

Real-Time Credit Card Fraud Detection Using Adaptive Machine Learning and Behavioral Analytics

Name : Ahmad Mostafa Abutalib

Student ID: 243002097

Dept: Science of AI

Organization: Midocean University

Country: UAE

Email:

243002097@st.midocean.edu.km

Abstract

Credit card fraud is becoming more common as people rely more on online payments and digital transactions. Detecting fraud quickly and accurately is a real challenge, especially because fraud patterns keep changing and the number of transactions is huge. Many of the older studies used machine learning, but they often had some clear issues—like using outdated or limited data, struggling with very few fraud cases compared to normal ones, or being too slow for real-time use. In this paper, we propose a new approach that's designed to work in real time. It uses several types of data—not just transaction details, but also user behavior and device information. We also use advanced models like XGBoost, LSTM, and DNN, and we make sure the system can keep learning and adapting over time. Our goal is to make fraud detection faster, smarter, and more useful in real-world systems like banks and online payment platforms.

Keywords—Credit Card Fraud Detection, Machine Learning, Deep Learning, Logistic Regression, Random Forest, XGBoost, LSTM, Imbalanced Data, Real-Time Processing, Adaptive Learning.

I. INTRODUCTION

Credit card fraud continues to rise globally, causing significant financial losses to individuals and institutions. As online transactions become more common, the need for accurate and real-time fraud detection systems becomes more urgent. While many machine learning-based approaches have been explored in recent years, they often suffer from key limitations—such as class imbalance, reliance on outdated or synthetic datasets, and inability to detect evolving fraud tactics in real time.

In this study, we introduce a practical and adaptive framework for real-time fraud detection. Our method leverages multiple data types (transactional, behavioral, and device-based), and integrates advanced models like XGBoost, LSTM, and DNN. By combining adaptive learning and real-world applicability, our approach aims to significantly improve the efficiency and accuracy of fraud detection systems in dynamic environments such as banking and e-commerce.

II. RELATED WORK

Over the past decade, many researchers have focused on detecting credit card fraud using various machine learning and deep learning techniques. These studies have shown that traditional rule-based systems are no longer effective in identifying evolving fraud patterns, especially with the rise of online and mobile transactions.

Some works have introduced ensemble models like Random Forest or XGBoost, which combine multiple decision trees to improve accuracy. Others explored deep learning methods such as Deep Neural Networks (DNNs) and Long Short-Term Memory (LSTM) networks to capture complex transaction behaviors over time. More recently, graph-based models like Graph Neural Networks (GNNs) have been applied to represent relationships between users and transactions.

While these approaches achieved high performance in experiments, they still face common limitations. Most of them rely on simulated or outdated datasets, making them hard to apply in real-time situations. Many models are also designed for offline detection and do not adapt to changing fraud tactics. Moreover, handling the imbalance between fraudulent and legitimate transactions remains a major challenge.

This study builds on these findings by proposing a real-time fraud detection system that integrates transactional, behavioral, and device-level data. It aims to overcome past limitations through adaptive learning and the use of diverse machine learning models.

III. CONCLUSION

This review has explored a wide range of recent studies in the field of credit card fraud detection, highlighting the strengths, limitations, and methodologies adopted in previous works. While significant progress has been made through the application of machine learning and deep learning techniques, common challenges remain, including severe class imbalance, limited interpretability of complex models, and the inability of static detection systems to adapt to evolving fraud tactics. Many prior studies also rely on outdated or simulated datasets, which limits their applicability to real-world environments.

Our analysis shows that future research should focus on integrating multi-source data—combining transactional, behavioral, and device-level information—while adopting adaptive learning techniques that can respond to changes in fraud patterns in real time. Furthermore, approaches that address class imbalance through advanced sampling strategies and cost-sensitive learning are essential for improving prediction accuracy and reducing false positives.

By addressing these gaps, future frameworks can become more scalable, practical, and effective in real-world payment systems, ultimately contributing to enhanced financial security and customer trust.