CREDIT CARD FRAUD DETECTION

COMS W-4995 AML Project

INTRODUCTION

Background and Context:

In the intricate landscape of financial transactions, credit card fraud stands as a persistent threat, marking the unauthorized use of credit cards for purchases or access to funds. The gravity of this criminal activity is underscored by a disconcerting reality – a global surge of over 10% in card fraud losses from 2020 to 2021, as outlined in the latest report. This alarming escalation highlights the pressing need for a sophisticated and precise model to combat the rising tide of fraudulent transactions. Fraudulent activities are inherently elusive, presenting a formidable challenge for any model aiming to discern them accurately. The rarity of such transactions adds another layer of complexity, demanding a nuanced approach to ensure the model learns effectively. Flagging an excessive number of transactions can incur significant financial repercussions, creating inefficiencies and inconveniences for cardholders and financial institutions alike. Conversely, overlooking or misclassifying a fraudulent transaction as legitimate poses an even greater risk, potentially leading to substantial financial losses and eroding trust in the security of financial systems. In this report, we delve into the multifaceted challenges posed by credit card fraud, emphasizing the critical role of an accurate and adaptive model in mitigating these risks. As we navigate the intricate realm of financial security, it becomes evident that the stakes are high, and the pursuit of precision is non-negotiable.

Dataset Used:

The dataset utilized for this analysis is sourced from Kaggle and encompasses a simulated credit card transaction timeline spanning from January 1, 2019, to December 31, 2020. This comprehensive dataset encompasses transactions conducted by 1000 customers across a network of 800 merchants. A notable characteristic of the dataset is its inherent imbalance, with a mere 0.6% of observations corresponding to the minority class, representing fraudulent transactions. This skewed distribution introduces a significant challenge in constructing a predictive model that effectively identifies and addresses the nuances of fraud cases amidst the predominantly non-fraudulent majority.

Data exploration and Feature Engineering:

In our initial data exploration, we found multiple features related to geographical location. To avoid multicollinearity, all but the features representing latitude and longitude were dropped (see Fig. 1 in the "Supplemental Images" file). We also observed that most of the events occurred between 10 PM and 3 AM (see Fig. 2), so we added a binary feature to indicate if the transaction fell within this time period. Additional feature engineering was performed on data that was found to be skewed, namely the features representing transaction amount and population. This was done by performing log transformations, which yielded multimodal normal distributions as illustrated in Fig. 3 and Fig. 4.

METHODOLOGY

Models Used:
In our pursuit of effective credit card fraud detection, we employed a diverse set of models. The Decision Tree mapped complex decision boundaries, KNN detected local patterns, and SVM identified optimal hyperplanes. Logistic Regression served as a baseline, while Random Forest aggregated decision trees for robustness. Light GBM and XGboost offered efficient gradient boosting, ADABoost combined weak learners, and the HistGradient Boost Classifier utilized histogram-based learning. A Neural Network with dropout regularization provided a sophisticated architecture. All these models were applied to the dataset to determine their prediction capabilities.

Data Handling:
To address the highly skewed dataset, we implemented oversampling, undersampling, SMOTE, and adjusted class weights. Oversampling generated synthetic instances of the minority class, undersampling reduced majority class instances, and SMOTE created synthetic instances through interpolation. Adjusted class weights were applied to prioritize the minority class during training.

Accuracy Metrics:
In evaluating model performance, precision measured the accuracy of positive predictions, recall assessed the ability to capture actual positives, and AUC provided a comprehensive measure of the model's ability to distinguish between positive and negative instances.

MODEL RESULTS

In hopes of building an optimal credit card fraud detection model, a thorough exploration of various techniques was undertaken to address the challenges posed by a highly imbalanced dataset. After rigorous experimentation, the final selection comprises a diverse ensemble of models, each tailored to provide a robust solution. All models achieved a notable feat by securing high AUC ROC scores, surpassing the 87% threshold, indicative of their effective discrimination between positive and negative classes.

Among the models, two emerged with distinct strengths, each excelling in specific metrics that cater to different aspects of fraud detection.
The standout performer, showcasing superior performance across various metrics, is the Light GBM with Balanced Weight (see Fig. 5). The Light GBM model achieved a remarkable recall score of 0.717 and a precision of 0.693 on the test dataset. Its AUC-ROC score of 0.858 signifies robust discriminative capabilities, while the F1-Score of 0.705 showcases a balanced trade-off between precision and recall. This model proved particularly adept at prioritizing the identification of fraudulent transactions while maintaining a reasonable level of precision.

Turning to the insights gleaned from the SHAP summary plots in Fig. 6, certain features stand out prominently. The feature Transaction Amount emerges as the most impactful, with increasing transaction amounts correlating with a higher likelihood of predicting a fraudulent transaction (Class 1). Additionally, the feature Transaction Category demonstrates substantial positive and negative impacts on Class 1 predictions, emphasizing the importance of transaction categories in fraud detection. Lastly, Risky Time ranks as the third most important, underscoring the effectiveness of encoding risky time in capturing relevant patterns for fraud detection.

These findings illuminate the critical role of transaction amount, transaction category, and time-related features in determining the likelihood of credit card fraud. The models' adept utilization of these features enhances their interpretability and provides actionable insights for refining fraud detection strategies in practical applications.

CONCLUSIONS

In the realm of credit card fraud detection, the presented comprehensive analysis underscores the critical need for precision and adaptability in combating the escalating threat of fraudulent transactions. The selection of Light GBM with Balanced Weight under the high recall criterion highlights its superiority in effectively identifying fraudulent transactions. Moving forward, the calibration of the Light GBM model using isotonic regression further enhances its reliability in reflecting the actual likelihood of fraud. Calibration ensures precision in risk assessment, aids in threshold selection, aligns with compliance standards, and facilitates effective model evaluation.

The SHAP summary plots provide valuable insights into feature importance, reaffirming the impact of transaction amount and transaction category on fraud predictions. In the evaluation over the test dataset, the Light GBM model emerges as the best in terms of F1-score, achieving a commendable balance between recall and precision. This robust performance, coupled with meticulous data handling techniques such as oversampling and adjusted class weights, positions the Light GBM model as a reliable tool for identifying fraudulent activities while minimizing false positives. As we navigate the complex landscape of financial security, the outcomes of this analysis provide a strong foundation for deploying the Light GBM model in credit card fraud detection following the procedures of the flowchart depicted in Fig. 7. Further validation and refinement on unseen datasets remain imperative for the seamless integration of the Light GBM model into real-world financial systems, enhancing resilience against the ever-evolving landscape of fraudulent transactions.

SUPPLEMENTAL IMAGES

Credit Card Fraud Detection

COMS - W4995 AML Project

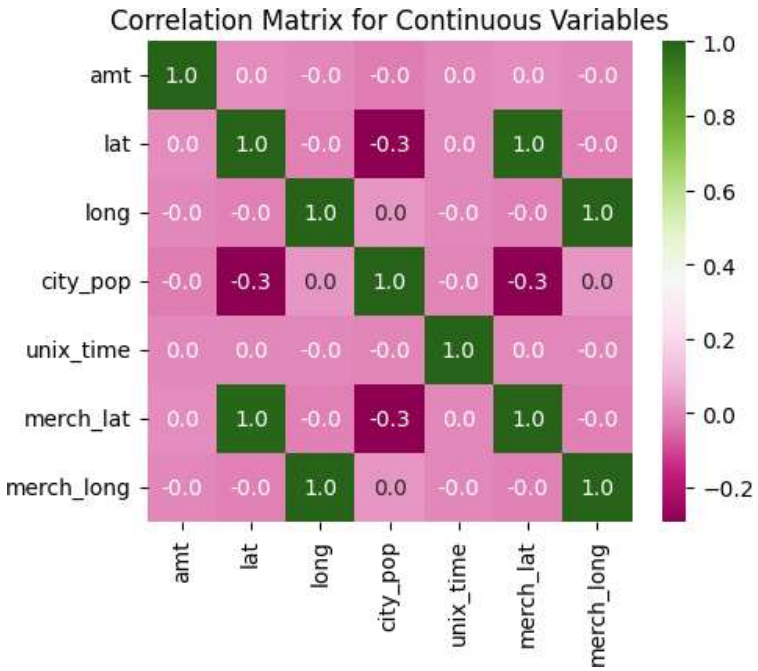

Figure 1

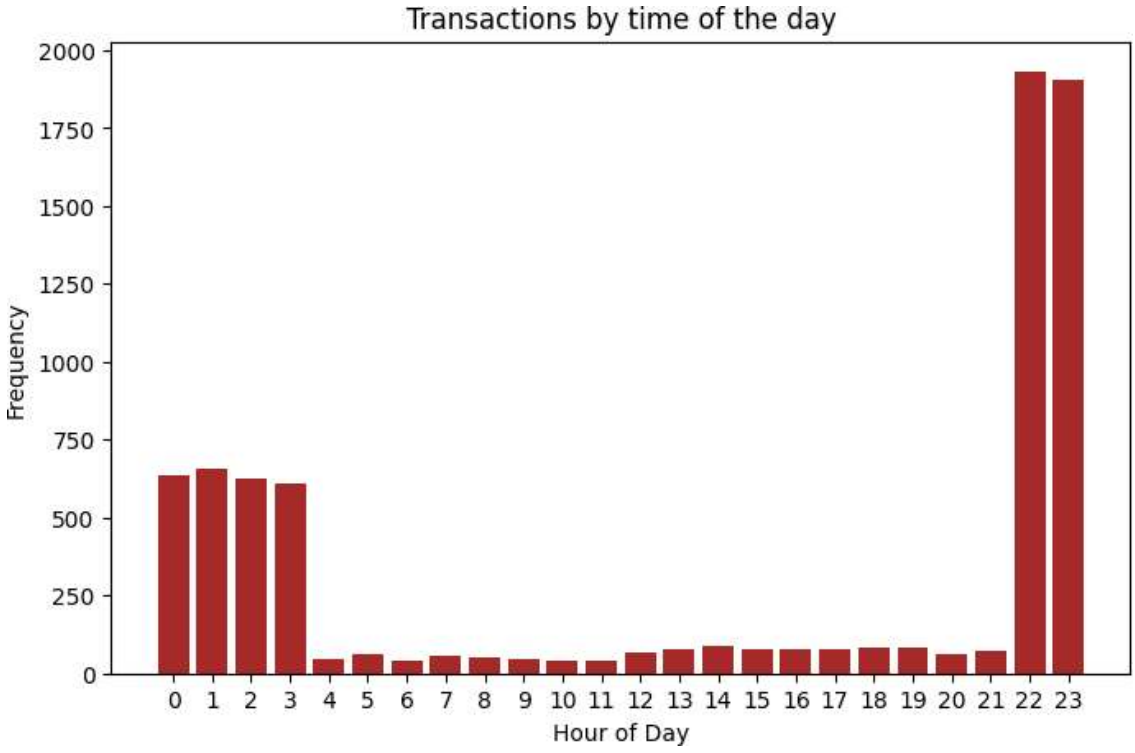

Figure 2

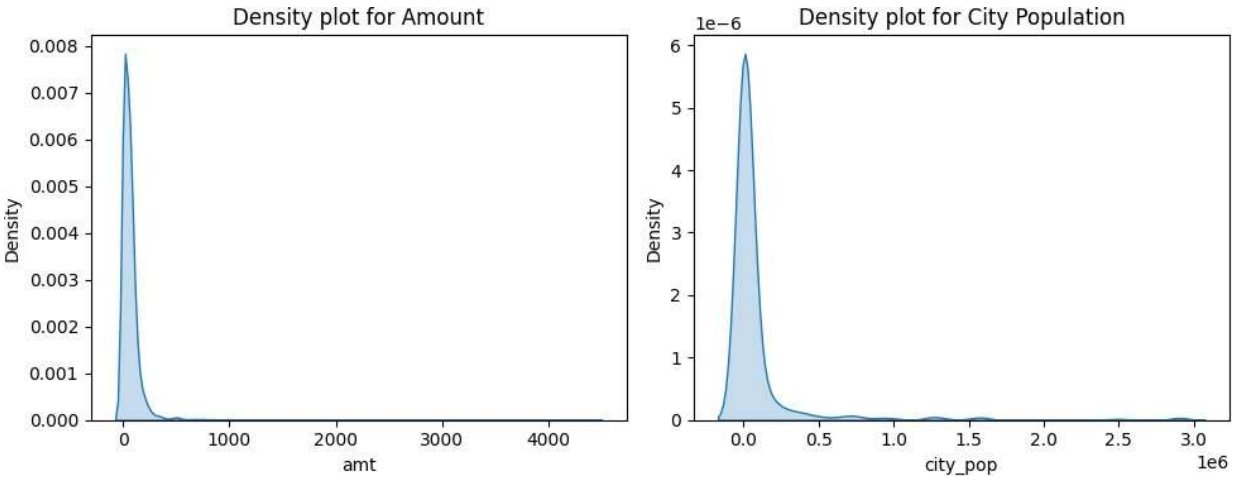

Figure 3: Density plots before log transformation

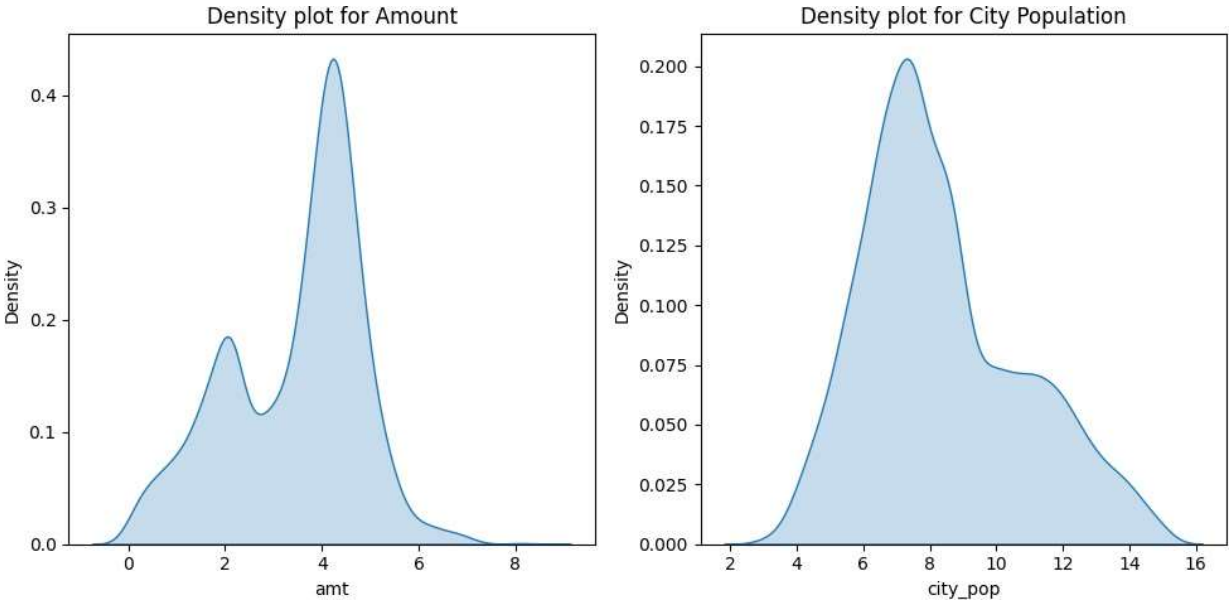

Figure 4: Density plots after log transformation

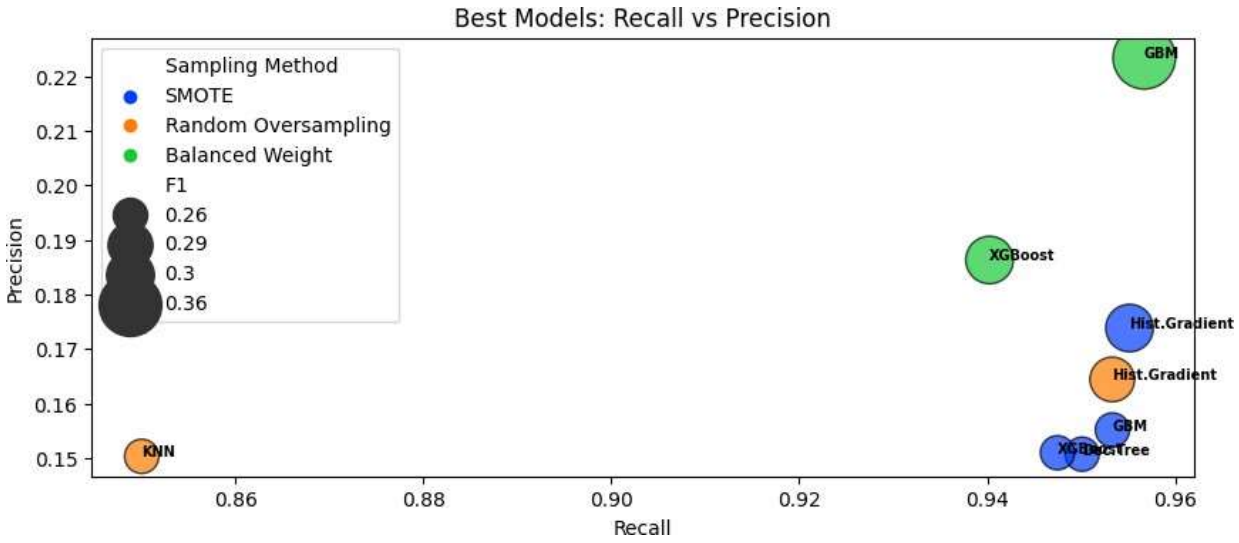

Figure 5: Choose models with high recall, at expense of precision.

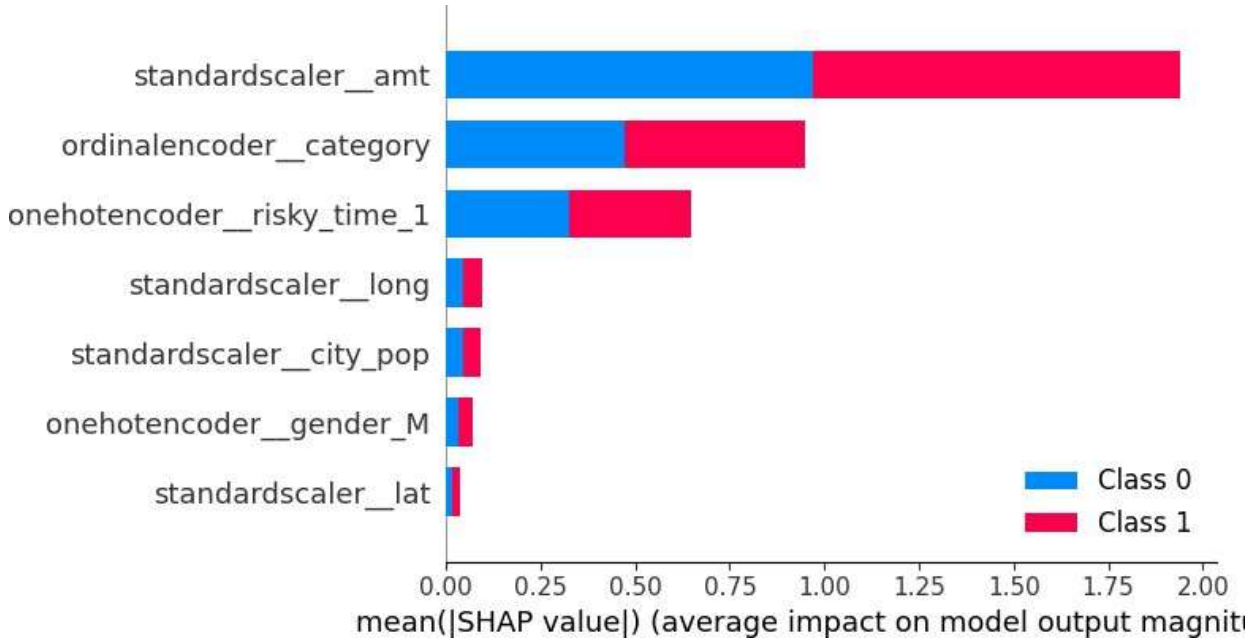

Figure 6: SHAP summary plot

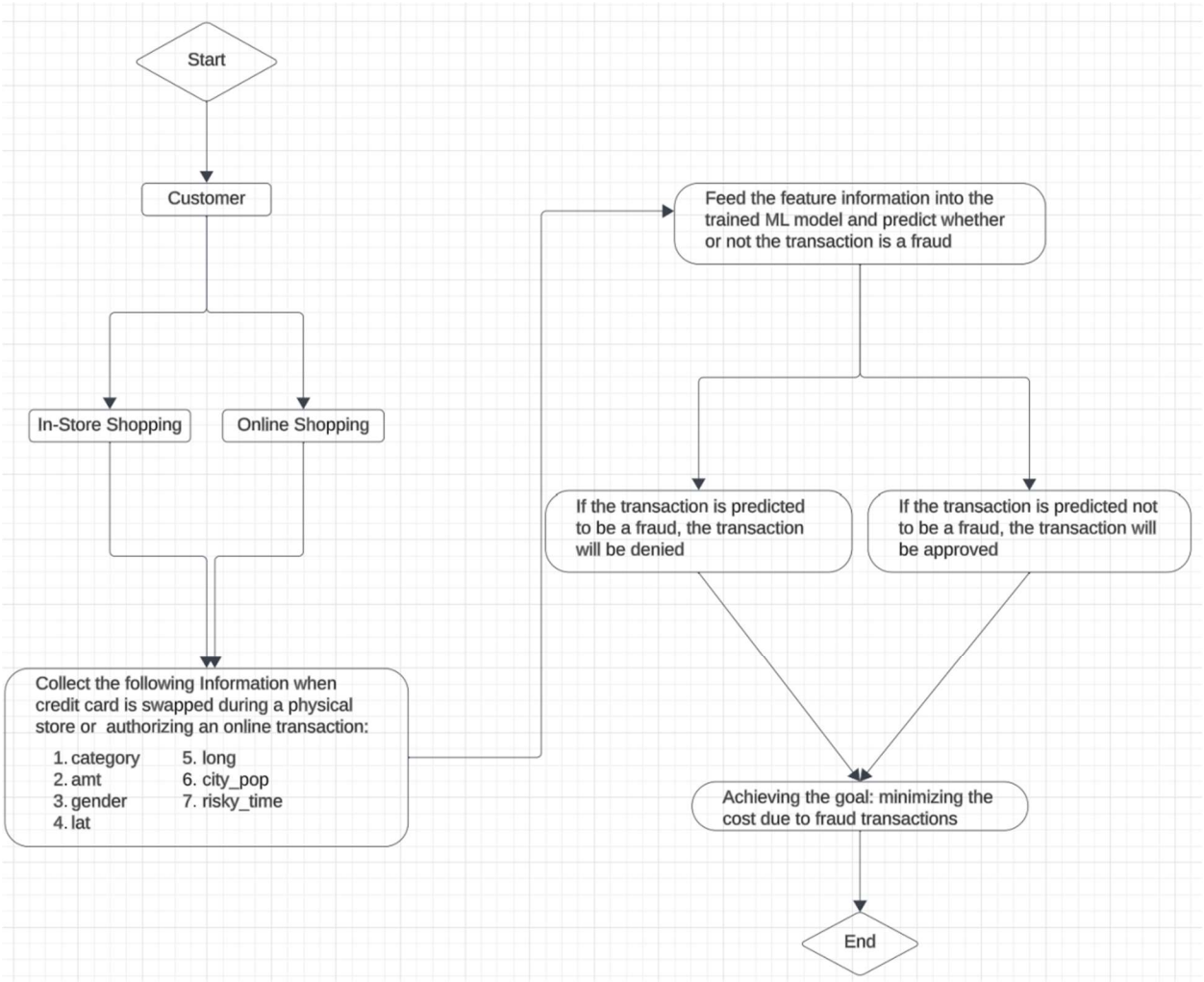

Figure 7: Flowchart for use in business setting