International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Fraud Detection in E-commerce – A Machine Learning Approach

Author: Shahid Siddique

Program: Master of Business Administration (2023–2025)
Institution: Galgotias University

Abstract

E-commerce platforms are increasingly threatened by fraud, ranging from identity theft to payment manipulation. Traditional rule-based systems often struggle to identify evolving fraud patterns. This study investigates the application of machine learning (ML) algorithms to enhance fraud detection accuracy in real time. Through a mixed-method approach involving survey data from 100 consumers and interviews with industry professionals, the research evaluates the effectiveness, challenges, and ethical implications of ML-based fraud detection systems.

1. Introduction

Online shopping growth has coincided with a rise in digital fraud. E-commerce businesses now face sophisticated fraudulent techniques that bypass traditional systems. Machine learning offers a dynamic alternative—learning from data to detect and prevent irregular behavior in transactions. This study explores how ML tools, such as supervised and unsupervised algorithms, can be integrated into e-commerce platforms to improve fraud prevention while preserving user experience.

2. Objectives

- Identify prevalent fraud types in online commerce.
- Evaluate the performance of ML algorithms in detecting fraud.
- Examine consumer awareness and trust in automated fraud detection systems.
- Assess implementation challenges including data privacy and false positives.

3. Methodology

- **Design:** Mixed-method (Quantitative + Qualitative)
- **Quantitative Component:** Survey of 100 frequent online shoppers.
- **Qualitative Component:** Interviews with 5+ cybersecurity professionals and e-commerce managers.
- **Analysis Tools:** Python (for ML modeling), SPSS (for statistical testing), Thematic analysis (for interview data).

Machine Learning Models Tested:

- Logistic Regression
- Decision Trees
- Random Forest
- Support Vector Machines

Evaluation Metrics:
Accuracy, Precision, Recall, F1-score, and Confusion Matrix.

4. Key Findings

Quantitative Highlights:

- 68.9% of fraud detection performance is predicted by variables such as ML usage, real-time monitoring, and multi-factor authentication.
- Machine learning emerged as the strongest predictor of fraud detection success ($\beta = 0.398$, $p < 0.001$).
- 74% of respondents believe ML improves fraud detection speed and accuracy.
- 58% of users express concern about how their data is used.

Qualitative Insights:

- Experts confirm ML models detect anomalies faster than traditional methods.
- Real-time monitoring and consumer behavior data are crucial for detecting fraud.
- False positives remain a significant concern, highlighting the need for balanced system calibration.
- Ethical data usage and transparency are key to maintaining user trust.

5. Discussion

The results align with existing academic research suggesting that ML enables dynamic fraud detection by continuously learning from data. However, user trust and privacy concerns must be addressed through ethical data handling and transparent practices. The integration of AI should not be fully autonomous—human oversight is critical to interpret model outputs and respond to edge cases.

6. Recommendations

- Implement layered fraud detection systems combining ML, real-time alerts, and human review.
- Prioritize data privacy with transparent consent policies.
- Tailor fraud detection strategies to specific industries and risk profiles.
- Invest in user education about fraud risks and protective measures.
- Continuously update ML models to adapt to new fraud patterns.

7. Conclusion

Machine learning offers robust potential in combating e-commerce fraud by identifying anomalies and adapting to new threats. While highly effective, ML systems must be designed responsibly, with careful attention to false positives, data ethics, and user trust. When strategically integrated, these systems can significantly enhance the security of online transactions and contribute to a safer digital marketplace.

Keywords:

E-commerce, Fraud Detection, Machine Learning, Cybersecurity, Data Ethics, Real-time Monitoring, AI in Business.