



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

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*



**Impact Factor: 8.699**

**Volume 14, Issue 12, December 2025**

# Intelligent Fraud Detection System for E-Commerce using Machine Learning

Mamidi Chandana<sup>1</sup>, Dr. P. Sivakrishna<sup>2</sup>, Dr. D.V Sateesh Kaladhar Reddy<sup>3</sup>

M. Tech, Dept. of CSE, Andhra Engineering College, Atmakur, SPSR Nellore, AP, India<sup>1</sup>

Professor, Dept. of CSE, Andhra Engineering College, Atmakur, SPSR Nellore, AP, India<sup>2</sup>

Assistant Professor, Dept. of CSE, Andhra Engineering College, Atmakur, SPSR Nellore, AP, India<sup>3</sup>

**ABSTRACT:** The detection and prevention of fraudulent transactions in e-commerce platforms has long been at the core of transaction security solutions. However, because e-commerce is concealed, it is challenging to catch attackers using just past order data. Many research try to develop technology that prevent fraud, but they don't consider how consumers' behavior is evolving from different perspectives. This complicates the process of identifying fraudulent behavior. This paper proposes a new method for detecting fraud by tracking user activity in real time using a combination of process mining and machine learning models. First, we develop a process model for the B2C e-commerce platform that incorporates user behavior identification. Second, a method for anomaly analysis that may be used to event logs to find noteworthy features is explained. We next use Ensemble Learning to integrate the gathered information into a classification model that identifies fraudulent activity.

**KEYWORDS:** Component, formatting, style, styling, insert.

## I. INTRODUCTION

Anti-fraud solutions are now essential to ensuring the security of online transactions due to the Internet's dynamic and dispersed character. When addressing new security threats, vulnerabilities are still identified by current fraud detection systems that concentrate on identifying unusual user activity. The ineffective process management of current fraud detection technologies throughout the trading process is a significant problem. One of the main problems that requires attention is the ineffective monitoring function. Because process capture is lacking in the current work, the detection perspective is typically insufficient. In order to do this, we suggest a process-based approach in which historical data is converted into controlled data and user behaviors are captured and examined in real-time. Furthermore, we integrate a multi-perspective approach for identifying anomalous behaviors.

In order to solve the anomaly detection in data flows, this research introduces a hybrid approach that gives information about each action incorporated in a control flow model, combining the benefits of process mining and machine learning models. This approach can dynamically detect changes in user behaviors, transaction processes, and noncompliance issues by modeling and evaluating the e-commerce system's business process. It can also thoroughly evaluate and identify fraudulent transactions from a variety of angles. The following is a list of this paper's significant contributions:

- 1) To identify the anomalies in e-commerce transactions, a conformance checking technique based on process mining is used.
- 2) To carry out thorough anomaly detection based on Petri nets, a user behavior detection technique is suggested.
- 3) To automatically classify fraudulent actions, an SVM model is created by integrating multiperspective process mining into machine learning techniques. A growing number of business transactions are now using web-based methods rather than the conventional cash-based method due to the growing popularity of e-commerce platforms. The COVID-19 pandemic has had a significant influence on the entity economy in recent years, but e-commerce has been relatively unscathed, which has helped the sector grow steadily.

By 2023, it is anticipated that business-to-consumer (B2C) e-commerce sales will total 6.5 trillion dollars. In recent years, new security dangers have surfaced, despite the fact that the spread of contemporary technology and the growth of e-commerce present improved chances for online firms. According to reports, the substantial rise in online fraud cases costs billions of dollars annually on a global scale.

## **II. LITERATURE SURVEY**

### **A. Electronic Payment Systems in Electronic Commerce**

Since it gives consumers a new way to purchase goods and services through electronic means—the Internet and the WWW being the most significant—electronic commerce is becoming increasingly significant in the modern economy. Trust is one of the most significant issues that this new mode of trade brings up about the manner in which payments are made. This essay begins by outlining some of the intricacies of electronic commerce payments in the modern economy, from the viewpoints of buyers and sellers. The distinctions between electronic and traditional payment methods are then discussed, along with how each handles the problems that have been observed. The benefits offered by electronic commerce are then used to identify electronic payment systems (EPS).

### **B. An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection**

Illegal acts pertaining to online financial transactions have grown more intricate and international in nature in recent years, causing significant financial losses for both consumers and businesses. Numerous methods have been put forth to prevent and identify fraud in online settings. Nevertheless, each of these methods has unique traits, benefits, and drawbacks in addition to sharing the objective of detecting and stopping fraudulent online transactions. In light of this, this paper examines the body of research on fraud detection in order to identify the algorithms that are employed and evaluate each one according to specific standards. The systematic quantitative literature review methodology was used to examine the research studies in the area of fraud detection. A hierarchical typology is created based on the most popular machine-learning algorithms in scholarly publications and their attributes. Therefore, by integrating three selection criteria accuracy, coverage, and costs our research presents the best methods for identifying fraud in a novel approach.

### **C. A comparison study of credit card fraud detection: Supervised versus unsupervised**

Due to the widespread use of credit cards for both online and offline purchases, the number of fraud transactions is rising daily. Therefore, an effective fraud detection mechanism is necessary to keep the payment system reliable. In order to compare several supervised and unsupervised methods for detecting credit card fraud, we conduct this study. This study specifically examines four unsupervised anomaly detection models: One-Class SVM (OCSVM), Auto-Encoder (AE), Restricted Boltzmann Machine (RBM), and Generative Adversarial Networks (GAN) in addition to six supervised classification models: Logistic Regression (LR), K-Nearest Neighbors (KNN), Support Vector Machines (SVM), Decision Tree (DT), Random Forest (RF), and Extreme Gradient Boosting (XGB). A public credit card transaction dataset from the Kaggle website, which includes 492 frauds out of 284,807 transactions, is used to train all of these models. Only supervised learning models make advantage of the transaction labels. Five-fold cross validation is used to assess each model's performance in terms of Area Under the Receiver Operating Curves (AUROC).



### III. PROPOSED SYSTEM

The overview of our proposed system is shown in the below figure.

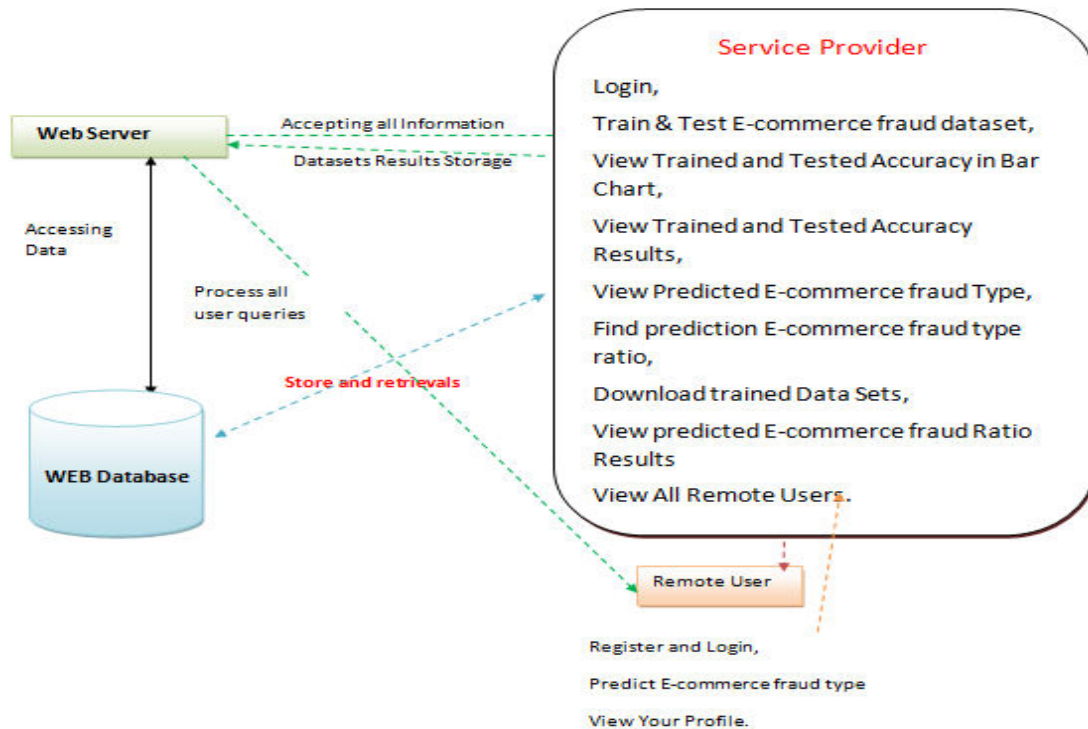


Fig. 1: System Overview

#### Implementation Modules

##### Service Provider:

- The Service Provider must use a working user name and password to log in to this module. Following a successful login, he can perform various tasks like browsing datasets and training and testing datasets. View the predicted fraud detection type in e-commerce transactions, view the fraud detection type in e-commerce transactions ratio, view the trained and tested accuracy in a bar chart, view the trained and tested accuracy results, View the results of the fraud detection type in e-commerce transactions ratio, download predicted data sets, and view all remote users.

##### Train and Test Model

- The service provider divided the used dataset in this module into 70% train data and 30% test data, respectively. Thirty percent of the data is regarded as test data, which is used to evaluate the model, and seventy percent is regarded as train data, which is used to train the model.

##### Graphical Analysis

- Show graphs such as the system's accuracy and predicted ratio in this module. The graph analysis takes into account a number of parameters. Plot charts such as bar charts and others at this phase.

##### Remote User:

- There are n users in this particular module. Before beginning any operations, the user should register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and permitted user name to log in. Following a successful login, the user will perform several

tasks, such as registering and logging in. Determine the type of fraud that will be detected in e-commerce transactions, Check out your profile.

## Implementation Algorithms Support Vector Machine

- Support-vector machines (SVMs, also known as support-vector networks) are supervised learning models in machine learning that use related learning methods to examine data for regression and classification. As a non-probabilistic binary linear classifier, an SVM training technique creates a model that allocates new samples to either category.

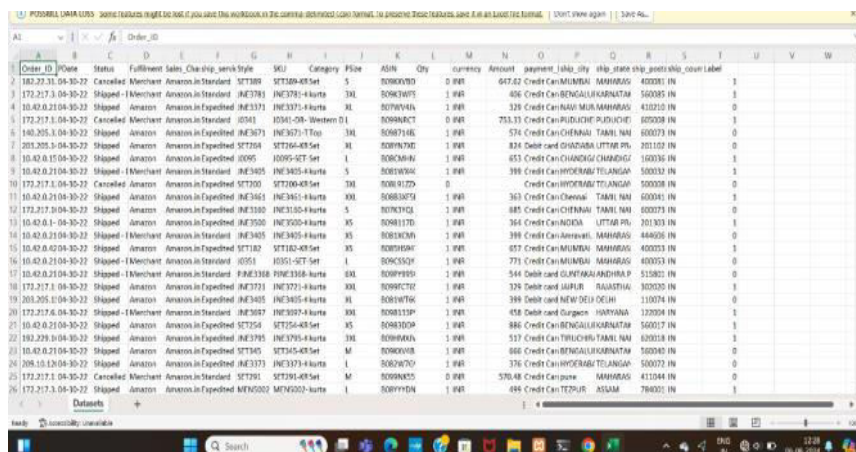
## Logistic Regression

- Among the most widely used machine learning algorithms, logistic regression falls under the category of supervised learning. With a given collection of independent factors, it is used to predict the categorical dependent variable.
- A categorical dependent variable's output is predicted by logistic regression. As a result, the result needs to be a discrete or category value. Yes or No, 0 or 1, true or false, etc., can be used, but probabilistic values that fall between 0 and 1 are provided rather than the precise values of 0 and 1.

## IV. RESULTS



Fig. 2: Home Page



Order ID	Date	Status	Fulfillment	Sales	Ship	Service	Style	SKU	Category	Price	ASIN	Qty	Currency	Amount	payment	ship	city	ship	state	ship	post	ship	cover	label
182.22.1.04-30-22	Cancelled	Merchant	Amazon.in	Standard	SET388	SET388-48-Set	5	ROB00VBD	0 INR	647.62	Credit Card	MUMBAI	MAHARASH	400081	IN	1								
172.217.1.04-30-22	Shipped	Merchant	Amazon.in	Standard	INE3781	INE3781-4-kurta	3XL	ROB0KWT5	1 INR	406	Credit Card	BENGALURU	KARNATAKA	540085	IN	1								
10.40.0.21.04-30-22	Shipped	Amazon	Amazon.in	Expedited	INE3371	INE3371-4-kurta	XL	ROB0V4VL	1 INR	328	Credit Card	RAIPUR	CHHATTISGARH	410210	IN	0								
172.217.1.04-30-22	Cancelled	Merchant	Amazon.in	Standard	JO541	JO541-28-Shorts	01	ROB0NACT	0 INR	753.75	Credit Card	PUDUCHERRY	PUDUCHERRY	620008	IN	1								
140.205.1.04-30-22	Shipped	Amazon	Amazon.in	Expedited	INE3671	INE3671-T-Shirt	3XL	ROB0P74E	1 INR	574	Credit Card	CHENNAI	TAMIL NADU	600073	IN	0								
201.205.1.04-30-22	Shipped	Amazon	Amazon.in	Expedited	SET364	SET364-48-Set	XL	ROB0P74D	1 INR	834	Debit card	CHANDIGARH	UTTAR PRADESH	201102	IN	0								
10.40.0.15.04-30-22	Shipped	Amazon	Amazon.in	Expedited	JO095	JO095-SET	1	ROB0CM4V	1 INR	453	Credit Card	CHANDIGARH	CHANDIGARH	160036	IN	1								
10.40.0.21.04-30-22	Shipped	Merchant	Amazon.in	Standard	INE3405	INE3405-4-kurta	5	ROB0W04C	1 INR	398	Credit Card	HYDERABAD	TELANGANA	500032	IN	1								
172.217.1.04-30-22	Cancelled	Amazon	Amazon.in	Expedited	SET350	SET350-48-Set	3XL	ROB0V1ZD	0		Credit Card	HYDERABAD	TELANGANA	500008	IN	0								
10.40.0.21.04-30-22	Shipped	Amazon	Amazon.in	Expedited	INE3461	INE3461-4-kurta	XXL	ROB0B30T9	1 INR	363	Credit Card	CHENNAI	TAMIL NADU	600041	IN	1								
172.217.1.04-30-22	Shipped	Amazon	Amazon.in	Expedited	INE3180	INE3180-4-kurta	5	ROB0Y7QZ	1 INR	485	Credit Card	CHENNAI	TAMIL NADU	600073	IN	0								
10.40.0.1.04-30-22	Shipped	Amazon	Amazon.in	Expedited	INE3500	INE3500-4-kurta	XS	ROB0B17D	1 INR	364	Credit Card	CHANDIGARH	UTTAR PRADESH	201103	IN	1								
10.40.0.21.04-30-22	Shipped	Merchant	Amazon.in	Standard	INE3405	INE3405-4-kurta	XS	ROB0KCM3	1 INR	398	Credit Card	Amravati	MAHARASHTRA	444006	IN	0								
10.40.0.02.04-30-22	Shipped	Amazon	Amazon.in	Expedited	SET3180	SET3180-48-Set	XS	ROB0Y04H	1 INR	457	Credit Card	CHENNAI	MAHARASHTRA	400023	IN	1								
10.40.0.21.04-30-22	Shipped	Merchant	Amazon.in	Standard	JO551	JO551-SET	1	ROB0C50Y	1 INR	771	Credit Card	MUMBAI	MAHARASHTRA	400033	IN	1								
10.40.0.21.04-30-22	Shipped	Merchant	Amazon.in	Standard	PAE3388	PAE3388-kurta	XXL	ROB0P98D	1 INR	544	Debit card	GUNTUR	ANDHRA PRADESH	515802	IN	0								
172.217.1.04-30-22	Shipped	Amazon	Amazon.in	Expedited	INE3721	INE3721-4-kurta	XXL	ROB0PCT2	1 INR	378	Debit card	JALPAIGURI	ASSAM	786005	IN	1								
201.205.1.04-30-22	Shipped	Amazon	Amazon.in	Expedited	INE3405	INE3405-4-kurta	XL	ROB0W70C	1 INR	398	Debit card	NEW DELHI	DELHI	110074	IN	1								
172.217.1.04-30-22	Shipped	Merchant	Amazon.in	Standard	INE3657	INE3657-4-kurta	3XL	ROB0B13P	1 INR	458	Debit card	Gurgaon	HARYANA	122004	IN	1								
10.40.0.21.04-30-22	Shipped	Amazon	Amazon.in	Expedited	SET354	SET354-48-Set	5	ROB0B30P4	1 INR	486	Credit Card	BENGALURU	KARNATAKA	560017	IN	1								
182.229.1.04-30-22	Shipped	Amazon	Amazon.in	Expedited	INE3795	INE3795-4-kurta	3XL	ROB0W4XV	1 INR	537	Credit Card	TRICHUR	TAMIL NADU	620018	IN	1								
10.40.0.21.04-30-22	Shipped	Amazon	Amazon.in	Expedited	SET3405	SET3405-48-Set	M	ROB0K0VB	1 INR	460	Credit Card	BENGALURU	KARNATAKA	560045	IN	1								
208.10.10.04-30-22	Shipped	Amazon	Amazon.in	Expedited	INE3371	INE3371-4-kurta	L	ROB0W70C	1 INR	378	Credit Card	HYDERABAD	TELANGANA	500072	IN	0								
172.217.1.04-30-22	Cancelled	Merchant	Amazon.in	Standard	SET394	SET394-48-Set	M	ROB0K4Z5	0 INR	570.48	Credit Card	Chennai	MAHARASHTRA	411004	IN	0								
172.217.1.04-30-22	Shipped	Amazon	Amazon.in	Expedited	MEF5002	MEF5002-kurta	L	ROB0PYD4	1 INR	498	Credit Card	TEZPUR	ASSAM	784001	IN	1								

Fig. 3: Datasets

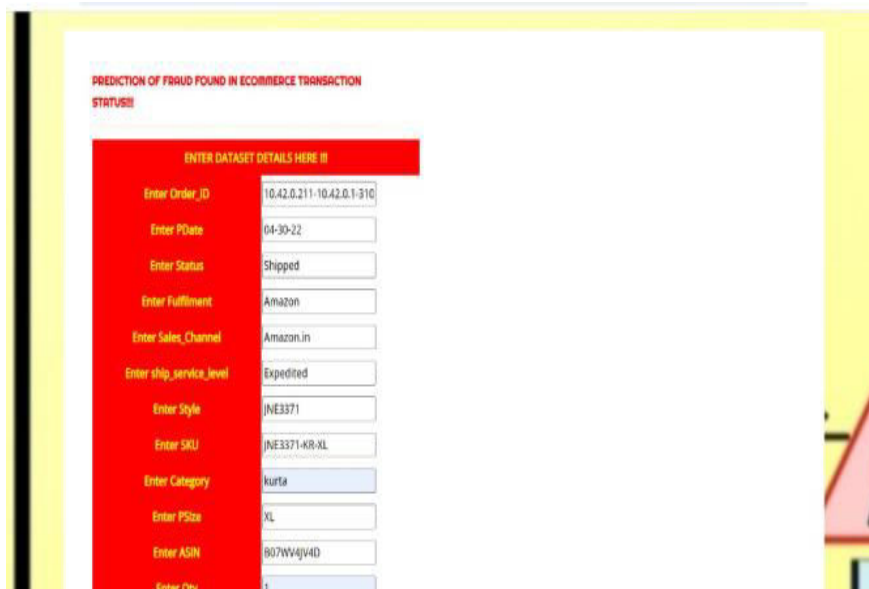


Fig. 4: Prediction of Fraud

**A Multi perspective Fraud Detection Method for Multi Participant Ecommerce Transactions**

Browser and Train & Test Data Sets View Trained and Tested Accuracy in Bar Chart View Trained and Tested Accuracy Results View Prediction Of Fraud Status in Ecommerce Transaction

View Fraud Detection Status Ratio in Ecommerce Transaction Download Trained Data Sets View Ecommerce Transaction Fraud Status Ratio Results View All Reports Users Logout

**Datasets Trained and Tested Results**

Model Type	Accuracy
Naive Bayes	50.95785448613927
SVM	50.191570881226856
Logistic Regression	51.34899616858238
Decision Tree Classifier	50.57472264367817
Extra Tree Classifier	50.38334176245211

Fig. 5: Model Accuracy

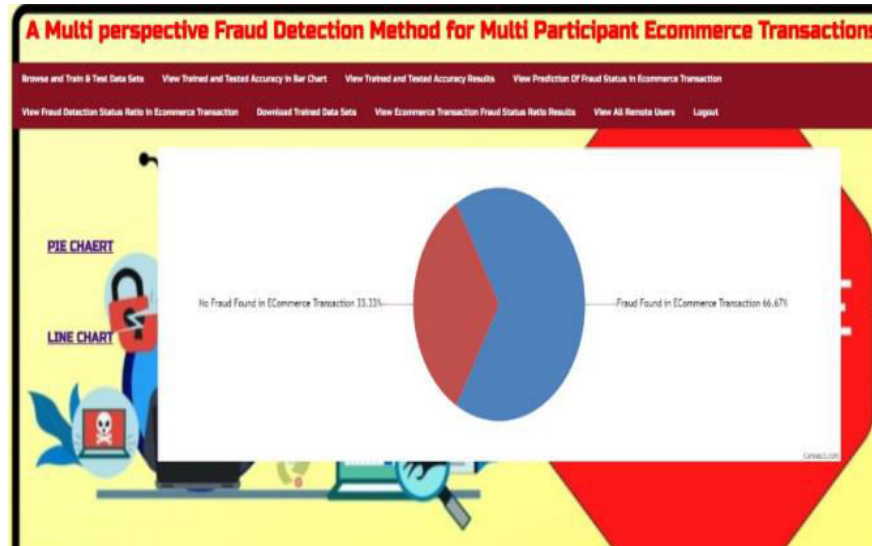


Fig. 6: Model Accuracy in Pie Chart.

## V. CONCLUSION

This study combined formal process modeling with dynamic user behaviors to create a hybrid approach to fraud transaction capture. The five main views that we used to study the e-commerce transaction process were control flow, resource, time, data, and user behavior patterns. This study developed an SVM model to detect fraudulent transactions and used high-level Petri nets as the foundation for process modeling to model the anomalous user behaviors. Our thorough testing demonstrated that the suggested approach is capable of successfully capturing fraudulent transactions and actions. Our suggested multi-perspective detection method fared better overall than the single-perspective detection method. In order to improve accuracy, we plan to include relevant deep learning and model verification techniques into the suggested framework in subsequent work. To improve the accuracy of risk identification, it will also be necessary in the future to add more time aspects to the behavior patterns.

## REFERENCES

- [1] Electronic Payment Systems in Electronic Commerce, R. A. Kuscü, Y. Cicekcisoy, and U. Bozoklu. IGI Global, Turkey, 2020, pp. 114–139.
- [2] M. Abdelrhim and A. Elsayed, "The Impact of COVID-19 Transmission on the E-Commerce Industry: The Situation of the World's Top 5 E-Commerce Firms." 10.2139/ssrn.3621166 is the doi for SSRN 3621166, 2020.
- [3] P. Rao and colleagues, "The link between environmental sustainability and e-commerce supply chain: An empirical study of the online retail industry." pages. 1938377, Cogent. Bus. Manag., vol. 8, no. 1, 2021.
- [4] Int. J. Res. Eng. Sci. Manag., vol. 3, no. 1, pp. 602-606, June 2020; S. D. Dhobe, K. K. Tighare, and S. S. Dake, "A review on prevention of fraud in electronic payment gateway using secret code."
- [5] A. Zainal, M. A. Maarof, and A. Abdallah, "A survey on fraud detection systems," April 2016, J. Netw. Comput. Appl., vol. 68, pp. 90-113.
- [6] "An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection," Info. Econ., vol. 23, no. 1, 2019, by E. A. Minastireanu and G. Mesnita.





INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details