iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.69284

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

A Multi-Perspective Fraud Detection Method for Multi-Participant Ecommerce Transaction

Mrs. Asha Jyothi Panchala[1], K Joshna[2], K Harika[3], M Guru Charan[4], Uday Kiran[5]
[1]*Asst. Prof, Dept of AIML, Ballari Institute of Technology and Management, Ballari, India*
[2, 3, 4, 5]*Dept of AIML, Ballari Institute of Technology and Management, Ballari, India*

Abstract: Tc. It integrates Support Vector Machines (SVM) for fraud classification, Petri nets for anomaly detection, and process mining for conformance checking, ensuring a scalable and robust detection system.
Keywords: Machine learning, Process mining, Anomaly detection, Real-time monitoring.

I. INTRODUCTION

The expansion of e-commerce, driven by advancements in modern technology, has revolutionized online business operations. However, the increasing reliance on digital transactions has also led to the emergence of sophisticated fraud schemes, resulting in substantial financial losses globally.

Furthermore, the inability of present systems to offer a multifaceted examination of transactional processes results in ineffective fraud detection and mitigation.This project suggests a multi-perspective fraud detection method to overcome these issues. mechanism for e-commerce transactions involving multiple participants. The method improves the identification and categorization of fraudulent transactions by introducing a hybrid strategy that blends machine learning models with process mining approaches. This technique enables thorough fraud detection by capturing user activity and transaction processes in real time and turning past data into useful insights.

A. Objectives

This research focuses on the following goals of the study:

1) Identify and classify suspicious transactions by examining user behavior and transaction anomalies.
2) Enhance fraud detection precision while reducing false positives for improved reliability.

II. RELATED WORKS

A. Literature Survey

[1] Machine Learning Algorithms for Fraud Detection (2019) by G Mesnita: This research explores various algorithms like decision trees and neural networks, assessing their effectiveness in detecting online fraud.

[2] Transaction Fraud Detection using Logical Graph of BP (2018) by Lutao Zheng et al.: Introduces a total-order logic graph to model transactional relationships, enhancing detection performance.

[3] Hybrid Association Rule Learning and Process Mining (2015) by Riyanarto Sarno et al.: Combines association rules and process mining to reduce false discoveries and boost detection accuracy.

III. PROPOSED METHOD

The proposed solution addresses anomaly detection in data flows through a hybrid approach that integrates process mining and machine learning techniques.

1) To identify the anomalies in e-commerce transactions, a conformance checking technique based on process mining is used.
2) For effective anomaly identification using Petri nets, a user behavior detection technique is proposed.

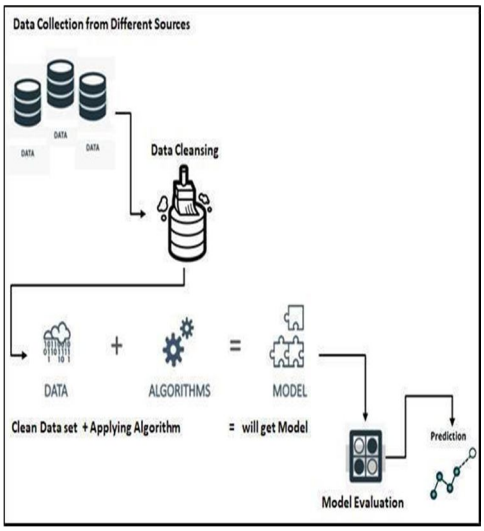


Figure 1 System Architecture

A. Architecture

The methodology encompasses data acquisition, preprocessing, model development, evaluation, and prediction to ensure accurate fraud detection. The key components of this approach include:

1) Data Collection

This includes transaction records, user activity logs, and other relevant information for fraud detection. Collecting diverse and comprehensive data strengthens the model's capability to detect potential fraud patterns effectively.

2) Data Cleaning

At this stage, the gathered data is processed for analysis by eliminating inconsistencies, errors, and irrelevant entries. Methods such as handling missing values, identifying and removing outliers, and normalizing data are utilized. This ensures that the dataset remains clean, well-structured, and suitable for effective modeling

3) Algorithm Application

This involves selecting the most appropriate algorithm, such as decision trees, neural networks, or clustering techniques, based on the project's objectives. These algorithms analyze the data to identify patterns linked to fraudulent activities.

4) Model Building

A predictive model is created utilizing the processed dataset and the selected algorithm. It evaluates patterns and correlations in the data to effectively detect possible fraudulent activities.

5) Prediction

The evaluated model is deployed in real-time or batch mode to flag suspicious activities or transactions. These predictions.

B. Workflow

The flowchart illustrates the workflow of an e-commerce fraud detection system, detailing the steps a user takes to interact with it. The process begins with the login step, where users enter their credentials. If the credentials are incorrect, access is denied, and they are prompted to retry.

The next step enables users to review fraud predictions in e-commerce transactions, determining whether a transaction is legitimate or fraudulent. Additionally, users can download trained datasets for further analysis or model refinement. The system also offers a feature to view all remote users, which may serve administrative or security purposes. Finally, the workflow concludes when the user logs out.

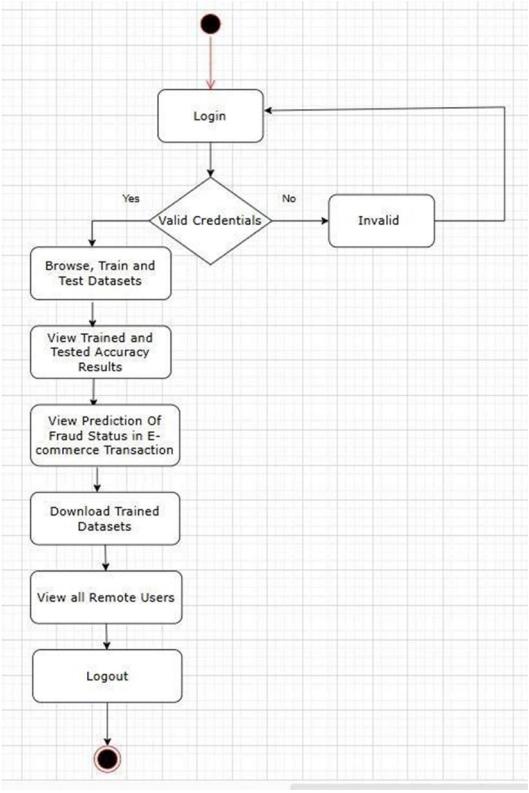


Figure 2 Data flow diagram

C. Sequence Models

Sequence models illustrate the order of object interactions and are depicted using UML sequence diagrams or collaboration diagrams. These dynamic models define the interaction flow for different operational modes. When documenting a design, it is crucial to develop a sequence model for each key interaction. If a use case model is created, a corresponding sequence model should be developed for every identified use case. The sequence diagram for the fraud detection system illustrates the step-by-step interaction of different components to detect and flag fraudulent activities. The process starts when a user or system submits transactional or behavioral data.

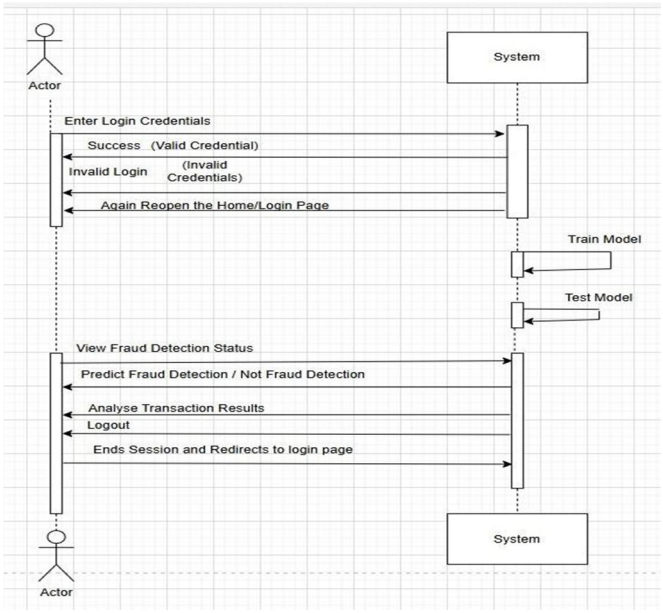


Figure 3 Sequence Models

D. UML(Unified Modeling Language)

In the Unified Modeling Language (UML), a use case diagram provides a high-level overview of a system's users, also known as actors, and their interactions with the system.

In certain scenarios, one use case (referred to as the extension) can extend another use case. This relationship signifies that the extended use case may incorporate the behavior of the extension under specific conditions. It is represented by a dashed arrow pointing from the extension use case to the extended use case, labeled "«extend»".

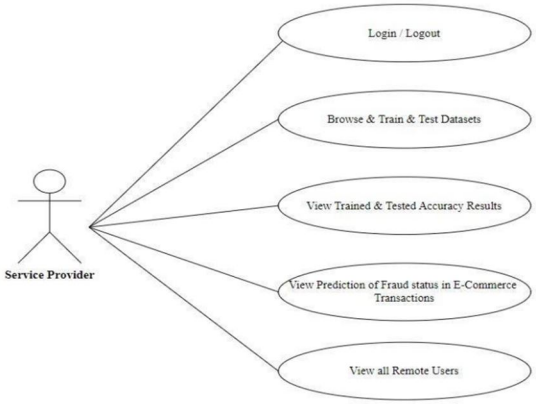


Figure 3 UML (Unified Modeling Language)

IV. RESULTS AND DISCUSSION

This research focused on evaluating e-commerce fraud detection using a dataset sourced from the Kaggle machine learning repository. The dataset comprised multiple attributes, all represented as floating-point values, along with a decision class indicating whether a transaction was fraudulent or legitimate. These metrics were analyzed to assess the model's capability in detecting fraudulent activities while minimizing errors in classification.

The study emphasized the significance of choosing an appropriate classifier for fraud detection and suggested that further enhancements could be achieved through experimentation with alternative algorithms or feature engineering techniques to improve model performance

V. FUTURE SCOPE

1) Integration with Blockchain: Enhance transaction security and transparency using blockchain technology.
2) AI-Powered Fraud Prediction: Incorporate advanced AI models for even better accuracy and adaptability.
3) Support for Diverse Payment Systems: Extend compatibility to detect fraud in emerging payment platforms like cryptocurrency.
4) Global Scalability: Adapt the system for international e-commerce markets with varying regulations and practices.
5) Real-Time Fraud Detection Develop real-time monitoring and alert mechanisms to instantly identify and prevent fraudulent transactions.
6) Explainable AI (XAI) for Transparency: Incorporate explainable AI methods to provide clear justifications for fraud detection decisions, enhancing user trust.
7) Multi-Factor Authentication (MFA) Integration: Strengthen security by implementing additional authentication steps for high-risk or suspicious transactions.
8) Graph-Based Fraud Detection: Apply graph analytics to uncover fraud networks and connections between suspicious entities.

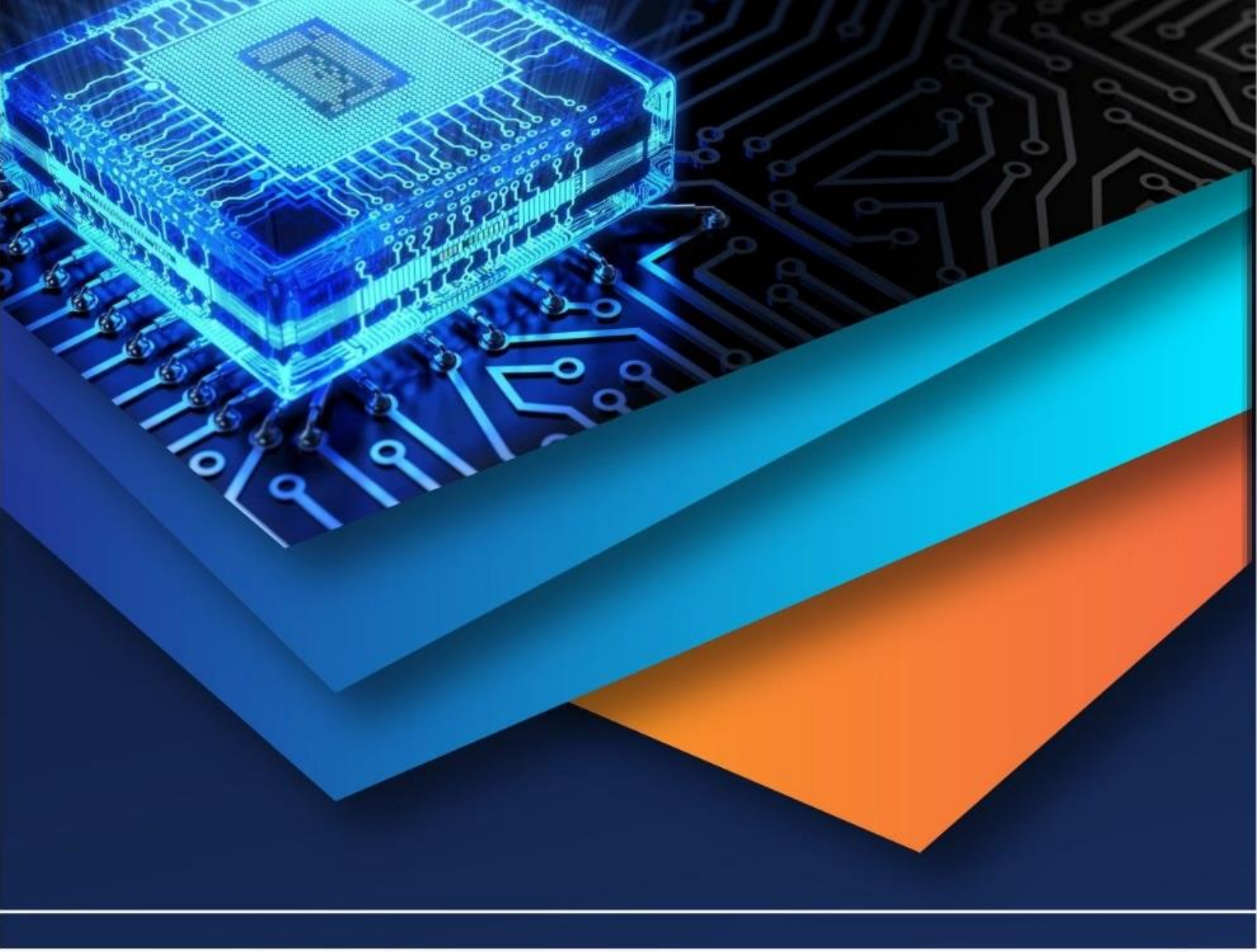
VI. ACKNOWLEDGMENT

We extend our sincere gratitude to everyone who contributed to the successful completion of this project, *A Multi-Perspective Fraud Detection Method for Multi-Participant E-Commerce Transactions*.

We are also deeply grateful to the Head of the Department for their encouragement and valuable suggestions, which played a crucial role in shaping our work.

REFERENCES

[1] R. A. Kuscu, Y. Cicekcisoy, and U. Bozoklu, Electronic Payment Systems in Electronic Commerce. Turkey: IGI Global, 2020, pp. 114–139
[2] P. Rao et al., "The e-commerce supply chain and environmental sustainability: An empirical investigation on the online retail sector." Cogent. Bus. Manag. 1938377, 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY