Chapter 10
Fraud Detection in E-Commerce Transactions Using Machine Learning Techniques and Quantum Networks

G. Rajeshwari
Dr. Mahalingam College of Engineering and Technology, India

S. Mownika
Dr. Mahalingam College of Engineering and Technology, India

G. Anupriya
Dr. Mahalingam College of Engineering and Technology, India

R. Kishore
Dr. Mahalingam College of Engineering and Technology, India

ABSTRACT

Fraud poses a significant threat across various sectors, with the e-commerce industry being particularly vulnerable based on quantum network. Using quantum networks for detecting fraud in e-commerce transactions has the potential to completely change online security. Quantum networks rely on the principles of quantum mechanics to provide the highest level of security when transmitting data. Companies facilitating online payments gather extensive data on user transactions, leveraging machine learning techniques to differentiate between legitimate and fraudulent activities. To enhance expertise in fraud detection, machine learning methods are employed

DOI: 10.4018/979-8-3693-5832-0.ch010

to identify online payment fraud within e-commerce transactions. The dataset, structured at the transaction level, is analysed to uncover patterns distinguishing fraudulent behaviour from normal transactions. Feature engineering, such as incorporating user-level statistics like mean and standard deviation, aids in pattern recognition—a common practice in models like LGBMs (light gradient boosting machines). Detecting fraud presents a challenge due to the imbalance between fraudulent and non-fraudulent data. The performance of the model is evaluated using metrics such as accuracy and F1 score. The current system employs Bayesian optimization techniques to refine LGBM and XGBoost models. The proposed model aims to identify consumer fraud by analysing purchasing patterns and historical data using machine learning methodologies, specifically adopting a classification approach. Tree-based methods, including tree-based bagging and boosting techniques such as LGBM, XGBoost, CatBoost, and deep learning, are utilized. The synthetic minority over-sampling technique (SMOTE) is used to balance the imbalanced data. The primary aim is to create a reliable fraud detection system that is suited to the e-commerce environment.

INTRODUCTION

The electronic exchange of goods and services via a variety of platforms, including PCs, tablets, smartphones, and other smart gadgets, is known as e-commerce. It includes a variety of exchanges, such as those between businesses and consumers, business and business, consumer and business, company and administration, and consumer and administration. In the past few years, there has been a significant increase in financial transactions, driven by the growth of financial institutions and the widespread adoption of online e-commerce. This surge in transactions has also led to a rise in fraudulent activities, especially in internet banking, posing a greater challenge in detecting and preventing fraudulent transactions. As credit card technology evolves, so does the sophistication of credit card fraud. Fraudsters continually adapt their tactics to mimic legitimate transactions, making fraud detection increasingly challenging. They invest efforts in understanding how fraud detection systems operate and persistently test and manipulate these systems, adding layers of complexity to fraud detection. Consequently, researchers continuously strive to develop innovative approaches or enhance the effectiveness of existing methods to combat these evolving fraudulent activities. The e-commerce industry faces vulnerabilities due to its reliance on online transactions, where sensitive information can be intercepted or compromised. Quantum networks enhance security by employing quantum encryption, rendering intercepted data unreadable due to the inherent properties of quantum mechanics, thereby mitigating fraud risks in e-commerce

Fundamentals of Quantum Computation and Basic Quantum Gates

Swathi Mummadiand Bhawana Rudra (2024). *Quantum Computing and Cryptography in Future Computers (pp. 33-50).*
www.irma-international.org/chapter/fundamentals-of-quantum-computation-and-basic-quantum-gates/352406