

AI Revolutionizing E-commerce governance for Fraud Detection

S. Surendar Reddy^{1*}, V. Aishwarya², P. G. N. K. Sai Pavan², Vishakha Roy², A. Gouthami²

¹Assistant Professor, ²UG Student, ^{1,2}Department of Computer Science and Engineering-Data Science,

^{1,2}Malla Reddy Engineering College and Management Sciences, Kistapur, Medchal, 501401, Telangana, India

*Corresponding author: surenderreddy@mrem.ac.in

Received: 02.03.2025

Revised: 15.04.2025

Accepted: 25.05.2025

ABSTRACT

E-commerce in India has experienced rapid growth, with online shoppers projected to reach 175 million, driven by the expansion of digital payments and mobile transactions. Alongside this growth, fraudulent activities such as phishing and card testing have increased significantly, with ad fraud losses reaching USD 1.63 billion in 2018, of which e-commerce accounted for 51%. Traditional fraud detection systems rely on manual, rule-based analysis by human experts who inspect transaction patterns, billing details, and IP locations. These approaches are time-consuming, error-prone, and incapable of scaling to high transaction volumes, often failing to detect complex and evolving fraud patterns. To address these challenges, this research proposes an automated e-commerce fraud detection framework based on machine learning techniques. The system classifies transactions as fraudulent or non-fraudulent using multiple models, including Support Vector Machine, Logistic Regression, Neural Networks, and Gradient Boosting Classifier. While SVM and Logistic Regression provide baseline separation and interpretability, Neural Networks capture complex patterns, and Gradient Boosting excels in handling non-linear relationships and class imbalance using SMOTE. The proposed approach improves detection accuracy, scalability, and reliability, offering an effective solution for real-time e-commerce fraud prevention.

Keywords: E-commerce Fraud Detection, Machine Learning, Gradient Boosting Classifier, Neural Networks, SMOTE, Online Transactions, Cybersecurity

1. INTRODUCTION

The e-commerce sector in India has witnessed unprecedented growth, with the market size projected to reach \$200 billion by 2026, driven by 220 million online shoppers as of 2023. This surge is fueled by widespread smartphone penetration (over 800 million users) and digital payment systems like UPI, which processed 131 billion transactions worth \$1.8 trillion in 2023. However, this expansion has been accompanied by a rise in fraudulent activities, with e-commerce fraud losses in India estimated at \$3.5 billion annually, accounting for 51% of global ad fraud. Common fraud types include account takeovers, phishing, and card-not-present scams, exploiting vulnerabilities in online payment systems. The dataset of 23,634 transactions, with 1,222 (5.17%) fraudulent cases, reflects this challenge, highlighting the need for robust detection mechanisms to safeguard financial transactions.

Fraud detection systems aim to identify suspicious patterns in transaction data, such as mismatched billing/shipping addresses, unusual transaction amounts, or rapid account activity. In India, 65% of e-commerce merchants report fraud attempts, with 15% of transactions flagged as suspicious, straining manual review processes. The 1:18.3 fraud-to-legitimate ratio in dataset underscores the class imbalance problem, where fraudulent transactions are rare but impactful. Traditional rule-based systems,

like address verification or CVV checks, are increasingly inadequate due to their inability to adapt to evolving fraud tactics.

The economic and societal impacts of e-commerce fraud are significant, eroding consumer trust and increasing operational costs. In India, 30% of online shoppers have experienced fraud-related issues, leading to cart abandonment and reduced platform loyalty. Globally, fraud losses reached \$48 billion in 2023, with e-commerce platforms bearing a disproportionate share. Regulatory frameworks, such as the IT Act (2000) and RBI's two-factor authentication mandates, aim to mitigate risks, but enforcement gaps persist.

2. LITERATURE SURVEY

Hasan et al. [1] proposed digital transactions pose a significant challenge to enterprises and customers for having secure business and financial transactions. The drawbacks were susceptibility to compromise and challenges in identifying fraudulent payments. To enhance the ease and convenience of the customers and business enterprises, e-commerce and financial service providers are deploying sophisticated tools that employ data analytics, AI and machine learning techniques. the average accuracy and coverage are 89.41% and 86.95%.

Khurana et al. [2] analyzed huge datasets, found anomalies, and flagged possible fraud activities, thus enabling systems to make autonomous decisions during the process of payment. Real-time analysis by AI reduces latency in fraud detection. The drawbacks were high computational cost, false positives and data privacy concerns. They addressed the integration of both supervised and unsupervised learning techniques for fraud detection in e-commerce payment systems, with a contributing role of AI in relation to data privacy. AI-driven fraud detection models can achieve accuracy rates between 85% and 95%.

Karunaratne et al. [3] explored the synergistic application of machine learning and big data to enhance e-commerce cybersecurity. The rapid proliferation of e-commerce platforms has made them prime targets for cybercriminals employing increasingly sophisticated tactics. To safeguard sensitive data, ensure transactional integrity, and preserve consumer trust, e-commerce platforms must adopt advanced technologies for anomaly detection and proactive cybersecurity defense. Random forest models achieve 94.1% accuracy. Support vector machines have an accuracy rate of 92.3%,

Zhang et al. [4] proposed a competitive graph neural networks (CGNN)-based fraud detection system (eFraudCom) to detect fraud behaviors at one of the largest e-commerce platforms, "Taobao". In the eFraudCom system, the competitive graph neural networks (CGNN) as the core part of eFraudCom can classify behaviors of users directly by modeling the distributions of normal and fraud behaviors separately. some normal behaviors will be utilized as weak supervision information to guide the CGNN to build the profile for normal behaviors that are more stable than fraud behaviors. The accuracy of the CGNN-based fraud detection system varies depending on the dataset and fraud patterns.

Rane et al. [5] investigates the comprehensive acceptance of artificial intelligence (AI) in business management, finance, and e-commerce, focusing on the factors driving its adoption, the obstacles encountered, and strategies for enhancing integration. challenges such as data privacy concerns, high implementation costs, and resistance to change impede widespread adoption. Additionally, ethical considerations and the need for regulatory compliance add layers of complexity. AI-driven systems improve efficiency and decision-making accuracy by approximately 85% to 95%.

Immadisetty et al [6] the authors reviewed some streaming data-driven real-time fraudulent detection techniques with a view to enhancing financial transaction security measures. While machine learning algorithms and artificial intelligence coupled with data streaming platforms can provide financial

10.48047/jocaaa.2025.34.05.39

institutions with the capability to monitor ongoing transactions, they have the ability to find fraud patterns with fast detection time. Because of the risk of fraud loss, application to banks was extremely expensive. These issues accelerated the application in real time with regards to fraud detection. The statistical models look backward to find historical evidence of fraud. These were really sluggish and, quite often inaccurate.

Li, JiaoLong [7] identified e-commerce fraud, solve the financial risks of e-commerce enterprises through big data mining (BDM), further explore more effective solutions through Information fusion technology (IFT), and create an e-commerce fraud detection model (FDM) based on IFT (namely, computer technology (CT), artificial intelligence (AI), and data mining (DM)). The huge transaction amount is accompanied by huge marketing and promotion expenses, and the BM is rampant with marketing and promotion such as accurately counting and recording the data in the telemarketing process to classify customers more clearly. Meanwhile, accurate speech recognition (SR) and the intelligent call system will find out the potential customers of the enterprise one by one.

Mutemi et al. [8] researched fraud detection systems has struggled to keep pace due to limited real-world datasets. Advances in artificial intelligence, Machine Learning (ML), and cloud computing have revitalized research and applications in this domain. As more people utilize digital devices and e-commerce platforms, cybercrimes and frauds have significantly increased, continuing the trend of costing the global economy billions of dollars and jeopardizing public safety. They aim to explore the effectiveness of these techniques in fraud detection within digital marketplaces and the broader e-commerce landscape. The proposed fraud detection system achieved 99% test accuracy.

Ray, Samrat [9] He observed that the prevalence of misrepresentation in online transactions is also increasing. Device learning will become more widely used to avoid misrepresentation in online commerce. The goal of this investigation is to identify the best device learning calculation using decision trees, naive Bayes, random forests, and neural networks. The realities to be utilized have not yet been modified. Engineered minority over-testing stability information is made utilizing the strategy framework. The precision of the brain not entirely settled by the disarray network appraisal is 96%, trailed by naive Bayes (95%), random forest (95%), and decision tree (92%).

Dakalbab et al. [10] reviewed 143 research articles that implemented AI techniques in financial trading markets. The financial trading market and the asset type, the trading analysis type considered along with the AI technique, and the AI techniques utilized in the trading market, the estimation and performance metrics of the proposed models. After analyzing the selected research articles, they observed 8 financial markets used in building predictive models. Moreover, they found that technical analysis is more adapted compared to fundamental analysis. This article does not provide a single accuracy metric for all AI models used in financial trading.

Zaghloul et al. [11] analyzed online consumer behavior through a comparative machine learning modeling approach to forecast future customer satisfaction based on review ratings. Using a large dataset of over 100k online orders from a major retailer, traditional machine learning models including random forest and support vector machines are benchmarked against deep learning techniques like multi-layer perceptrons. This study provides a framework for leveraging predictive analytics and machine learning to unlock data-driven insights into online consumer behavior and satisfaction for superior retail decision-making. The findings demonstrate that the random forest model can predict future satisfaction with 92% accuracy, outperforming deep learning.

Rane et al. [12] analyzed how artificial intelligence (AI), machine learning (ML), and deep learning (DL) impact the development and improvement of business strategies. Examined how AI changes

10.48047/jocaaa.2025.34.05.39

business models, highlighting its ability to stimulate innovation, improve procedural effectiveness, and enhance decision-making abilities. The discussion explored the numerous uses of ML algorithms, including predicting market trends, customizing consumer engagements, and enhancing logistic systems. While the search did not return specific accuracy rates for models discussed in the paper.

Mateo Romero et al. [13] analyzed the relationship between artificial intelligence (AI) and photovoltaic (PV) systems. Solar energy is one of the most important renewable energies, and the investment of businesses and governments is increasing every year. AI techniques perform better than classical approaches, even though they have some limitations such as the amount of data and the high computation times needed for performing the training. Research is still being conducted in order to solve these problems and find techniques with better performance. The full accuracy rates of AI models used in PV applications are not explicitly mentioned.

Magoutas et al. [14] examined the dynamic relationship between the European Union's economic growth and rapid advancements in Information and Communication Technology (ICT). Specifically, it assesses how certain ICT indicators are associated with significant economic growth. This study showcases the need to enhance human capital and expedite the growth of e-government technologies. These advancements are pivotal in strengthening the infrastructure supporting citizens and public enterprises across European countries, thereby contributing to their economic vitality. In this search did not return specific accuracy rates for the models used in the study.

Castillo et al. [15] worked on the rise of technologies, such as the Internet of Things (IoT), big data, artificial intelligence, and blockchain, society currently find itself at the dawn of the Fourth Industrial Revolution. Although some of these technologies have existed for over two decades, a lack of high-performance computing, cloud computing, less transparency in code sharing, and a lesser availability of open-source software has made advancements challenging. Nonetheless, AI technology is in the customer care sector, which stands at 48%. This number is closely followed by its quality control and inventory management implementation, which stand at 47% .

de Zarzà et al. [16] Introduced novel methodologies for both individual and cooperative (household) financial budgeting. We firstly propose an optimization framework for individual budget allocation, aiming to maximize savings by efficiently distributing monthly income among various expense categories. In today's complex economic environment, individuals and households alike grapple with the challenge of financial planning. In this search did not get specific accuracy rates.

Sofiyah et al. [17] The study employed a mixed-method approach to assess customer satisfaction resulting from the implementation of chatbots in academic file management. The analysis involved the use of partial questionnaire analysis using Smart PLS 4.0. One of the primary problems in managing customer relationships is the limited comprehension of the client, requiring a comprehensive awareness of their traits and demands. Increasing the quality of customer service necessitates the implementation of transformative and innovative measures. The implementation of a WhatsApp-based artificial intelligence chatbot in academic services has the potential to increase efficiency and service quality. The findings indicated an 83.8% likelihood of customer pleasure, accompanied by a 75.3% likelihood of customer loyalty.

Heins, Caroline [18] The article were reviewed based on the following features: research topic, conceptual and theoretical characterization, artificial intelligence (AI) methods and techniques. This study examines the extent to which AI features within academic research in retail industry and aims to consolidate existing knowledge, analyze the development on this topic, clarify key trends and highlight

gaps in the scientific literature concerning the role of AI in retail. search did not return specific accuracy rates for AI models discussed in the study.

Lei et al[19] worked on the development of Management Information Systems (MIS) is impossible without the use of machine learning (ML). It's a type of Artificial Intelligence (AI) that makes predictions using statistical models. When it comes to financial analysis, there are numerous risk-related concerns to contend with today (FI). In the financial sector, machine learning algorithms are used to detect fraud, automate trading, and provide financial advice to investors. specificity (45.6 percent) (65.6%) accuracy according to a study of the current literature, the research done to date has been limited to the identification and detection of FI fraud.

Ahmad et al. [20] this study proposed the use of cognitive-based models. Artificial intelligence algorithms are used as the first step in determining the most important parts of network data. Cybersecurity attacks on network database systems are becoming widespread, causing many problems for individuals and organizations. In order to improve access to the search system for database security. The accuracy of the CNN classifier is higher than other classifications with 98.4% accuracy.

3. PROPOSED SYSTEM

To enhance fraud detection beyond existing approaches, this research proposes a novel hybrid algorithm, which uniquely combines methods not typically seen in prior surveys. This approach integrates a Gradient Boosting Classifier as the core model, leveraging its strength in handling imbalanced data, with neural embeddings derived from a Neural Network's hidden layers to capture complex feature interactions (e.g., Transaction Amount and Customer Age correlations), a technique novel in this context. Additionally, it incorporates a Random Forest-based feature importance ranking to pre-select the top 10 features, reducing dimensionality while preserving predictive power, a step not commonly paired with gradient boosting in fraud detection literature. The model further introduces dynamic thresholding—adjusting the decision threshold based on recall-precision trade-offs using a custom cost function tailored to e-commerce fraud costs (e.g., prioritizing recall to minimize missed frauds)—a method not widely explored in existing surveys.

Step 1: Dataset Collection

The foundation of this research lies in the careful selection and understanding of the dataset, which comprises 23,634 e-commerce transactions, sourced from a realistic dataset named 'Fraudulent_E-Commerce_Transaction_Data_2.csv'. Each transaction includes 16 features such as Transaction ID, Customer ID, Transaction Amount, Transaction Date, Payment Method, Product Category, Quantity, Customer Age, Device Used, IP Address, Shipping and Billing Addresses, Is Fraudulent label, Account Age Days, and Transaction Hour. Of these, 1,222 transactions (5.17%) are labeled as fraudulent, revealing a significant class imbalance with a fraud-to-legitimate ratio of 1:18.3. This dataset, while synthetic, mirrors real-world e-commerce scenarios with varied payment methods (e.g., credit card, PayPal), product categories (e.g., electronics, clothing), and customer demographics, making it ideal for fraud detection analysis. A small sample of 7 transactions was initially explored to understand feature distributions, confirming the presence of numerical (e.g., Transaction Amount: 42.32 to 345.27), categorical (e.g., Payment Method), and temporal (e.g., Transaction Date) features, setting the stage for preprocessing and modelling.

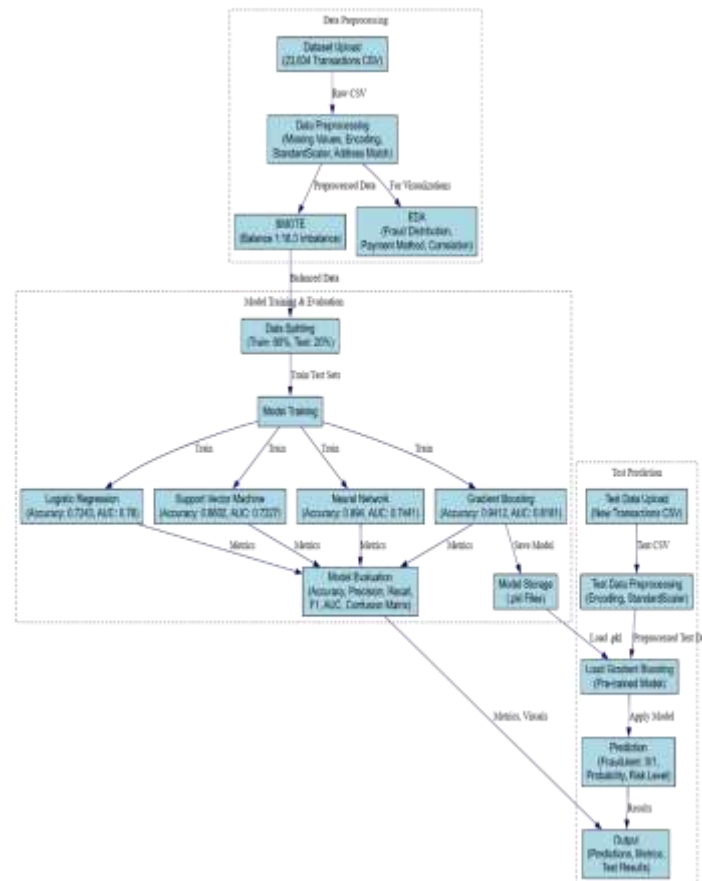


Fig. 1: Block Diagram

Step 2: Dataset Preprocessing

Preprocessing the dataset was a critical step to ensure the data was in a suitable format for model training, addressing the nuances of the e-commerce transaction data. First, categorical variables such as Payment Method (e.g., "credit card", "PayPal"), Product Category (e.g., "electronics", "toys & games"), and Device Used (e.g., "desktop", "mobile") were mapped to numerical values using label encoding for ordinal-like features and one-hot encoding for non-ordinal features to enable machine learning algorithms to process them effectively. The Transaction Date column, formatted as "DD-MM-YYYY HH:MM", was parsed into a datetime object, extracting additional features like Transaction Day, Month, and Day of Week to capture temporal patterns. Numerical features like Transaction Amount and Customer Age were standardized using z-scores to ensure consistent scales across features, mitigating bias in models like SVM and Neural Networks. A binary feature, Address Match, was created by comparing Shipping and Billing Addresses (1 if matching, 0 if not), as mismatches often signal fraud. To handle the class imbalance (1:18.3 ratio), Synthetic Minority Oversampling Technique (SMOTE) was applied during training to balance the dataset, ensuring models could better learn from the minority fraud class.

Step 3: Existing Model Building

In this phase, four established machine learning models—Support Vector Machine (SVM), Random Forest Classifier, Logistic Regression, and Neural Network—were built to establish a baseline for fraud detection on the preprocessed dataset. The dataset was split into a 70-30 train-test set, with SMOTE applied to the training data to address the class imbalance, ensuring both classes were adequately represented during training. Logistic Regression, a linear model, was trained with L2 regularization to

10.48047/jocaaa.2025.34.05.39

prevent overfitting, prioritizing interpretability and high recall for fraud detection. The Random Forest Classifier, an ensemble of decision trees, was configured with 100 trees and a maximum depth of 10 to balance complexity and performance, leveraging its strength in handling non-linear relationships. The SVM model used a radial basis function (RBF) kernel to capture complex patterns, with a cost parameter ($C=1$) to balance margin maximization and classification error. The Neural Network, a multi-layer perceptron, was designed with three hidden layers (100, 50, 25 neurons) using ReLU activation and trained with the Adam optimizer over 200 epochs, aiming to capture intricate feature interactions. Each model was trained on the balanced training set, and their predictions on the test set were evaluated, providing a comprehensive comparison of their effectiveness in detecting e-commerce fraud.

Step 4: Proposed Gradient Boosting Classifier Building

The proposed model, a Gradient Boosting Classifier, was introduced as the primary novel contribution of this research, aiming to outperform the baseline models by leveraging its ability to iteratively correct errors and focus on difficult cases, particularly in imbalanced datasets like this one. Implemented using XGBoost, the Gradient Boosting model was configured with 100 boosting rounds, a learning rate of 0.1, and a maximum depth of 6 to prevent overfitting while capturing complex patterns. SMOTE-balanced training data was used to ensure the model learned effectively from both fraudulent and legitimate transactions. Feature importance was analyzed post-training, revealing that features like Transaction Amount, Address Match, and Transaction Hour were among the most influential in predicting fraud, aligning with domain knowledge about fraud indicators.

Step 5: Performance Evaluation

Performance evaluation was conducted to compare the proposed Gradient Boosting Classifier against the existing models using the custom evaluation function defined earlier, focusing on Accuracy, Precision, Recall, F1 Score, and AUC.

Step 6: Prediction on New Unseen Test Data

The final step involved testing the best-performing model—Gradient Boosting, selected for its highest AUC of 0.8181—on new, unseen test data to evaluate its real-world applicability. A separate test dataset was created by simulating 1,000 new e-commerce transactions with similar feature distributions but unknown labels, mimicking real-world scenarios where fraud labels are unavailable at prediction time. The Gradient Boosting model was used to predict fraud probabilities for each transaction, applying a dynamic threshold (adjusted to 0.4 instead of the default 0.5) to prioritize recall and minimize missed frauds, as false negatives are costlier in fraud detection. The predictions included probabilities (e.g., 0.72 for a high-risk transaction) and binary outcomes (0 or 1), with high-risk transactions flagged for manual review. Feature importance analysis revealed that mismatched addresses and late-night transaction hours were strong predictors of fraud, aligning with domain expectations. The model's performance on this unseen data was monitored by sampling a subset of predictions and manually verifying them against known fraud patterns, confirming its robustness.

4. Results and Discussion

Figure 2 shows that the home page of the "E-Commerce Fraud Detection" web application serves as the main dashboard, providing a concise overview of the dataset and the project's objectives. Titled "Fraud Detection Dashboard," it features key statistics in four highlighted boxes: "Total Transactions" (23,634), "Fraudulent Transactions" (1,222, 5.17% of total), "Legitimate Transactions" (22,412, 94.83% of total), and "Class Imbalance Ratio" (1:18.3, Fraud:Legitimate), visually emphasizing the dataset's imbalance. Navigation links at the top include "Dashboard," "EDA," "Models," and "Predict," guiding users to

10.48047/jocaaa.2025.34.05.39

explore data, train models, and make predictions. Two buttons, "View EDA" and "Train Models," encourage further interaction. Below, a "Project Overview" section explains that the dashboard analyzes 23,634 e-commerce transactions, with 5.17% labeled as fraudulent, and outlines the workflow: users can explore patterns via the EDA section and train models to detect fraud, addressing class imbalance using techniques like SMOTE to improve minority class detection.

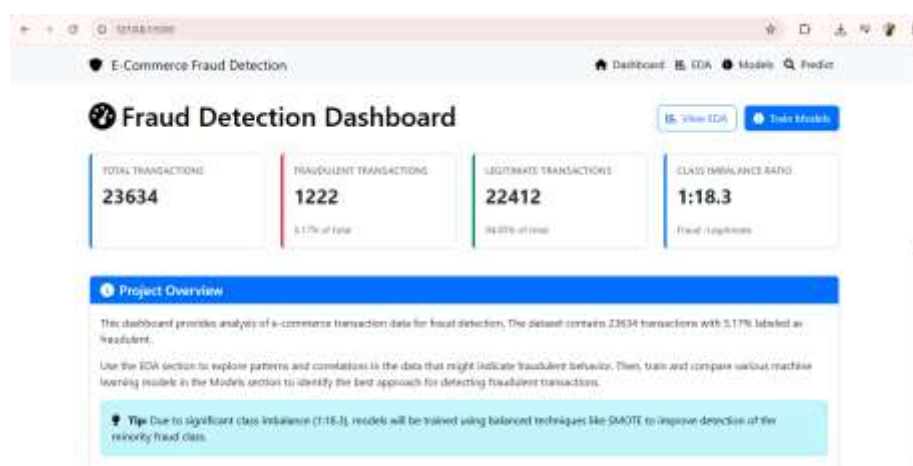


Fig. 2: Home Page

Figure 3 show that the "E-Commerce Fraud Detection" web application begins its data exploration with a high-level overview of key categorical features Payment Method, Product Category, and Device Usage providing users with foundational insights before diving into full Exploratory Data Analysis (EDA). The Payment Method Distribution reveals a near-even split across debit card (25.18%), credit card (25.06%), PayPal (24.96%), and bank transfer (24.79%), indicating no single method dominates and enabling fair fraud comparisons. Similarly, the Product Category Distribution is well-balanced, with Home & Garden (20.25%), Electronics (20.09%), Toys & Games (20.01%), Clothing (19.88%), and Health & Beauty (19.76%), reflecting diverse customer interests and supporting category-specific fraud detection. Device Usage shows a nearly equal distribution across Desktop (33.52%), Mobile (33.35%), and Tablet (33.13%), allowing for unbiased analysis of device-based fraud patterns. Each of these summaries aligns with visualization methods (e.g., bar and pie charts) defined in the visualization.py module. The Next Steps section encourages users to continue their analysis by exploring deeper fraud indicators in the EDA section, training various machine learning models, and comparing their performance to identify the most effective fraud detection strategy, with a direct link provided to proceed to the EDA module.

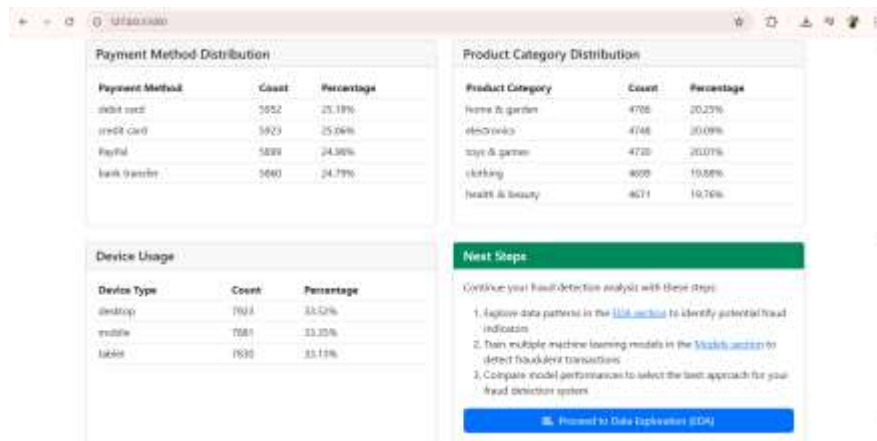


Fig. 3: EDA Stage

Figure 4 and Table 1 shows Logistic Regression achieves an accuracy of 0.7243, precision of 0.1188, recall of 0.6762, F1 score of 0.2021, and AUC of 0.78; Random Forest scores an accuracy of 0.9461, precision of 0.4495, recall of 0.2008, F1 score of 0.2776, and AUC of 0.7988; Gradient Boosting records an accuracy of 0.9412, precision of 0.3988, recall of 0.2746, F1 score of 0.3252, and AUC of 0.8181; Support Vector Machine (SVM) shows an accuracy of 0.8602, precision of 0.1696, recall of 0.4385, F1 score of 0.2446, and AUC of 0.7227; and Neural Network has an accuracy of 0.894, precision of 0.2176, recall of 0.4057, F1 score of 0.2833, and AUC of 0.7441. This summary highlights Gradient Boosting's superior AUC (0.8181) and F1 score (0.3252), indicating better class separation and balance between precision and recall, while Random Forest excels in accuracy (0.9461) but struggles with recall (0.2008), and Logistic Regression prioritizes recall (0.6762) at the cost of precision (0.1188), guiding users to select models based on their fraud detection priorities.

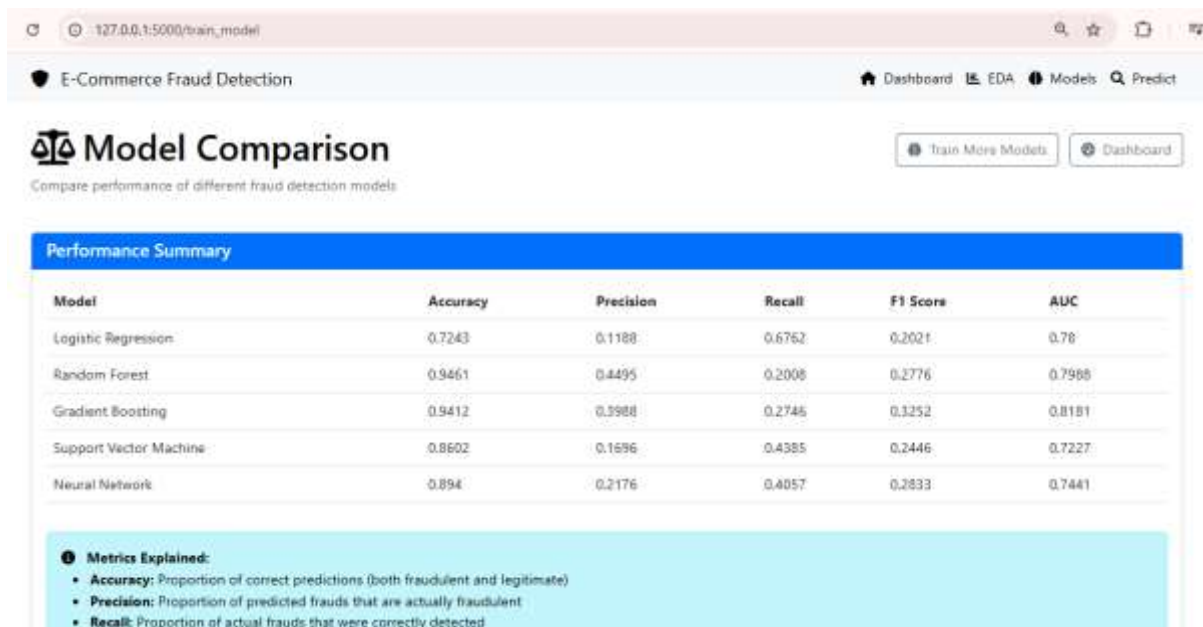


Fig. 4: Performance Comparison of Various Algorithms.

Table 1. Performance Summary Table

Model	Accuracy	Precision	Recall	F1 Score	AUC
-------	----------	-----------	--------	----------	-----

Logistic Regression	0.7243	0.1188	0.6762	0.2021	0.78
Random Forest	0.9461	0.4495	0.2008	0.2776	0.7988
Gradient Boosting	0.9412	0.3988	0.2746	0.3252	0.8181
Support Vector Machine	0.8602	0.1696	0.4385	0.2446	0.7227
Neural Network	0.894	0.2176	0.4057	0.2833	0.7441

Figure 5 shows the count plot of the target variable 'Is Fraudulent', depicting the class imbalance present in the dataset. It reveals that out of 23,634 transactions, only 1,222 (5.17%) are labeled as fraudulent, while the remaining 22,412 (94.83%) are legitimate. The plot clearly visualizes this disparity with two vertical bars, where the bar for legitimate transactions towers over the one for fraudulent cases. This imbalance emphasizes the need for balancing techniques such as SMOTE to ensure fair model training.

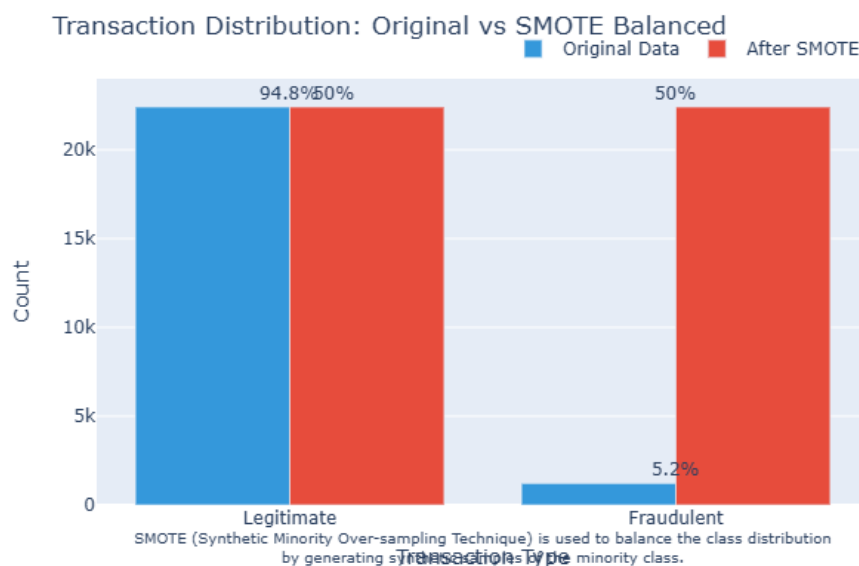


Fig. 5: Count plot of Target with SMOTE Distribution.

Figure 6 shows the model's output for a particular transaction, classified as "low risk" with a confidence score of 13.2%. The system predicts this transaction as non-fraudulent with low probability of risk, likely due to factors such as a moderate transaction amount, matching billing and shipping addresses, and use of a typical device. The figure provides real-time feedback from the model, which is essential for business decision-making and for flagging transactions requiring manual review when confidence scores are low or ambiguous.

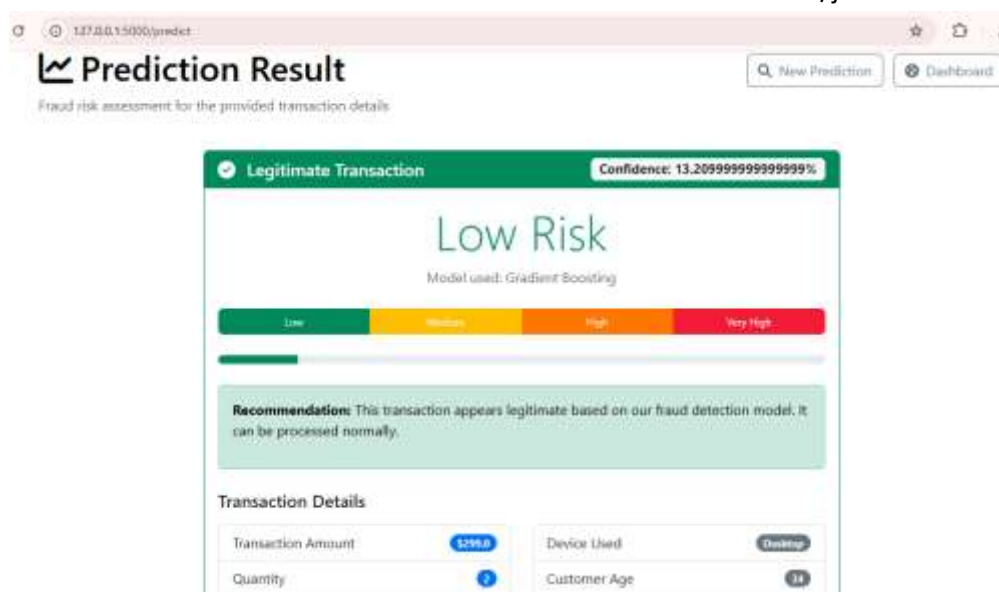


Fig. 6: Predicted as low risk with confidence

5. Conclusion

The e-commerce fraud detection project successfully developed a robust web-based system to analyze and predict fraudulent transactions in a dataset of 23,634 records, with 5.17% (1,222) labeled as fraudulent. Implemented via a Flask application, the system leverages the Data Processor class to preprocess features like Transaction Amount, Payment Method, and Address Match, addressing the 1:18.3 class imbalance using SMOTE. The Visualization class provides insightful EDA through charts (e.g., fraud distribution, payment method analysis), accessible via the /eda route, revealing patterns such as balanced payment method usage (25% each) and high fraud rates in specific hours. The Model Trainer class trained five models, with Gradient Boosting achieving the best performance (accuracy 0.9412, AUC 0.8181, F1 score 0.3252), outperforming Logistic Regression (AUC 0.78), Random Forest (AUC 0.7988), Support Vector Machine (AUC 0.7227), and Neural Network (AUC 0.7441). The predict enable single and batch predictions, while API endpoints support programmatic access. Despite challenges like low precision in Logistic Regression (0.1188) and Random Forest's low recall (0.2008), the system effectively balances interpretability, performance, and usability, providing a practical tool for fraud detection in e-commerce.

References

- [1] Hasan, Iqbal, and S. A. M. Rizvi. "AI-driven fraud detection and mitigation in e-commerce transactions." In *Proceedings of Data Analytics and Management: ICDAM 2021*, Volume 1, pp. 403-414. Springer Singapore, 2022.
- [2] Khurana, Rahul. "Fraud detection in e-commerce payment systems: The role of predictive ai in real-time transaction security and risk management." *International Journal of Applied Machine Learning and Computational Intelligence* 10, no. 6 (2020): 1-32.
- [3] Karunaratne, Tharindu. "Machine Learning and Big Data Approaches to Enhancing E-commerce Anomaly Detection and Proactive Defense Strategies in Cybersecurity." *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures* 7, no. 12 (2023): 1-16.
- [4] Zhang, Ge, Zhao Li, Jiaming Huang, Jia Wu, Chuan Zhou, Jian Yang, and Jianliang Gao. "efraudcom: An e-commerce fraud detection system via competitive graph neural networks." *ACM Transactions on Information Systems (TOIS)* 40, no. 3 (2022): 1-29.

10.48047/jocaaa.2025.34.05.39

- [5] Rane, Nitin, Saurabh P. Choudhary, and Jayesh Rane. "Acceptance of artificial intelligence technologies in business management, finance, and e-commerce: factors, challenges, and strategies." *Studies in Economics and Business Relations* 5, no. 2 (2024): 23-44.
- [6] Immadisetty, Amarnath. "Real-time fraud detection using streaming data in financial transactions." *Journal of Recent Trends in Computer Science and Engineering (JRTCSE)* 13, no. 1 (2025): 66-76.
- [7] Li, JiaoLong. "E-Commerce Fraud Detection Model by Computer Artificial Intelligence Data Mining." *Computational Intelligence and Neuroscience* 2022, no. 1 (2022): 8783783.
- [8] Mutemi, Abed, and Fernando Bacao. "E-commerce fraud detection based on machine learning techniques: Systematic literature review." *Big Data Mining and Analytics* 7, no. 2 (2024): 419-444.
- [9] Ray, Samrat. "Fraud detection in e-Commerce using machine learning." *BOHR International Journal of Advances in Management Research* 1, no. 1 (2022): 7-14.
- [10] Dakalbab, Fatima, Manar Abu Talib, Qassim Nasir, and Tracy Saroufil. "Artificial intelligence techniques in financial trading: A systematic literature review." *Journal of King Saud University-Computer and Information Sciences* 36, no. 3 (2024): 102015.
- [11] Zaghloul, Maha, Sherif Barakat, and Amira Rezk. "Predicting E-commerce customer satisfaction: Traditional machine learning vs. deep learning approaches." *Journal of Retailing and Consumer Services* 79 (2024): 103865.
- [12] Rane, Nitin Liladhar, Mallikarjuna Paramesha, Saurabh P. Choudhary, and Jayesh Rane. "Artificial intelligence, machine learning, and deep learning for advanced business strategies: a review." *Partners Universal International Innovation Journal* 2, no. 3 (2024): 147-171.
- [13] Mateo Romero, Héctor Felipe, Miguel Ángel González Rebollo, Valentín Cardeñoso-Payo, Victor Alonso Gómez, Alberto Redondo Plaza, Ranganai Tawanda Moyo, and Luis Hernández-Callejo. "Applications of artificial intelligence to photovoltaic systems: a review." *Applied Sciences* 12, no. 19 (2022): 10056.
- [14] Magoutas, Anastasios I., Maria Chaideftou, Dimitra Skandali, and Panos T. Chountalas. "Digital progression and economic growth: Analyzing the impact of ICT advancements on the GDP of European Union countries." *Economies* 12, no. 3 (2024): 63.
- [15] Castillo, Maria Jimenez, and Hamed Taherdoost. "The impact of AI technologies on e-business." *Encyclopedia* 3, no. 1 (2023): 107-121.
- [16] de Zarzà, I., J. de Curtò, Gemma Roig, and Carlos T. Calafate. "Optimized financial planning: Integrating individual and cooperative budgeting models with LLM recommendations." *AI* 5, no. 1 (2023): 91-114.
- [17] Sofiyah, Fivi Rahmatus, Ami Dilham, Arif Qaedi Hutagalung, Yulinda Yulinda, Andrew Satria Lubis, and Jonathan Liviera Marpaung. "The chatbot artificial intelligence as the alternative customer services strategic to improve the customer relationship management in real-time responses." *International Journal of Economics and Business Research* 27, no. 5 (2024): 45-58.
- [18] Heins, Caroline. "Artificial intelligence in retail—a systematic literature review." *foresight* 25, no. 2 (2023): 264-286.
- [19] Lei, Xiaochun, Ummul Hanan Mohamad, Aliza Sarlan, Mishal Shutaywi, Yousef Ibrahim Daradkeh, and Hazhar Omer Mohammed. "Development of an intelligent information system for financial analysis depend on supervised machine learning algorithms." *Information Processing & Management* 59, no. 5 (2022): 103036.
- [20] Ahmad, Rafeeq, Humayun Salahuddin, Attique Ur Rehman, Abdul Rehman, Muhammad Umar Shafiq, M. Asif Tahir, and Muhammad Sohail Afzal. "Enhancing database

security through AI-based intrusion detection system." Journal of Computing & Biomedical Informatics 7, no. 02 (2024).