Credit Card Fraud Detection: A Comparative Analysis of Traditional Machine Learning and Neural Network Approaches

Abstract:

Credit card fraud is a big concern in the financial industry -- as fraudulent transactions cause substantial financial loss to both consumers and businesses. Fraud methods have evolved in a way that has made detection very challenging, creating the need for advanced systems that can detect fraud in real-time. This project, aligned with the deep learning theme, aims to play a role in this challenge by developing and comparing various machine learning models for credit card fraud detection, with a focus on both traditional methods and a neural network architecture.

To provide a comprehensive evaluation, this project utilizes two distinct datasets. The first is the Kaggle European Credit Card Fraud dataset, which contains transaction data from European cardholders over a two-day period in 2013. The dataset is highly imbalanced, with only 0.172% of its 284,807 transactions labeled as fraudulent, presenting a significant challenge for machine learning models. Furthermore, the "time" feature in this dataset does not represent meaningful temporal sequences, making it less suitable for sequence-based models such as Long Short-Term Memory (LSTM) or Gated Recurrent Units (GRU).

The second dataset, **PaySim**, simulates mobile money transactions between users, agents, and merchants in a financial ecosystem. PaySim, like the Kaggle dataset, is also highly imbalanced, though its fraud patterns differ, simulating the behaviors seen in mobile money systems. PaySim also includes a "time" feature, which, while representing the sequence of events, still poses challenges similar to those in the Kaggle dataset because it lacks true temporal dependencies between individual accounts or users.

The key research questions guiding this project are:

1. How do traditional machine learning models, such as XGBoost and random forest, compare with neural network architectures like multi-layer perceptrons (MLPs) in detecting credit card and mobile money fraud?
2. How can we effectively manage class imbalance across both datasets to enhance model performance?
3. How do the complexity and computational efficiency (e.g., training time, inference speed) of traditional machine learning models compare to neural network architectures for fraud detection?

To address these questions, the project will focus on three models: **XGBoost**, **random forest**, and **MLPs**. **XGBoost** is an ensemble learning method known for its high accuracy and performance on imbalanced datasets, making it a strong candidate for both datasets. **Random forest**, a traditional ensemble method, offers robustness and interpretability, particularly in handling feature interactions, which makes it useful for identifying patterns in fraud detection. The inclusion of **MLPs**, a feedforward neural network, will provide a neural network-based perspective for comparison, offering insights into how non-tree-based methods perform relative to traditional models.

While one of the studies being compared (Mienye et al., 2024) utilizes LSTMs and GRUs, which are effective for datasets with clear temporal dependencies, this project will focus on models that are more suited to the structure of these particular datasets, where the time variable does not represent continuous sequences for individual cardholders. Techniques to address class imbalance such as SMOTE, will also be explored to improve model performance.

Results will be compared against the findings of Mienye et al. (2024), and Divakar et al. (2019), while possibly introducing new insights by focusing on models more appropriate for non-sequential data. While there are few studies utilizing the PaySim dataset, comparisons will be drawn from broader research in mobile payment fraud detection, which shares relevant characteristics with PaySim.

This project will be implemented in Python, using scikit-learn for traditional machine learning models and TensorFlow/Keras for neural network models. Data manipulation and visualization will be handled using pandas, numpy, matplotlib, and seaborn.

References:

Divakar & Chitharanjan (2019) Divakar K, Chitharanjan K. Performance evaluation of credit card fraud transactions using boosting algorithms. *International Journal of Electronics Communication and Computer Engineering (IJECCE)* 2019;10(6) 2249–071X.

Mienye, I. D., & Jere, N. (2024). Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. IEEE Access, 12, 96893–96910.

Spann, Delena D. Fraud Analytics : Strategies and Methods for Detection and Prevention. 1st edition. Hoboken, New Jersey: Wiley, 2014. Print.

Raschka, S., & Mirjalili, V. (2019). Python machine learning : machine learning and deep learning with python, scikit-learn, and tensorflow 2