

Multi-Perspective Fraud Detection Method For Multi-Participant E-Commerce Transactions Using Machine Learning

Bhagyashree ¹, Dr. Shravankumar Arjunagi ²

¹Student, Department of Artificial Intelligence and Data Science, Sharnbasva University, Kalaburagi, India.

²Associate Professor, Department of Artificial Intelligence and Data Science, Sharnbasva University, Kalaburagi, India.

ABSTRACT

The growth of online shopping platforms has significantly increased the number of digital transactions, which has also led to a rise in fraudulent activities. Detecting such fraud efficiently has become an essential requirement for maintaining secure and trustworthy e-commerce systems. This project presents a machine learning-based approach for identifying fraudulent transactions by analyzing historical transaction data and user behavior patterns. The proposed system follows a structured workflow that includes data cleaning, feature selection, handling of imbalanced data, and model training. Supervised learning algorithms such as Logistic Regression, Random Forest, and XGBoost are applied to classify transactions as genuine or fraudulent. The performance of these models is evaluated using multiple metrics to ensure accurate and reliable detection. The results demonstrate that machine learning techniques can effectively capture complex fraud patterns and outperform traditional rule-based systems. This framework can be integrated into real-time e-commerce platforms to enhance transaction security and reduce financial risk.

Keywords: E-commerce, Fraud, Machine Learning.

I. INTRODUCTION

E-commerce has changed the way people buy and sell goods by enabling fast and convenient online transactions. With the increasing reliance on digital payment systems, online platforms are now handling millions of transactions every day. While this growth has improved customer experience and business reach, it has also created opportunities for fraudulent activities. Fraudsters exploit weaknesses in online systems by using stolen identities, fake accounts, and unauthorized payment methods, leading to financial losses and reduced customer trust. Traditional fraud detection methods are mainly based on fixed rules and manual verification. These techniques can identify known fraud patterns but struggle to detect new and evolving fraud strategies. As transaction volumes increase, manual monitoring becomes inefficient and prone to errors. Static rules also result in higher false alerts, which negatively affect genuine users. Machine learning provides an intelligent and data-driven solution to this problem. By learning from historical transaction data, machine learning models can automatically identify abnormal behavior and adapt to changing fraud patterns. This project focuses on building a supervised machine learning-based fraud detection system for e-commerce platforms. The system analyzes transaction and user behavior data to accurately identify fraudulent activities while supporting scalable and real-time transaction monitoring. In recent years, the increasing use of digital payment methods such as credit cards, debit cards, and online wallets has made e-commerce platforms more convenient but also more vulnerable to fraudulent activities. Fraudsters continuously experiment with new techniques, including automated scripts, account takeovers, and misuse of personal information, to bypass traditional security mechanisms. As a result, fraud patterns are no longer simple or predictable, making detection more challenging for conventional systems.

One of the major difficulties in fraud detection is the large volume of data generated by e-commerce platforms on a daily basis. Each transaction produces multiple data points related to customer behavior, transaction timing, device usage, and geographical location. Manually analyzing this information is not feasible, and rule-based systems are unable to capture the hidden relationships within such complex datasets. This creates a need for intelligent systems that can process large-scale data efficiently and learn meaningful patterns without constant human intervention.

1.1.Problem Statement

The rapid expansion of e-commerce platforms has resulted in a significant increase in online transactions, making these systems vulnerable to fraudulent activities. Incidents such as unauthorized payments, fake user accounts, and misuse of customer identities pose serious threats to transaction security. Existing fraud detection systems largely depend on rule-based logic and manual checks, which are not effective against continuously evolving fraud techniques. Another major challenge is the imbalance in transaction data, where fraudulent cases occur far less frequently than genuine transactions. This imbalance makes accurate detection difficult and often leads to missed fraud cases or false alerts. Therefore, there is a need for an automated and intelligent fraud detection system that can analyze large volumes of transaction data, learn hidden fraud patterns, and provide accurate real-time predictions. Such a system should enhance security, reduce financial losses, and improve trust in e-commerce platforms.

1.2.Objectives

- Examine transaction records and user behavior to identify patterns that distinguish fraudulent activities from legitimate purchases.
- Establish a reliable data preparation workflow that addresses inconsistencies, missing values, and the imbalance between genuine and fraudulent transactions.
- Analyze the influence of behavioral, temporal, and transactional attributes on fraud occurrence within online commerce platforms.
- Implement learning-based models capable of recognizing complex and evolving fraud patterns without relying on fixed rule sets.
- Compare multiple classification approaches to understand their strengths and limitations under real-world transaction conditions.
- Support early identification of high-risk transactions to reduce financial losses and operational overhead for e-commerce platforms.

II. LITERATURE REVIEW

1. Adaptive Behavior-Based Machine Learning for Detecting Fraud in Multi-User E-Commerce Transactions.

Author(s): N. Swetha, CH Sri Lakshmi Prasanna

Published in: International Journal of Engineering Research and Science & Technology, 2025, Vol. 21, Issue 2

Summary: This study introduces a behavior-focused framework to identify fraudulent activities in e-commerce platforms where multiple participants interact during transactions. Unlike traditional methods that rely solely on transaction amounts or user details, this approach analyzes the sequence of actions within a transaction to uncover abnormal patterns. By applying machine learning algorithms to event-level data extracted from transaction logs, the system adapts to evolving fraud strategies. Results show that this adaptive, behavior-based model significantly outperforms conventional static detection systems in identifying complex fraud scenarios.

2. Enhancing Online Payment Security Using Machine Learning and Hybrid Detection Models.

Author(s): V. Pavan Kumar et al.

Published in: Journal of Survey in Fisheries Sciences, 2024, Vol. 11, Issue 4

Summary: This research focuses on improving fraud detection in online payment systems by leveraging machine learning and deep learning techniques. The study uses historical transaction datasets to train multiple predictive models capable of distinguishing legitimate payments from fraudulent ones. Special attention is given to addressing data imbalance through resampling methods to improve detection accuracy. Experimental findings indicate that hybrid and ensemble-based models offer higher reliability and precision compared to single-model approaches, making them highly effective for real-world online payment fraud prevention.

3. Supervised Machine Learning for Fraud Identification in E-Commerce Platforms.

Author(s): Nikita Verma, Kshiti Uboveja, Manoj Kumar Singh

Published in: International Journal of Futuristic Innovation in Engineering, Science and Technology, 2023

Summary: This work investigates the application of supervised machine learning methods to detect fraudulent activities in e-commerce transactions. The research emphasizes preprocessing transaction data and selecting critical features that influence fraud prediction. Several classification algorithms are evaluated to determine

their effectiveness in managing large-scale transaction datasets. The study concludes that machine learning-based systems provide superior adaptability and accuracy compared to traditional rule-based methods, enabling more efficient detection of fraudulent behavior.

4. **Comprehensive Analysis of Machine Learning Techniques for Detecting Fraud in E-Commerce Platforms.**

Author(s): Abed Mutemi & Fernando Bação

Published in: The review article was published in Big Data Mining and Analytics in 2024 under Volume 7, Issue 2.

Summary: This systematic review examines a wide range of research studies related to fraud detection in e-commerce using machine learning techniques. The authors analyze existing approaches based on learning methods, feature engineering strategies, and evaluation metrics. The review identifies commonly used algorithms and emerging trends such as deep learning and hybrid detection frameworks. It also highlights key research challenges, including limited labeled data and difficulties in deploying models in real-world environments.

5. **A detailed examination of methods and strategies for detecting and preventing fraudulent transactions in e-commerce platforms.**

Author(s): Vinicius Peixoto Rodrigues et al.

Published in: This literature review appeared in the journal Electronic Commerce Research and Applications during its 2022 publication period.

Summary: This paper provides an extensive review of fraud detection and prevention mechanisms used in e-commerce systems. It discusses various techniques ranging from statistical analysis to advanced machine learning-based anomaly detection. The review emphasizes the importance of real-time fraud monitoring and integrated prevention strategies. The study also identifies research gaps related to system scalability and adaptability, highlighting the need for intelligent systems that can respond to evolving fraud patterns.

6. **Unsupervised Learning-Based Identification of Fraudulent E-Commerce Transactions Using Contrastive Models.**

Author(s): Xuan Li, Yuting Peng, Xiaoxuan Sun, et al.

Published on: The study was released in 2025 as a publicly accessible preprint through the arXiv research repository.

Summary: The study presents an unsupervised fraud detection approach that does not rely on labeled transaction data. By using contrastive learning techniques, the model learns meaningful representations of normal transaction behavior. Fraudulent activities are identified as deviations from learned patterns. The results show that unsupervised learning methods can effectively detect anomalies and are particularly useful in situations where labeled fraud data is scarce or incomplete.

7. **Application of Machine Learning for Identifying Fraud in Online E-Commerce Transactions.**

Author(s): Murat Golyeri, Sedat Celik, Fatma Bozyigit, Deniz Kiling

Published in: The findings were presented in a peer-reviewed research publication released in 2023.

Summary: This research evaluates the performance of multiple supervised machine learning models for detecting fraud in e-commerce transaction data. The study focuses on feature extraction from transaction logs and analyzes how different features impact classification accuracy. The experimental results demonstrate that ensemble and boosting-based models provide better detection performance than simpler classifiers, confirming the importance of feature-driven learning in fraud detection systems.

8. **An Overview of Fraud Detection Techniques Applied in E-Commerce Systems.**

Author(s): Priya J Rana, Jwalant Baria

Published in: This survey was published in the International Journal of Computer Applications in 2015 as part of Volume 113 (Issue 14).

Summary: This survey offers an overview of fraud detection techniques used in e-commerce platforms, covering both traditional methods and early machine learning-based approaches. It discusses classification, anomaly detection, and rule-based systems while analyzing their strengths and limitations. The paper serves as a foundational reference for understanding the evolution of fraud detection methodologies and provides context for modern machine learning-based solutions.

9. **Leveraging Random Forest Algorithms for Identifying Fraud in Online E-Commerce Activities.**

Author(s): Geetha Prathiba, Ch Shravani, A Ashritha, E Lavanya

Published in: The research was published in the International Journal of Engineering in Computer Science in the year 2024.

Summary: This study focuses on the Random Forest algorithms of detecting fraud in complex e-commerce environments involving multiple participants. By combining transaction behavior analysis with ensemble learning, the approach captures hidden fraud patterns more effectively. The results indicate that Random Forest models improve detection accuracy and reduce false classifications, making them suitable for handling distributed and large-scale transaction systems.

10. **Artificial Intelligence-Based Anomaly Detection Techniques for E-Commerce Services.**

Author(s): P. M. Mah, I. Skalna, T. Pelech – Pilichowski

Published in: This article appeared in the Journal of Theoretical and Applied Electronic Commerce Research during the 2025 publication year.

Summary: This research proposes an AI-driven framework for identifying anomalies and fraudulent behavior in e-commerce services. The approach integrates machine learning and anomaly detection techniques to analyze transaction behavior and service performance indicators. The study emphasizes interpretability, scalability, and real-time processing, demonstrating that intelligent detection systems can enhance transaction security while maintaining operational efficiency.

III. SYSTEM ANALYSIS

3.1 Existing System

In traditional e-commerce platforms, fraud detection is mainly carried out using rule-based mechanisms or manual inspection of transactions. These systems typically depend on predefined conditions such as unusually high transaction amounts, repeated login attempts, or previously identified suspicious accounts. Although these approaches are straightforward to implement, they suffer from several critical drawbacks that limit their effectiveness in modern online environments. The major limitations of the existing system are as follows:

- **Limited adaptability:** This architecture may look static inside nature, fail to adjust to continuously changing and sophisticated fraud techniques used by attackers.
- **High Rate of Misclassifications :** Legitimate transactions are often incorrectly flagged as fraudulent, while certain fraudulent activities may go undetected due to rigid rule definitions.
- **Time-consuming process:** Manual verification and cross-checking of transactions require significant time and effort, making the system inefficient for handling large volumes of online transactions.
- **Inability to learn from historical data:** Traditional systems do not automatically improve based on past transaction behavior and lack the capability to update detection logic using historical transaction patterns.

3.2 Proposed System

This adopts an intelligent learning-driven approach to detect fraudulent activity within e-commerce platforms. Instead of relying on static rule definitions, the system learns from historical activity data to recognize suspicious behavior patterns. The major functional elements of the system are outlined as follows:

- **Transaction Data Preparation :** The system begins by refining raw transaction records to improve data reliability. This includes handling incomplete entries, removing duplicate records.
- **Feature Identification and Refinement :** Important transaction and user behavior attributes such as purchase amount, transaction timing, location patterns, device usage, and customer activity trends are examined. Features that strongly contribute to fraud identification are retained, while less informative attributes are removed to improve model efficiency.
- **Learning-Based Fraud Detection :** Instead of depending on predefined thresholds, the system employs supervised machine learning algorithms that learn fraud patterns from labeled transaction data.
- **Data Imbalance Control :** Since fraudulent cases occur less frequently, specialized balancing techniques are incorporated during training to prevent bias toward normal activities and to strengthen fraud recognition capability.
- **Prediction Quality Analysis :** Model outputs are examined using multiple reliability indicators to ensure accurate fraud identification while limiting incorrect alerts for genuine users.
- **Scalability and Real-Time Capability :** The proposed framework is designed to support large-scale transaction processing and can be integrated into live e-commerce platforms. This allows continuous monitoring of transactions and enables early detection of suspicious activities.

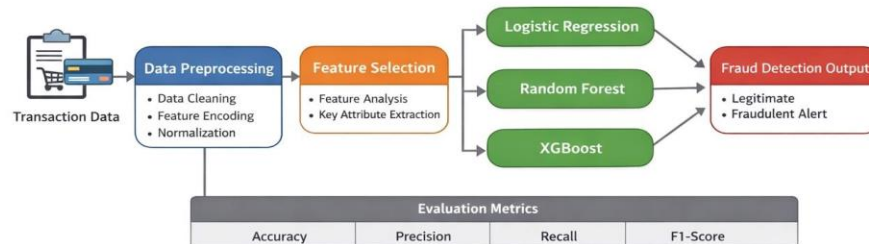


FIGURE 1 : SYSTEM FLOW DIAGRAM OF E-COMMERCE FRAUD DETECTION

IV. METHODOLOGY

The methodology of this project focuses on identifying fraudulent e-commerce transactions using machine learning techniques. Historical transaction data is cleaned and prepared to remove inconsistencies and handle class imbalance. Relevant transaction and behavioral features are analyzed to capture meaningful fraud patterns. Supervised learning models are trained to classify transactions as legitimate or fraudulent based on learned behavior. Model performance is evaluated to ensure reliable and scalable fraud detection.

4.1 Data Collection

The project utilizes a dataset consisting of historical e-commerce transaction records collected from online transaction sources. Each transaction entry contains attributes such as transaction identification details, user-related information, transaction value, time of purchase, geographical indicators, and other behavioral or categorical features. The dataset includes both genuine and fraudulent transactions, making it suitable for supervised learning phase.

4.2 Data Preprocessing

Transaction datasets often contain incomplete, inconsistent, and non-numeric values that are not directly suitable for machine learning algorithms. To address these issues, the following preprocessing steps are performed:

- **Data Cleaning and Validation** : Raw transaction records are examined to identify missing, duplicate, or inconsistent entries. Incomplete records are either corrected or removed to ensure the reliability of data used for fraud detection.
- **Transformation of Categorical Attributes** : Transaction attributes that contain non-numeric information, such as device type or browser details, are transformed into numerical formats. This enables machine learning models to process behavioral and transactional patterns effectively.
- **Numerical Feature Adjustment** : Continuous variables such as transaction amount and time-related values are adjusted to maintain comparable ranges.
- **Handling Class Imbalance** : Balancing techniques are applied during training to ensure the model learns fraud patterns without bias toward normal transactions.
- **Final Data Consistency Check** : After preprocessing, the dataset is reviewed to confirm that all features are properly formatted, balanced, and suitable for our model.

4.3 Feature Selection and Analysis

Feature selection focuses on identifying transaction attributes that have a significant influence on fraud detection. Selecting relevant features improves prediction accuracy while reducing computational overhead. The following methods are applied:

- Correlation-Based Analysis: Features with strong relationships to fraud outcomes are identified for further analysis.
- Iterative Feature Reduction: Less informative features are gradually removed to retain only the most impactful predictors.
- Domain-Based Selection: Transaction characteristics are selected based on practical understanding of e-commerce fraud behavior and purchasing patterns.

4.4 Machine Learning Model Implementation

To classify transactions as legitimate or fraudulent, multiple supervised learning algorithms are implemented:

- Reference Classifier: Logistic Regression is applied as a baseline learner to provide an initial understanding of fraud-related patterns and serve as a comparison point for advanced models.
- Ensemble-Based Classifier: Random Forest is used to improve detection reliability by combining multiple decision paths and capturing complex behavior variations within transaction data.
- Boosted Classification Model: XGBoost is employed to strengthen fraud identification by focusing on high-risk cases and improving prediction quality under imbalanced data conditions.
- Learning Phase Execution: All classifiers undergo supervised learning using labeled activity data after preprocessing and feature refinement to ensure stable and consistent learning behavior.
- Model Outcome Comparison: Prediction outputs from all models are examined under the same evaluation conditions to determine the most dependable approach for e-commerce fraud identification.

4.5 Performance Assessment of Fraud Classification Models

The performance of each machine learning model is assessed using standard evaluation metrics to ensure reliable fraud detection:

- Overall Prediction Accuracy: This measure reflects how well the model classifies transactions in general. However, it is interpreted carefully since fraud cases form only a small portion of the dataset.
- Fraud Prediction Precision: It indicates the correctness of fraud alerts generated by the model. Higher precision helps reduce unnecessary blocking of legitimate customer transactions.
- Detection Recall: This represents the model's ability to successfully identify fraudulent transactions. A strong recall value ensures that fewer fraud cases remain undetected.
- Balanced Performance Score: A combined performance score is used to evaluate how well the model balances fraud detection accuracy and false alert reduction, especially under imbalanced data conditions.
- Error Pattern Analysis: Prediction results are further examined to understand misclassification behavior, including wrongly flagged genuine transactions and missed fraud cases. This analysis supports model refinement and performance improvement.

4.6 System Deployment Considerations

The methodology also considers fraud detection system in e-commerce platforms:

- Real-Time Monitoring: Continuous analysis of incoming transactions to detect suspicious behavior instantly.
- Scalability: Capability to process large transaction volumes without affecting system performance.
- Periodic Model Retraining: Updating the model with recent transaction data to adapt to evolving fraud techniques.
- Alert Mechanism: Generating notifications or alerts whenever fraudulent transactions are detected for immediate action.

V. SYSTEM ARCHITECTURE

5.1 Structural Description of the Fraud Detection Framework

This E-commerce Fraud Detection platform is designed to efficiently identify suspicious transactions and prevent fraud using advanced machine learning techniques. The architecture is modular, allowing each component to perform a specific role while working together seamlessly. At the core, the system handles transaction data by first performing data preprocessing and feature engineering to extract meaningful patterns. These processed data points are then fed into various ML models. The architecture also includes evaluation and monitoring mechanisms to check the capability and ensure accurate predictions. Additionally, a user interface layer provides interaction capabilities for administrators and analysts to review flagged transactions and insights generated by the system.

5.2 System components

The system's operation relies on the core components outlined here:

User Interface Module: This module allows users or administrators to provide transaction input and view fraud detection results. It acts as the interaction layer between the system and end users.

Transaction Data Module: This component stores historical and real-time e-commerce transaction data. The data includes transaction amount, time, customer behavior attributes, and transaction identifiers used for fraud analysis.

Data Preprocessing Module: This module is responsible for making raw transaction content, it should effectively taken by machine learning models. It examines incoming transaction records to identify missing values, duplicate entries, and inconsistent information. Categorical attributes such as browser type or device details are converted into numerical representations to support computational analysis. Numerical features are adjusted to maintain comparable value ranges, ensuring balanced learning. The module also addresses class imbalance by applying appropriate techniques so that fraudulent transactions receive sufficient importance during model training.

Feature Selection Module: The feature selection module identifies the most relevant transaction attributes that contribute to fraud detection. Selecting optimal features improves model accuracy and reduces computational complexity.

Machine Learning Model Module: This module performs the core task of learning fraud patterns from processed transaction data. It utilizes supervised learning algorithms that are trained using labeled examples of legitimate and fraudulent transactions.

- Logistic Regression is used to establish baseline performance, while Random Forest and XGBoost are applied to capture complex and non-linear fraud behaviors. Each model learns transaction characteristics based on historical behavior rather than fixed rules.
- The models analyze transaction patterns to determine whether an activity is potentially fraudulent.

Model Evaluation Module: This module assesses the ability of trained models by analyzing prediction results. Multiple evaluation measures are used to ensure balanced fraud detection performance. Accuracy provides an overall view of correct predictions, while precision and recall focus on fraud-specific detection quality.

- The F1-score is used to balance precision and recall, particularly under imbalanced data conditions. A confusion matrix is also examined to understand misclassification patterns and support model refinement.

Fraud Classification Output Module: The fraud classification output module generates the final decision based on model predictions. The operation is categorized according to learned patterns. Legitimate transactions are approved for further processing, while suspicious transactions are flagged for review or immediate action. The output can be displayed to administrators or integrated with monitoring systems to trigger alerts. This module ensures timely response to fraudulent activities and supports secure transaction handling.

5.3. Architecture flow

1. Transaction-related activity data is obtained from stored datasets as well as real-time e-commerce operations for security analysis.
2. Incoming data is cleaned and validated to remove incomplete records, repeated entries, and irregular values before further processing.
3. Raw attributes are reorganized and encoded into a uniform data format that enables efficient computational analysis.
4. Behavioral and transactional indicators that contribute most to fraud identification are isolated for further processing.
5. The refined dataset is supplied to learning modules that study historical behavior to recognize fraud-related patterns.
6. Trained supervised classifiers examine activity behavior and assign a risk score indicating potential fraud.
7. Prediction outputs are examined to determine the consistency and dependability of fraud identification results.
8. Each activity is then categorized as normal or suspicious based on the model's decision logic.
9. Normal activities proceed without interruption, while suspicious cases trigger alerts for manual review or preventive action.

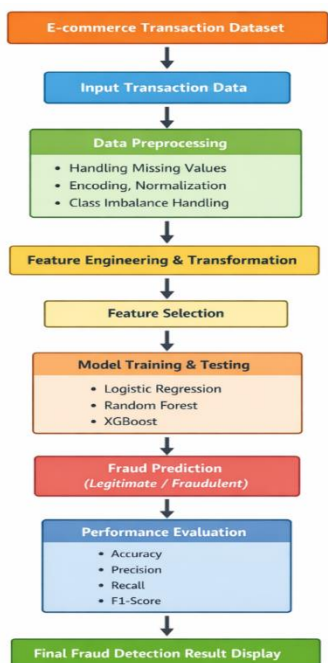


FIGURE 2: STRUCTURAL PROCESS FLOW REPRESENTATION

VI. RESULT

E-commerce Fraud Detection
Prediction: Legal

Customer Details

Source: Browser: Sex: Age:

Transaction Details

Country Name: No of Device Occur: Signup Month: Signup Day:

Signup Day Name: Purchase Month: Purchase Day: Purchase Day Name:

Purchase Over Time:

Predict

© 2024 E-commerce Fraud Detection App | Developed by Md Emon Hasan

6.1. Customer Details

1. Source : This field represents the medium through which the customer accessed the e-commerce platform, such as direct access, referral links, or advertisements. Source information helps the system understand entry patterns and identify access points that may be associated with higher fraud risk.
2. Browser : The browser field indicates the web browser used by the customer to perform the transaction. This attribute assists in identifying unusual browser usage patterns that may indicate automated or suspicious activity.
3. Age : Age represents the customer's age group or numerical age value. Age-related transaction behavior helps distinguish between normal purchasing habits and irregular activity patterns.

6.2. Transaction Details

1. Country name : This field specifies the country from which the transaction is initiated. Location information plays a crucial role in identifying transactions originating from unexpected or high-risk regions.
2. Number of device occurrences : This attribute records how many devices are associated with a single user account. Frequent changes in devices can indicate account compromise or fraudulent access.
3. Signup day : This field indicates the day of the week on which the user signed up. Certain signup patterns can be linked with suspicious account creation behavior.
4. Signup day name : This attribute captures the textual representation of the signup day. It supports temporal pattern analysis related to user registration behavior.
5. Purchase month : Purchase month specifies when the transaction occurred. Seasonal and monthly trends are useful in identifying abnormal purchasing behavior.
6. Purchase day : This field indicates the day of the month when the transaction was made. Sudden spikes in purchases on unusual days may indicate fraudulent attempts.
7. Purchase over time : This field captures the time difference or duration between signup and purchase or between multiple purchases. Rapid purchases within a short time span are commonly associated with fraudulent transactions.

6.3. Sources of these details.

- Customer information is collected during user registration and login activities.
- Transaction-related attributes are generated during purchase and payment processing.
- Device and browser data are obtained from session-level tracking mechanisms.
- Temporal features are derived from system timestamp associated with user actions.

VII. CONCLUSION

This work demonstrates the practical use of supervised machine learning techniques for detecting fraudulent activity in e-commerce environments. By examining historical activity records and user behavior patterns, the proposed system is capable of distinguishing between genuine and suspicious activities with improved consistency. The structured approach to data preparation and feature refinement enables the learning models to capture meaningful fraud indicators rather than relying on predefined rules. Experimental observations show that ensemble-based classifiers, particularly Random Forest and XGBoost, are effective in recognizing complex and evolving fraud patterns, even when fraudulent instances are limited in number. The system architecture is designed to be modular and scalable, allowing seamless integration into existing e-commerce platforms for continuous monitoring and early risk identification. Overall, the proposed framework supports enhanced transaction security, reduces potential financial exposure, and contributes to maintaining customer trust in online commerce systems. Future work can focus on incorporating adaptive learning mechanisms and advanced deep learning models to further strengthen fraud detection capabilities in real-time operational environments.

REFERENCES

1. A 2023 publication by A. Dal Pozzolo, G. Bontempi, and M. Snoeck discusses machine learning-based approaches for detecting fraud within online payment transactions, featured in Expert Systems with Applications.
2. Carcillo, F., Dal Pozzolo, A., Bontempi, G., & Snoeck, M. (2023). Supervised learning methods for financial fraud detection: A comparative study. IEEE Access, 11, 84215–84228.
3. Aggarwal, C. C. (2023). Machine Learning for Fraud Detection. Springer, Cham.

4. Chen, T., & Guestrin, C. (2024). XGBoost: A scalable tree boosting system for structured data analysis. *ACM Computing Surveys*, 56(2), 1–36.
5. Breiman, L. (2023). Random forest classifiers for large-scale data analysis. *Machine Learning*, 112(4), 1015–1036.
6. Pedregosa, F., Varoquaux, G., Gramfort, A., et al. (2024). Scikit-learn: Tools for machine learning in Python. *Journal of Machine Learning Research*, 25, 1–18.
7. Bahnsen, A. C., Aouada, D., & Ottersten, B. (2023). Feature engineering and imbalance handling in fraud detection systems. *Knowledge-Based Systems*, 263, 110287.
8. Kaggle. (2024). E-commerce fraud detection datasets for machine learning research.
<https://www.kaggle.com>
9. Goodfellow, I., Bengio, Y., & Courville, A. (2023). *Applied Machine Learning for Structured Data*. MIT Press.
10. Hasan, Md. E. (2024). E-commerce Fraud Detection using Machine Learning. GitHub Repository.
<https://github.com/Md-Emon-Hasan/ML-Project-E-commerce-Fraud-Detection>