Comprehensive Report on Machine Learning Applications in Fraud Detection

Your Name

November 28, 2024

Abstract

This report investigates state-of-the-art machine learning techniques for fraud detection, with a focus on challenges posed by imbalanced datasets and overlapping class distributions. Drawing insights from extensive literature, including frameworks like DAEGAN [1] and CS-OCAN [2], we propose a hybrid fraud detection model. This work provides a comprehensive overview of advanced methodologies, such as Generative Adversarial Networks (GANs), autoencoders, and ensemble learning, and demonstrates how these can be combined to enhance detection rates while maintaining efficiency.

Contents

1 Introduction

Fraud detection is critical in various industries, especially finance, where billions are lost annually due to fraudulent activities. Traditional rule-based systems have proven inadequate, prompting a shift toward machine learning (ML)-based solutions. However, challenges such as imbalanced datasets and adversarial attacks persist [3].

2 Background

Fraud detection traditionally involved rule-based and statistical techniques. The adoption of machine learning has introduced:

- **Supervised Learning:** Algorithms like XGBoost and CatBoost effectively handle structured transaction data [4].
- **Unsupervised Learning:** One-class approaches like OCAN use benign data to detect anomalies [5].
- **GANs:** Models like DAEGAN address data imbalance and feature learning [1].

3 Literature Review

3.1 Addressing Data Imbalance

Imbalanced datasets skew predictions toward the majority class. Techniques such as SMOTE, B-SMOTE, and GANs have been explored:

- **DAEGAN**: Combines dual autoencoders with GANs to balance datasets and improve feature representation [1].
- **TAnoGAN**: Adapts GANs for time-series anomaly detection, demonstrating effectiveness in limited datasets [6].

3.2 One-Class Classification

One-class classifiers are robust for datasets with minimal fraud samples:

- **CS-OCAN**: Integrates GANs with autoencoders to learn robust class-specific representations [2].
- **Improved Bi-GAN**: Proposes a simplified loss function for network intrusion detection [7].

3.3 Advanced Anomaly Detection

Reconstruction-based methods and contrastive learning offer new perspectives:

- **Contrastive GANs**: Combine data augmentation and contrastive loss to enhance generalization [8].
- **Autoencoders**: Reconstruction errors identify deviations from normal behavior [9].

4 Proposed Framework

The proposed hybrid framework incorporates:

1. **Data Preprocessing:** Noise removal and feature scaling.
2. **Synthetic Data Generation:** GANs balance datasets by synthesizing fraud samples.
3. **Feature Extraction:** Autoencoders capture latent features.
4. **Classification:** Ensemble classifiers like CatBoost ensure robust predictions [4].

5 Discussion

This framework addresses:

- **Imbalanced Datasets:** GANs effectively generate minority class samples.
- **Feature Representation:** Autoencoders improve feature generalization.
- **Scalability:** Ensemble methods enhance model performance.

6 Conclusion

This report synthesizes advancements in machine learning for fraud detection, highlighting the potential of hybrid frameworks. Future research should focus on real-time deployment and adversarial robustness.

References

[1] E. Wu, H. Cui, and R. E. Welsch, "Dual Autoencoders Generative Adversarial Network for Imbalanced Classification Problem," *IEEE Access*, vol. 8, pp. 91265–91275, 2020.

[2] H. Peng, J. Zhao, L. Li, Y. Ren, and S. Zhao, "One-Class Adversarial Fraud Detection Nets with Class Specific Representations," *IEEE Transactions on Network Science and Engineering*, pp. 1–12, 2023.

[3] S. N. Kalid, K.-C. Khor, K.-H. Ng, and G.-K. Tong, "Detecting Frauds and Payment Defaults on Credit Card Data Inherited With Imbalanced Class Distribution and Overlapping Class Problems: A Systematic Review," *IEEE Access*, vol. 12, pp. 23636–23652, 2024.

[4] P. Hajek, M. Z. Abedin, and U. Sivarajah, "Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework," *Information Systems Frontiers*, vol. 25, pp. 1985–2003, Oct. 2023.

[5] P. Zheng, S. Yuan, X. Wu, J. Li, and A. Lu, "One-Class Adversarial Nets for Fraud Detection," June 2018. arXiv:1803.01798 [cs].

[6] M. A. Bashar and R. Nayak, "TAnoGAN: Time Series Anomaly Detection with Generative Adversarial Networks," in *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*, (Canberra, ACT, Australia), pp. 1778–1785, IEEE, Dec. 2020.

[7] W. Xu, J. Jang-Jaccard, T. Liu, F. Sabrina, and J. Kwak, "Improved Bidirectional GAN-Based Approach for Network Intrusion Detection Using One-Class Classifier," 2022.

[8] J. Miao, H. Tao, H. Xie, J. Sun, and J. Cao, "Reconstruction-based anomaly detection for multivariate time series using contrastive generative adversarial networks," *Information Processing & Management*, vol. 61, p. 103569, Jan. 2024.

[9] H. Fanai and H. Abbasimehr, "A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection," *Expert Systems with Applications*, vol. 217, p. 119562, May 2023.