

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

Name : Ahmad Mostafa Abutalib

Student ID: 243002097

Dept: Scince of AI

Organization: Midocean University

Country: UAE

Email: 243002097@st.midocean.edu.km

Abstract

Credit card fraud is still a quickly growing problem in today's financial systems, and it has a big effect on banks, e-commerce sites, and users all over the world. The Nilson Report says that fraud losses around the world were \$28.65 billion in 2020 and will likely reach \$35.67 billion by 2023 [1]. The rise in online shopping, mobile wallets, and digital banking is driving this upward trend. These technologies make life easier, but they also create new security holes that scammers use to steal money through phishing, account takeovers, and fake identity fraud [2].

Conventional rule-based fraud detection systems, which depend on fixed thresholds like transaction amount, location, or merchant type, have shown to be ineffective against progressively adaptive and advanced attack strategies [3]. As a result, machine learning (ML) and deep learning (DL) methods like Logistic Regression, Random Forest, XGBoost [4], LSTM [5], and hybrid CNN-SVM models [6] have shown to work better in tests.

Even with these improvements, there are still some big problems. The use of the old Kaggle 2013 dataset mostly hides new fraud patterns that are connected to mobile payments and cross-border schemes [7]. A severe class imbalance, in which fraudulent instances account for less than

0.2% of transactions, further diminishes detection efficacy [8]. Furthermore, the majority of previous endeavors exist solely as offline prototypes, devoid of the scalability and adaptability requisite for real-time banking operations [9].

This paper proposes an adaptive framework that addresses these limitations by integrating multi-source data—encompassing transactional, behavioral, and device-level information—and deploying advanced machine learning (ML) and deep learning (DL) models, including XGBoost, LSTM, and Deep Neural Networks (DNN). Adaptive learning mechanisms that allow for continuous model updates are at the heart of our approach. This makes sure that we can respond to new fraud tactics as they come up. The goal of this work is to come up with a scalable, practical way to improve fraud prevention in today's financial environments.

Background

Since electronic payment systems first came out, credit card fraud has been a big problem. In the 1980s and 1990s, most fraud was caused by stealing physical cards or making fake cards using methods like magnetic stripe skimming [1]. As a result, the introduction of EMV (Europay, Mastercard, and Visa) chip technology in the late 1990s and early 2000s made it much harder for people to commit fraud at physical terminals. But this technological progress unintentionally led to a rise in online and card-not-present (CNP) fraud [2].

With the rise of e-commerce, mobile wallets, and peer-to-peer digital payment platforms, criminals have been able to use more advanced methods like phishing, SIM-swapping, malware injection, and making fake identities. These new threats have made old ways of stopping fraud less effective, so we need to come up with real-time, data-driven detection systems [3]. By 2023, online and mobile fraud accounted for more than 70% of global credit card fraud cases, resulting in losses amounting to billions of dollars [4].

The evolution of fraud detection has kept pace with improvements in data access. Initially, methods relied exclusively on transactional data; however, as fraudulent strategies advanced, professionals began to incorporate behavioral and device-level data to obtain more comprehensive contextual signals [5]. There are still big problems, like the fact that fraudulent transactions make up less than 0.2% of all data, which leads to biased models [6], and the fact that the Kaggle 2013

dataset is too old and doesn't include new fraud techniques [7]. Moreover, the phenomenon of concept drift, which refers to the changing patterns of fraud over time, highlights the need for adaptive, real-time detection solutions that can learn and change constantly [8].

Introduction

In the last forty years, credit card fraud has changed a lot. At first, the threats were mostly physical, like stealing cards and making fake magnetic stripes [10]. The worldwide switch to EMV chip technology cut down on fake fraud, but it also led to more online and CNP fraud. Modern fraudsters use phishing, malware, SIM-swapping, and fake identities to take advantage of digital ecosystems, which makes it harder than ever for traditional detection systems to catch them [2].

There are big effects on both money and reputation. As global fraud losses rise by almost 10% each year [1], businesses are dealing with higher operating costs, more pressure from regulators, and a loss of trust from customers. These circumstances underscore the pressing necessity for intelligent, adaptive detection systems that transcend static, rule-based frameworks [3].

Machine learning is now an important part of modern fraud detection because it can find small and complicated fraud patterns in huge datasets. Random Forest and XGBoost [4] are examples of ensemble methods that improve predictive accuracy. Deep neural networks (DNNs) are another type of method that can find complex, non-linear relationships. Recurrent architectures, such as LSTM [5], are great at finding patterns of fraud over time, and hybrid models (like CNN-SVM) can handle noise in the data [6].

Even though there has been a lot of progress, there are still three big problems: (1) extreme data imbalance, which makes classifiers favor legitimate transactions [8]; (2) reliance on old datasets that don't show how fraud is done now [7]; and (3) the fact that most models only work in batch or offline settings [9].

This study presents a holistic framework that integrates transactional, behavioral, and device-level data within a real-time adaptive learning context. The proposed solution aims to deliver

both scalability and practical applicability for deployment in financial institutions, e-commerce, and fintech sectors by leveraging XGBoost, LSTM, and DNN.

Research Problem, Questions, and Objectives

Research Problem	Research Questions	Research Objective
Traditional fraud detection systems are static, slow to adapt, and generate high false positives.	Q1: How can machine learning improve detection accuracy compared to rule-based systems?	Objective 1: Build a real-time fraud detection framework using ML/DL.
	Q2: Which algorithm provides the best trade-off between accuracy and speed?	
	Q3: How can adaptive learning help maintain system accuracy over time?	Objective 2: Implement adaptive learning for continuous improvement.

Related Work

In recent years, detecting credit card fraud has become a major area of research in both academia and industry. The transition from fixed fraud patterns to dynamic, adaptive attacks has accelerated the implementation of machine learning and deep learning techniques.

Traditional approaches: Early systems used statistical methods and Logistic Regression, which made them easy to understand but not very good at catching complicated fraud patterns [10]. As fraud tactics changed, rule-based systems quickly became useless [3].

Machine learning methods: Ensemble models like Random Forest and XGBoost became popular because they could model how features interact and deal with moderate class imbalance [4]. But because they rely on static datasets, they can't easily adapt to new types of fraud.

Deep learning techniques: Neural architectures such as DNNs, CNNs, and LSTMs have been developed to analyze spatial and temporal transaction patterns [5], [6], [13]. Hybrid models, such as CNN+GRU+MLP, have attained accuracy rates of up to 100% on the Kaggle dataset [15]. To fix class imbalance, SMOTE-based oversampling has also been used [16].

Even with these improvements, there are still three main problems: using old datasets, not performing well in real time, and not being able to understand black-box models. These problems have made it hard for experimental models to be used in big financial systems in the real world.

Summary of Related Works

Reference	Year	Method(s)	Dataset	Results
[9]	2024	MLP	Kaggle (2013)	98%
[10]	2023	Hybrid CNN-SVM	Kaggle (2013)	91.05%
[11]	2021	MLP-OSCNN	Kaggle (2013)	98%
[12]	2023	CNN (no pooling)	Kaggle (2013)	83.72%
[13]	2024	LSTM	Kaggle (2013)	96.3%
[14]	2020	BiLSTM + BiGRU	Custom (YourAllModelsData)	91.37%
[15]	2024	CNN + GRU + MLP	Kaggle (2013)	100%

Reference	Year	Method(s)	Dataset	Results
[16]	2024	NN + SMOTE	Kaggle (2013)	99%

Conclusion

This review has followed the progression of credit card fraud detection from simple rule-based systems to advanced machine learning and deep learning methods. Models like CNN, LSTM, and hybrid ensembles have gotten very good at getting things right (over 95% [9], [15]), but they can't be used in real life because they depend on old datasets, can't adapt to new fraud tactics, and can't change in real time.

Even though it's easy to use the Kaggle 2013 dataset over and over again, it doesn't show how fraud happens today with mobile wallets, peer-to-peer payments, and fake identities. Additionally, oversampling methods such as SMOTE [16] rectify class imbalance but may distort data distributions and hinder model generalizability. Model explainability is still a big problem because deep learning models are hard to understand, which makes it harder to follow the rules and makes people less likely to trust them.

Future studies should focus on:

Combining transactional, behavioral, and device-level information to get better fraud signals is called multi-source data integration.

Adaptive learning: Using online learning and concept drift detection to find new patterns of fraud.

Explainable AI (XAI): Making detection models more clear and easy to understand.

Federated learning: Making it easier for institutions to work together while keeping their privacy intact so they can share fraud intelligence.

By dealing with these problems, future systems can be deployed in real time on a large scale, which will make digital payment systems safer and more reliable.

References

- [1] Nilson Report, Global Fraud Loss Statistics, 2023.
- [2] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *Journal of Network and Computer Applications*, vol. 68, pp. 90–113, 2016.
- [3] S. Bhattacharyya et al., "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.
- [4] S. Chen, H. Huang, and L. Tian, "Credit card fraud detection using XGBoost and random forest," *IEEE Access*, vol. 8, pp. 31517–31525, 2020.
- [5] I. Ibraheem et al., "Credit Card Fraud Detection Using Improved Deep Learning Models," *ResearchGate*, 2024. [Online]. Available: <https://www.researchgate.net/publication/377830394>
- [6] X. Zhang et al., "Hybrid CNN-SVM for credit card fraud detection," *Wiley Online Library*, 2023. [Online]. Available: <https://onlinelibrary.wiley.com/doi/full/10.1155/2023/8134627>
- [7] Kaggle, "Credit Card Fraud Detection Dataset (2013)," [Online]. Available: <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>
- [8] A. Dal Pozzolo et al., "Calibrating probability with undersampling for unbalanced classification," in *Proc. IEEE Symposium on Computational Intelligence and Data Mining*, 2015.
- [9] IEEE, "MLP for Credit Card Fraud Detection," *IEEE Xplore*, 2024. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10595068>
- [10] X. Zhang et al., "Hybrid CNN-SVM Credit Card Fraud Detection," *Wiley Online Library*, 2023. [Online]. Available: <https://onlinelibrary.wiley.com/doi/full/10.1155/2023/8134627>
- [11] IEEE, "MLP-OSCNN Results for Fraud Detection," *IEEE Xplore*, 2021. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/9480639>
- [12] M. Al-Hadi, "CNN without pooling for credit card fraud detection," *IAJIT Journal*, vol. 20, no. 2, pp. 150–160, 2023. [Online]. Available: <https://ccis2k.org/iajit/images/year2023/No.2/20341.pdf>
- [13] I. Ibraheem et al., "LSTM-Based Fraud Detection," *ResearchGate*, 2024. [Online]. Available: <https://www.researchgate.net/publication/377830394>

- [14] Y. H. Muhakabartay, "BiLSTM and BiGRU for fraud detection," ResearchGate, 2020. [Online]. Available: <https://www.researchgate.net/publication/340968896>
- [15] S. Lee et al., "Combining CNN, GRU, and MLP architectures for fraud detection," Journal of Big Data, Springer, 2024. [Online]. Available: <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-01048-8>
- [16] M. Ahmed et al., "Enhancing Credit Card Fraud Detection: A Neural Network and SMOTE Integrated Approach," ResearchGate, 2024. [Online]. Available: <https://www.researchgate.net/publication/378583709>