The machine learning algorithm discovers patterns connected to both legitimate and fraudulent transactions by examining these characteristics. The fraud detection model is trained and assessed using the dataset, allowing the system to instantly identify suspicious activity and categorise fresh transactions.

amount	payment_method	location	ip	is_fraud
8445	net_banking	US	171.174.170.81	0
5115.19	net_banking	CN	95.25.112.121	0
9678.16	wallet	DE	51.105.121.194	0
2188.34	debit_card	GB	195.110.164.126	0
952.83	wallet	DE	141.250.247.54	0
8103.12	debit_card	GB	12.130.104.103	1
742.06	wallet	AU	70.17.181.9	0
3541.14	wallet	DE	144.8.75.189	0
2048.76	upi	AU	196.150.125.12	0
5215.93	credit_card	CN	36.184.50.44	0
9160.36	credit_card	FR	218.144.249.195	0
7103.98	credit_card	DE	19.56.241.190	0
8676.69	debit_card	FR	52.60.145.21	0
8705.36	debit_card	DE	141.22.41.210	0
8034.43	debit_card	CN	195.232.117.64	0
916.7	wallet	DE	24.85.243.248	0

Fig: Dataset

VI. Experimental Results and Analysis

A machine learning prediction model was coupled with a web-based application to implement the suggested e-commerce fraud detection system. Via a web interface, the system enables administrators or users to input transaction parameters including IP address, location, payment method, and transaction amount. The trained machine learning model processes these inputs to ascertain if the transaction is authentic or perhaps fraudulent.

The user interface offers an easy-to-use, interactive form for entering transaction details. The system transmits the input data to the backend model for analysis after the user presses the Predict Fraud button. The transaction attributes are assessed by the machine learning model, which then contrasts them with patterns discovered from past transaction data. The model forecasts whether the transaction is legitimate or fraudulent based on this analysis. The suggested system's fraud prediction interface is depicted in the figure. The interface shows the prediction result following analysis and has fields for adding transaction information. In the given example, the model has found suspicious patterns in the input data, as evidenced by the system's identification of the transaction as possibly fraudulent.

Administrators can swiftly spot suspicious activity and take the appropriate steps to stop financial losses thanks to its real-time prediction capacity. The system can effectively execute automated fraud detection and offers a user-friendly environment for tracking transaction activity thanks to the combination of a machine learning model with an online interface.

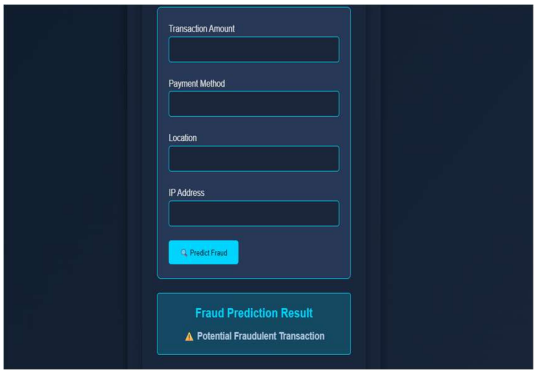

Fig: Fraud Detection Interface Showing Transaction Input and Prediction Result

VII. Conclusion

This study presents a machine learning-based method for identifying fraudulent transactions on e-commerce sites. To find suspicious activity, the suggested system examines transaction data, including IP address, location, payment method, and transaction amount. The technology may identify trends in past transaction data and categorise future transactions as authentic or fraudulent by using machine learning algorithms. Users can enter transaction information and receive real-time fraud detection findings thanks to the prediction model's integration with a web-based interface. This makes it easier for administrators to see possibly fraudulent transactions fast and take the appropriate precautions. The technology offers an automated solution that lowers manual labour and boosts fraud detection effectiveness.

References

[1] V. J. Hodge and J. Austin, "A survey of outlier detection methodologies," Artificial Intelligence Review, vol. 22, no. 2, pp. 85–126, 2004.

[2] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," in IEEE Symposium on Computational Intelligence and Data Mining, 2015, pp. 159–166.

[3] 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.

[4] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," Artificial Intelligence Review, vol. 34, no. 1, pp. 1–14, 2010.

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

[6] R. Jurgovsky, M. Granitzer, K. Ziegler, et al., "Sequence classification for credit-card fraud detection," Expert Systems with Applications, vol. 100, pp. 234–245, 2018.

