E-Commerce Fraud Detection Based on Machine Learning

IEEE BASE PAPER TITLE:

E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review

IEEE BASE PAPER ABSTRACT:

The e-commerce industry's rapid growth, accelerated by the COVID-19 pandemic, has led to an alarming increase in digital fraud and associated losses. To establish a healthy e-commerce ecosystem, robust cyber security and anti-fraud measures are crucial. However, research on 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. While ML and data mining techniques are popular in fraud detection, specific reviews focusing on their application in e-commerce platforms like eBay and Facebook are lacking depth. Existing reviews provide broad overviews but fail to grasp the intricacies of ML algorithms in the e-commerce context. To bridge this gap, our study conducts a systematic literature review using the Preferred Reporting Items for Systematic reviews and Meta-Analysis (PRISMA) methodology. We aim to explore the effectiveness of these techniques in fraud detection within digital marketplaces and the broader e-commerce landscape. Understanding the current state of the literature and emerging trends is crucial given the rising fraud incidents and associated costs. Through our investigation, we identify research opportunities and provide insights to industry stakeholders on key

ML and data mining techniques for combating e-commerce fraud. Our paper examines the research on these techniques as published in the past decade. Employing the PRISMA approach, we conducted a content analysis of 101 publications, identifying research gaps, recent techniques, and highlighting the increasing utilization of artificial neural networks in fraud detection within the industry.

OUR PROPOSED ABSTRACT:

The project titled "E-Commerce Fraud Detection Based on Machine Learning" addresses the critical challenge of identifying fraudulent transactions in e-commerce platforms. Developed using Python for backend processing and HTML, CSS, and JavaScript for the frontend interface, the system is integrated within the Flask web framework to deliver a responsive and interactive user experience.

The project leverages two advanced machine learning models: a Stacking Classifier and an XGB Classifier. The Stacking Classifier achieves an impressive train accuracy of 100% and a test accuracy of 99%, while the XGB Classifier attains a train accuracy of 96% and a test accuracy of 95%. These high performance metrics underscore the models' effectiveness in distinguishing between legitimate and fraudulent transactions.

The dataset utilized comprises 23,634 synthetic records generated through Python's Faker library, enriched with custom logic to emulate realistic transaction patterns and fraudulent scenarios. The dataset includes 16 features such as Transaction ID, Customer ID, Transaction Amount, Payment Method, and a binary indicator for fraudulent activity, among others. These features collectively capture the intricacies of transaction behaviors and customer profiles, enabling robust fraud detection.

The project's results demonstrate the potential of machine learning techniques in enhancing security and trust in e-commerce environments, providing a powerful tool for preventing financial loss due to fraudulent activities.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium i3 Processor.
- Hard Disk : 500 GB.
- Monitor : 15'' LED.
- Input Devices : Keyboard, Mouse.
- Ram : 8 GB.

SOFTWARE REQUIREMENTS:

- Operating System : Windows 10 / 11.
- Coding Language : Python 3.12.0.
- Web Framework : Flask.
- Frontend : HTML, CSS, JavaScript.

REFERENCE:

Abed Mutemi, Fernando Bacao, "E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review", Big Data Mining and Analytics (Volume: 7, Issue: 2, June 2024), IEEE Journal 2024.