Bellevue University

Credit Card Fraud Detection

Ashley Mayo

Final Project

February 26th, 2025

DSC 630: Predictive Analytics

Professor Farley

Introduction

Credit card fraud is a growing concern in today’s digital economy, costing financial institutions billions of dollars annually and weakening consumer confidence in online transactions (Nguyen et al., 2020). Detecting fraudulent transactions efficiently is particularly difficult due to their rarity in large datasets, leading to high false negative rates that allow fraudulent activity to go undetected (Brown & Williams, 2022). Traditional fraud detection methods struggle with this imbalance, making it necessary to explore advanced machine learning techniques to improve detection accuracy while minimizing false positives.

This project aims to develop a predictive fraud detection model using the Credit Card Fraud Detection Dataset from Kaggle. The dataset comprises 284,807 anonymized transactions, with only 492 identified as fraudulent, representing a severe class imbalance of 0.17% fraudulent transactions. To address this challenge, this study leverages Principal Component Analysis (PCA) features, time-based transaction data, and amount-related insights to build a robust fraud detection system. Given its complexity and real-world relevance, this dataset serves as an ideal foundation for testing advanced machine learning techniques.

The objective of this project is to improve fraud detection accuracy by utilizing the Synthetic Minority Oversampling Technique (SMOTE) to balance the dataset and testing multiple classification models, including Logistic Regression, Random Forest, and LightGBM. By developing a model that effectively identifies fraudulent transactions without excessive false positives, this research aims to contribute to the development of real-time fraud detection solutions that protect consumers and financial institutions from financial losses.

Summary of Methods and Results

Exploratory data analysis (EDA) revealed important transaction trends. A bar chart confirmed the extreme class imbalance, underscoring the necessity for class balancing techniques. A box plot of transaction amounts showed that fraudulent transactions tend to cluster around specific values, a trend consistent with findings by Smith and Patel (2021), who reported that fraudsters often attempt to mimic typical spending patterns to avoid detection. A histogram of transaction frequency over time revealed that fraudulent transactions peak during certain hours, suggesting that fraud is more prevalent at specific times. To further investigate temporal patterns, a time-series plot of fraudulent transaction rates was generated, highlighting spikes in fraudulent activity during off-peak hours when detection measures might be less stringent.

Since the dataset had no missing values, data preprocessing involved feature standardization and class balancing. The Synthetic Minority Oversampling Technique (SMOTE) was applied to the training dataset to mitigate class imbalance. The dataset was split into an 80% training set and a 20% testing set. Under-sampling was also tested but was found to reduce data variability, making SMOTE the preferred approach. To improve model interpretability, feature correlation analysis was conducted, revealing that certain PCA-transformed features exhibited strong relationships with fraudulent activity, further guiding feature selection.

This project employed three machine learning models: Logistic Regression, Random Forest, and LightGBM. Logistic Regression served as a baseline model due to its simplicity and interpretability. Random Forest was used for feature importance analysis, while LightGBM, a gradient boosting algorithm, was chosen as the primary model for classification. Gradient boosting algorithms have been found to outperform traditional machine learning models in fraud detection by effectively handling class imbalances and capturing complex data patterns (Brown & Williams, 2022). To fine-tune model performance, hyperparameter tuning was conducted using grid search and cross-validation, optimizing parameters such as the learning rate, max depth, and number of estimators for LightGBM.

Model evaluation was based on precision, recall, and F1-score to ensure a balance between fraud detection accuracy and minimizing disruptions to legitimate transactions. LightGBM significantly outperformed Logistic Regression and Random Forest, achieving a higher recall rate while maintaining reasonable precision. Feature importance analysis identified V12, V14, and V17 as the most influential features in detecting fraudulent transactions, with transaction amount also playing a significant role. A Precision-Recall curve confirmed that LightGBM effectively balances fraud detection performance. A confusion matrix was generated to further assess the model's classification accuracy, revealing a substantial reduction in false negatives compared to the other models. Additionally, Receiver Operating Characteristic (ROC) curves were plotted to compare model performance in terms of overall classification ability.

To better understand model behavior, SHAP (SHapley Additive exPlanations) values were computed for LightGBM, providing insight into individual feature contributions to fraud classification. This analysis demonstrated that certain PCA features had nonlinear interactions that significantly influenced classification decisions, reinforcing the value of using an advanced boosting algorithm. The findings suggest that leveraging both engineered transaction features and PCA-transformed data enhances fraud detection accuracy and robustness.

Conclusion

This study demonstrated that LightGBM was the most effective model for detecting fraudulent credit card transactions when combined with SMOTE for class balancing. The results indicated that implementing real-time fraud monitoring using LightGBM could significantly reduce fraudulent transactions without negatively impacting legitimate users (Smith & Patel, 2021). Financial institutions could further enhance fraud detection by integrating dynamic thresholding techniques to adjust fraud detection sensitivity based on time-of-day patterns and transaction amounts (Brown & Williams, 2022).

While the model performs well, further improvements should be explored. Future research would involve deep learning techniques such as autoencoders for anomaly detection, ensemble models combining LightGBM and Random Forest for improved accuracy, and fairness-aware machine learning to ensure models do not disproportionately impact specific customer demographics. Ethical considerations remain critical, as excessive false positives can inconvenience customers, while false negatives can lead to financial losses. Optimizing fraud detection models requires continuous monitoring, threshold tuning, and bias mitigation strategies to ensure fairness and effectiveness.

By integrating these improvements, fraud detection systems can achieve greater accuracy, efficiency, and fairness, ultimately reducing financial fraud and enhancing consumer trust in digital transactions.

References

Brown, T., & Williams, K. (2022). Fraud detection in financial transactions using machine learning. Computational Finance Review, 4(2), 12-27.

Nguyen, H., Gupta, S., & He, X. (2020). Machine learning approaches for credit card fraud detection. Journal of Financial Data Science, 2(3), 45-62.

Smith, J., & Patel, R. (2021). A comparative study of credit card fraud detection algorithms. International Journal of Artificial Intelligence & Machine Learning, 6(1), 89-105.