FraudBot

Team 20: Karim Chmayssani, Blake Milstead, & Ryan Franqui

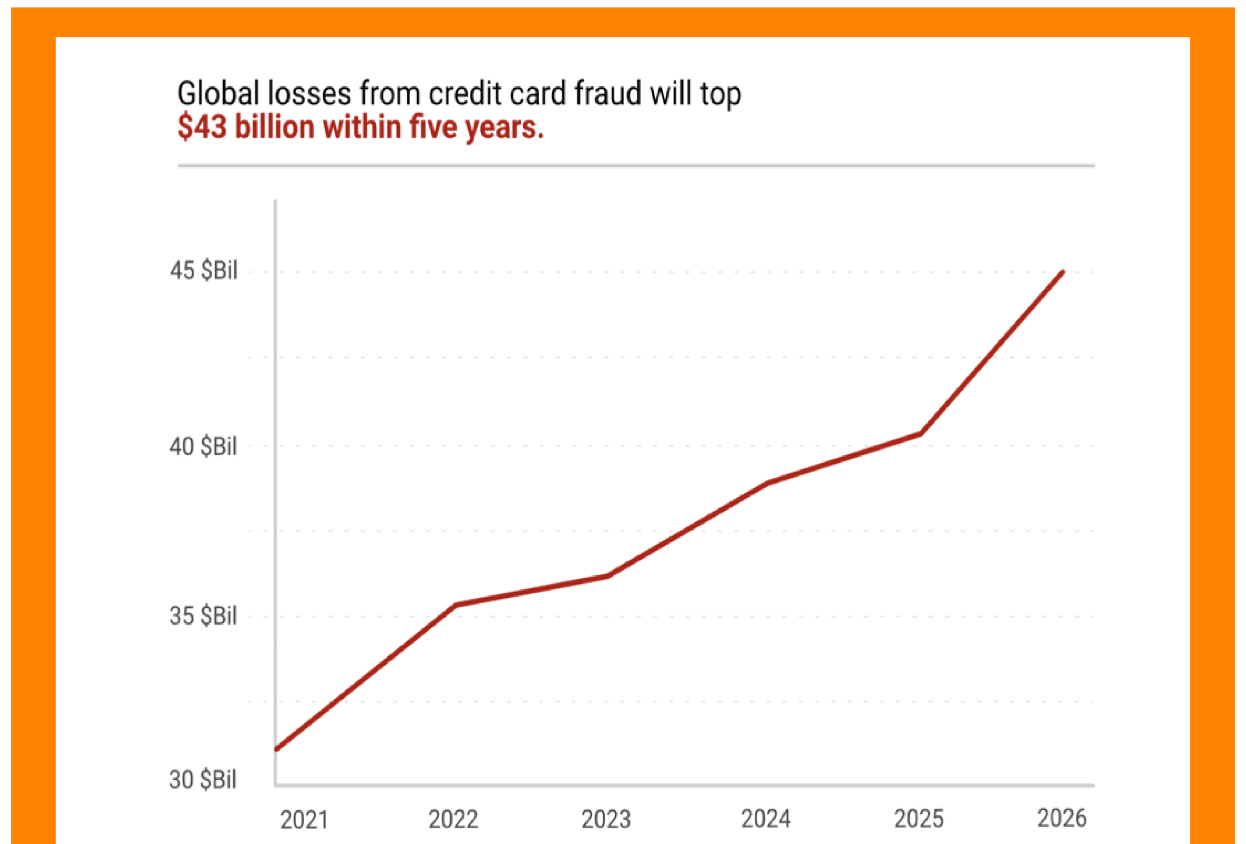
THE UNIVERSITY OF TENNESSEE KNOXVILLE

Abstract

Fraud detection systems play a pivotal role in securing financial systems and reducing risks associated with illicit transactions. This study presents a comprehensive Python-based fraud detection pipeline, designed with modularity and scalability in mind. The pipeline integrates preprocessing, feature selection, hyperparameter tuning, k-fold cross-validation, and model management, leveraging cutting-edge machine learning techniques. Preliminary results demonstrate the pipeline's capability to achieve high precision, recall, and ROC-AUC scores on imbalanced datasets, highlighting its potential for real-world deployment in fraud detection scenarios. This poster discusses the pipeline's architecture, key challenges in implementation, and future directions, including deployment in production environments.

Motivation

- Credit card fraud affects **1 in 4** of all cardholders in previous years.
- Human verification of purchases is made impossible by quantity of transactional data

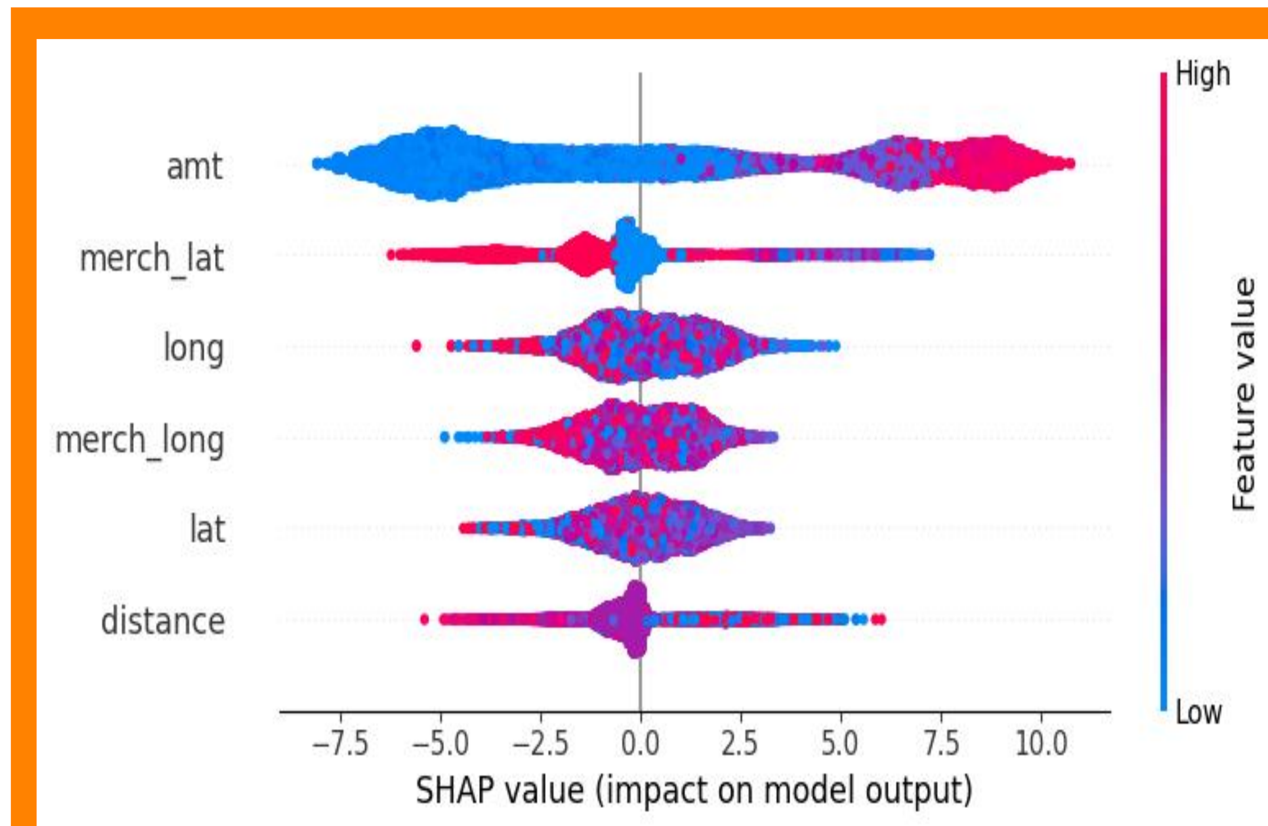


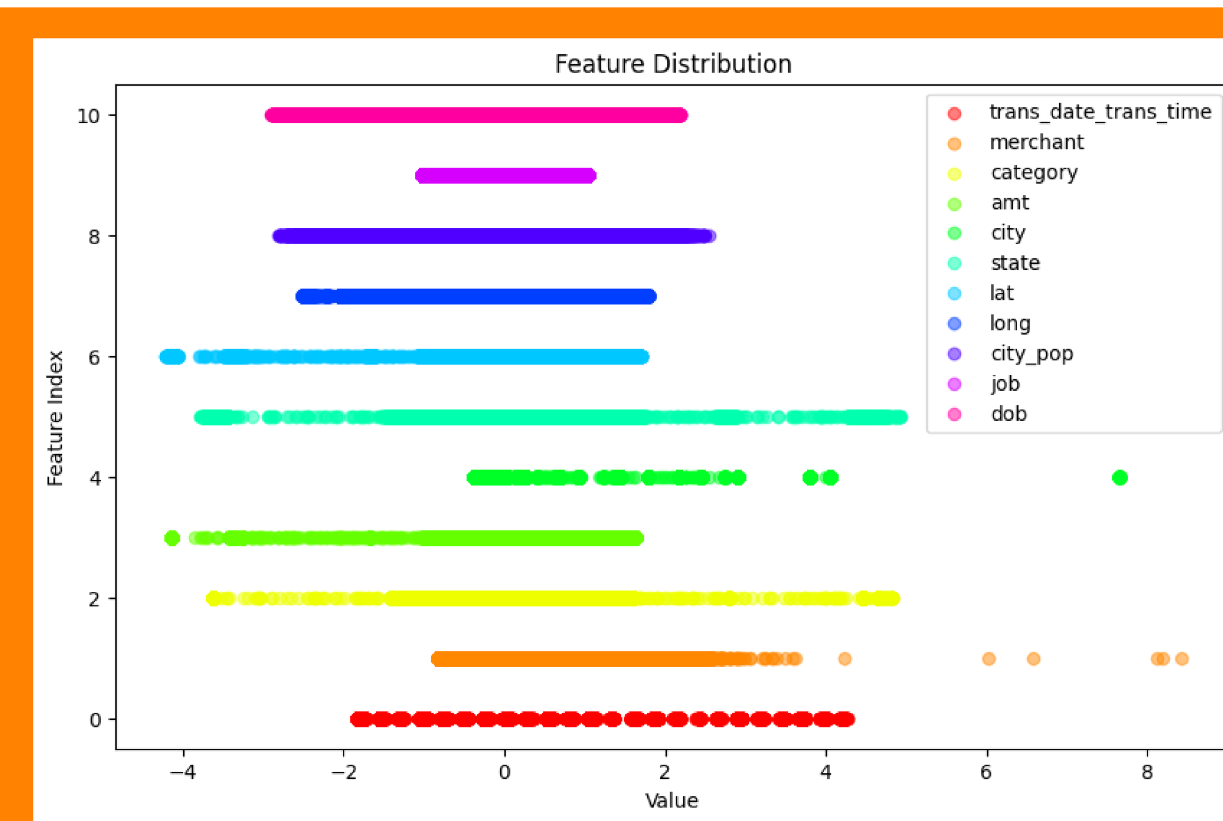
Source: https://merchantcostconsulting.com/

- The faster fraud can be detected, the more damage can be minimized. By improving the way that fraud is recognized, we can potentially protect **millions** of clients' personal and business financial assets.

Methodology

Binary classification problems with unbalanced datasets are best validated using metrics such as recall, precision, and f1-score, as highlighted in [1], [2]. We engineered new features using the dataset, including a fraud risk encoding and a Euclidean distance between the merchant and consumer. The data is then preprocessed by filling in missing values with imputation and classes are balanced with SMOTE.

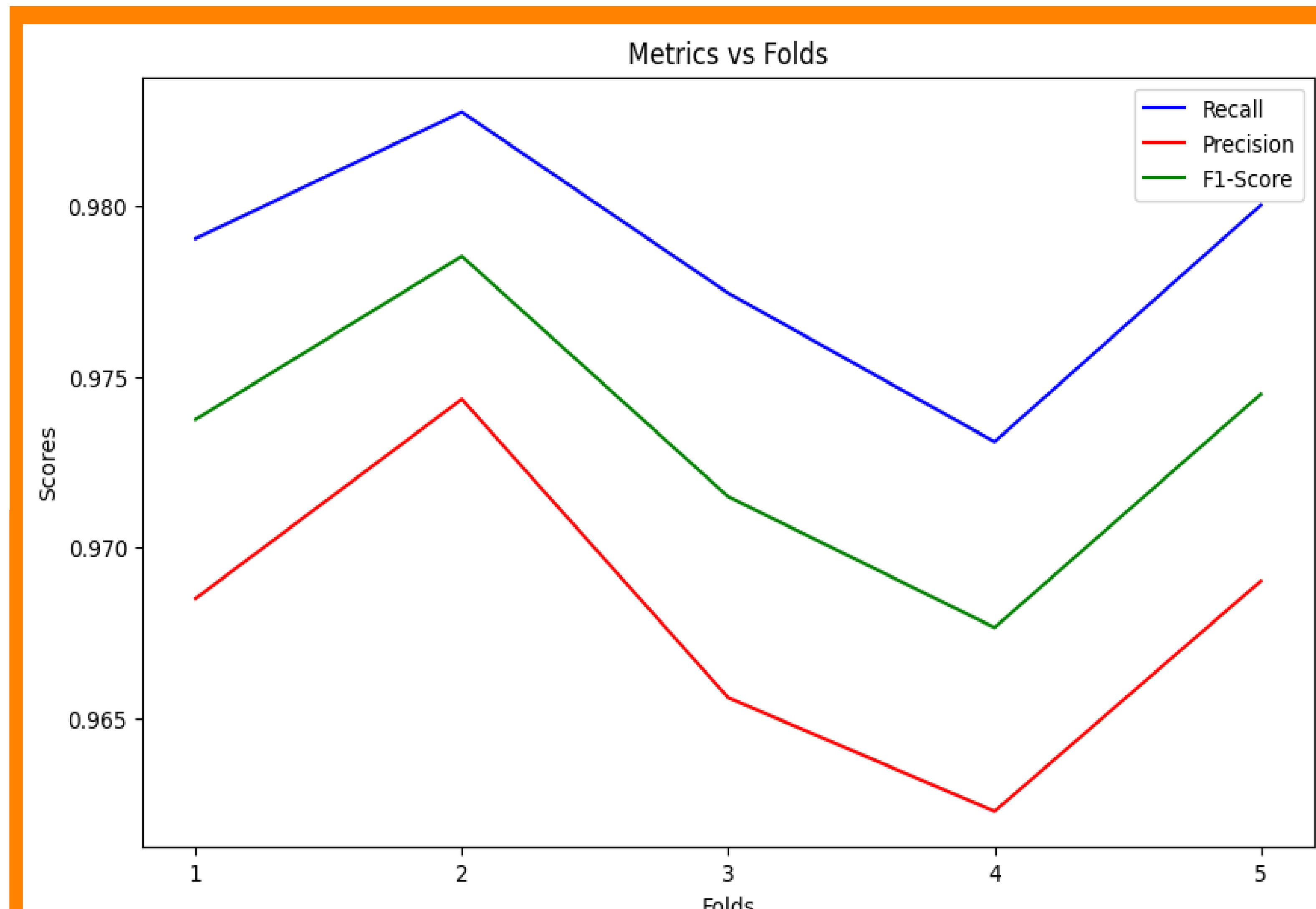




The model itself employs the ensemble learning method XGBClassifier, utilizing gradient boosting to combine multiple weak learning methods and produce a strong result. Recursive Feature Elimination (RFE) was used to narrow our features, and hyperparameter tuning with RandomSearchCV was conducted to finalize the model parameters. Validation is conducted using k-fold cross-validation.

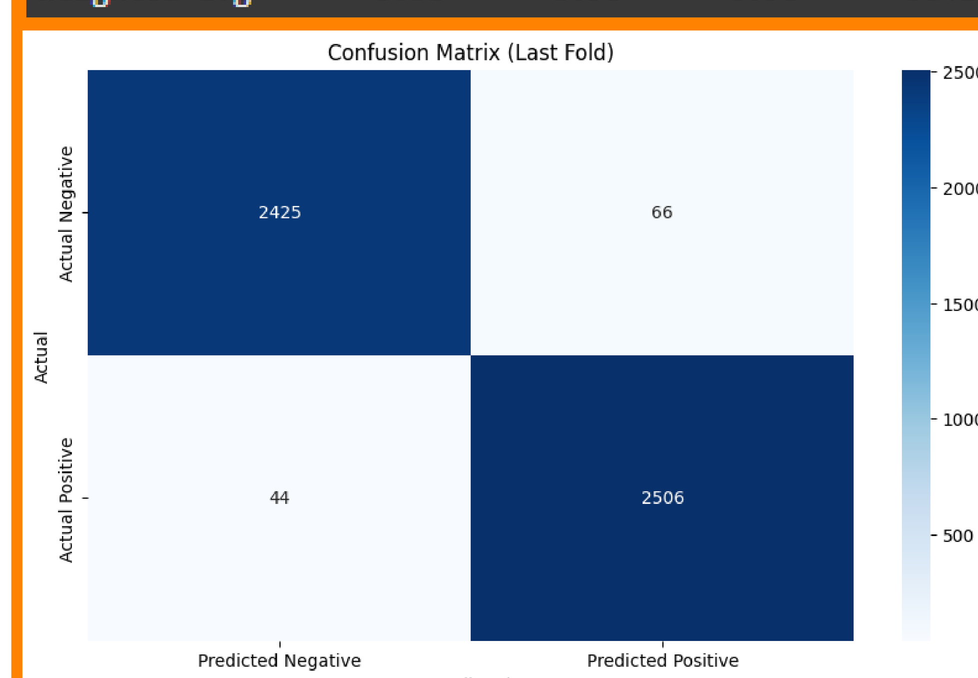
Results

The model produced on the second fold of k-fold cross-validation achieved the best results across all folds. This model has a false negative rate of 1.72% and false positive rate of 2.65%. These results give us confidence that our pipeline can accurately and effectively predict fraudulent transactions.



Classification Report:

	precision	recall	f1-score	support
0	0.98	0.97	0.98	2491
1	0.97	0.98	0.98	2550
accuracy			0.98	5041
macro avg	0.98	0.98	0.98	5041
weighted avg	0.98	0.98	0.98	5041



Lessons Learned

Pre-Tuned Feature Model Results

Classification Report:

	precision	recall	f1-score	support
0	0.97	0.96	0.96	2487
1	0.96	0.97	0.97	2553
accuracy			0.96	5040
macro avg	0.96	0.96	0.96	5040
weighted avg	0.96	0.96	0.96	5040

- Initially, we did not properly normalize or clean our dataset before applying complex transformations to the features. As a result, our initial evaluation using accuracy alone was insufficient to assess whether our model effectively achieved its goal of detecting fraud.
- Recognizing the importance of a holistic evaluation, we shifted to metrics such as recall, precision, and F1-score, which provided a clearer picture of the model's ability to detect fraud and balance false positives and false negatives effectively.
- Finally, we tested the effects of feature selection pre-training with the features of highest importance. However, we found that RFE alone performed better.

Selected References

1. T. Saito and M. Rehmsmeier, "The Precision-Recall Plot Is More Informative than the ROC Plot When Evaluating Binary Classifiers on Imbalanced Datasets," PLOS ONE, vol. 10, no. 3, pp. e0118432, Mar. 2015. [Online]. Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0118432. [Accessed: Dec. 2, 2024].D. J. Hand,
2. Christen, and N. Kirielle, "F*: an interpretable transformation of the F-measure," Machine Learning, vol. 110, no. 3, pp. 451–456, Mar. 2021. [Online]. Available: https://link.springer.com/article/10.1007/s10994-021-05964-1. [Accessed: Dec. 2, 2024].

Acknowledgments

We sincerely thank Dr. Santos for his guidance and expertise, the TAs for their support and feedback, and our classmates for their collaboration and encouragement throughout this project.