IntelliFraud: Bank Account Fraud Detection using Machine Learning

Nukta Bhatia | Emir Talundzic | Piyush Shivrain
Ashish Puri | Jagannath Banerjee | Peter Kovari
CSE 6242 Data & Visual Analytics
Fall 2023

Objectives

Motivation/Introduction

Each year significant costs are incurred by banks due to fraudulent accounts. Tracing back individuals involved in fraudulent activities is challenging, time-consuming, and expensive.

Why is this important?

According to the Federal Trade Commission, institutions incurred a cost of $8.8 billion that was passed to consumers, marking a 44% surge from 2021. Additionally, the FTC reported losses due to identity theft grew from $1.8 in 2019 to $3.3 billion in 2020 and $5.8 billion in 2021.

Our approach

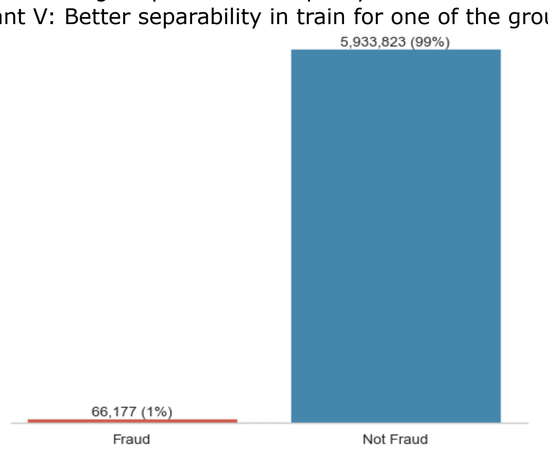
We built Intellifraud, A Fraud Detection System leveraging graph network analysis and machine learning classifiers (Voting & stacking), to identify and prevent fraudulent activities. The system offers users an intuitive interface with detailed statistical analyses. With features like interactive dashboards and comprehensive metric evaluations, inference explanation it ensures efficient and accurate identification of fraudulent patterns in various transactions.
2021.

Dataset

- Bank Account Fraud Dataset Suite (NeurIPS2022)
- Downloaded from Kaggle
- 6 synthetic Variants - 6million rows, 1.4 GB data
- Realistic, robust test bed based on a present-day, real-world dataset for fraud detection
- Each dataset has distinct controlled types of bias
- Extremely low prevalence of positive (fraud) class
- Privacy techniques (noise addition), feature encoding added

Variants

- Base: Samped to represent original dataset
- Variant I: Higher groupsize disparity than base
- Variant II: Higher prevalence disparity than base
- Variant III: Better separability for one of the groups
- Variant IV: Higher prevalence disparity in train
- Variant V: Better separability in train for one of the groups



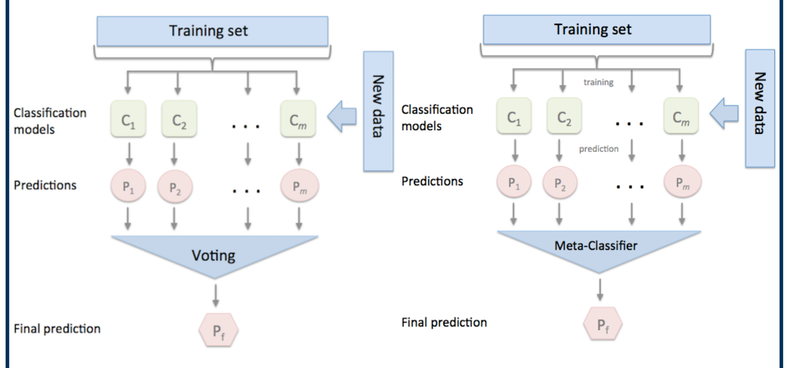
Fraud vs Non-Fraud Count (All Variants)

Sampling Strategy

We undersampled fraudulent vs non-fraudulent data at ratios of 1:1, 1:2, and 1:3 to emphasize learning from the minority class.

Models

- **LGBM Classifier**
  Employs boosting to efficiently train decision trees, optimizing for speed and accuracy
- **AdaBoost Classifier**
  Combines weak learners to create a robust model, assigning more weight to misclassified instances for improved accuracy
- **XGB Classifier**
  Enhances predictive performance by sequentially refining weak learners and minimizing errors
- **Voting Classifier**
  Integrates predictions from multiple algorithms to make collective decisions, enhancing model accuracy through voting mechanism
- **Stacking Classifier**
  Integrates diverse model predictions by training a meta model, leveraging the strengths of individual models for improved overall performance



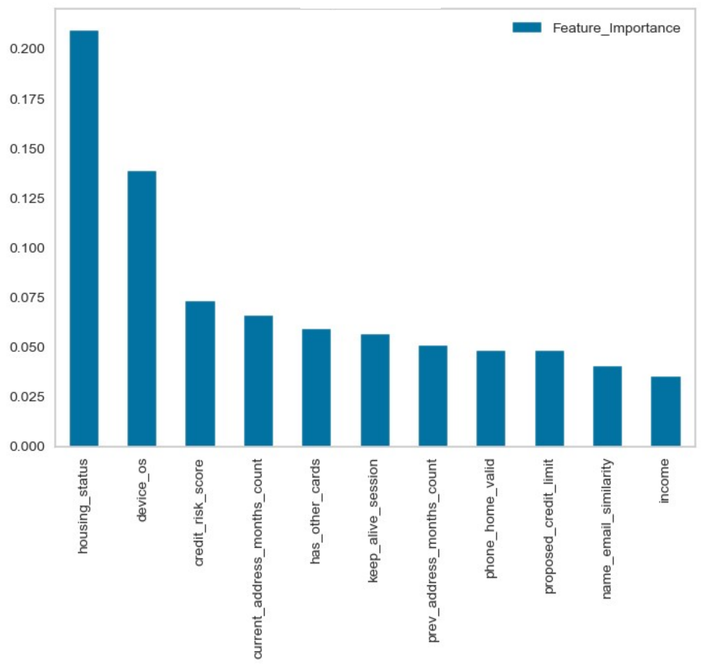
Working of Voting & Stacking Classifiers

Feature Selection

Variance Threshold
Removed low variance feature: device_fraud_count

Pearson's Correlation Matrix
Removed highly correlated feature: velocity_4w

Random Forest Classifier Feature Importance
Top 11 features:
housing_status; device_os; credit_risk_score; has_other_cards; current_address_months_count; keep_alive_session; prev_address_months_count; phone_home_valid; proposed_credit_limit; income; name_email_similarity



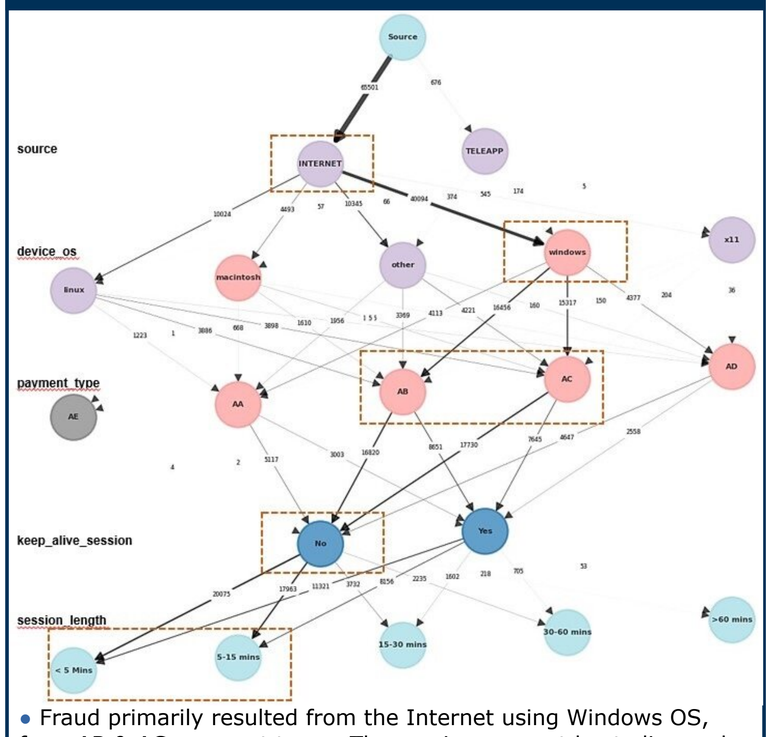
Most Important Features

Implementation

Dataset Partition:
80% Train; Stratified 5-Fold Cross Validation; 20% Test
Tournament-style Procedure:

- **Stage 1:** Graph network visualization to see fraudulent transaction flow through various subsystems
- **Stage 2:** Train variants of the models using sampling strategies
- **Stage 3:** Analyze and provide best performing model using AUC-ROC & F1 Score due to the imbalanced dataset

Results: Stage 1



- Fraud primarily resulted from the Internet using Windows OS, from AB & AC payment types. The session was not kept alive and lasted either 5-15 minutes or less than 5 minutes.

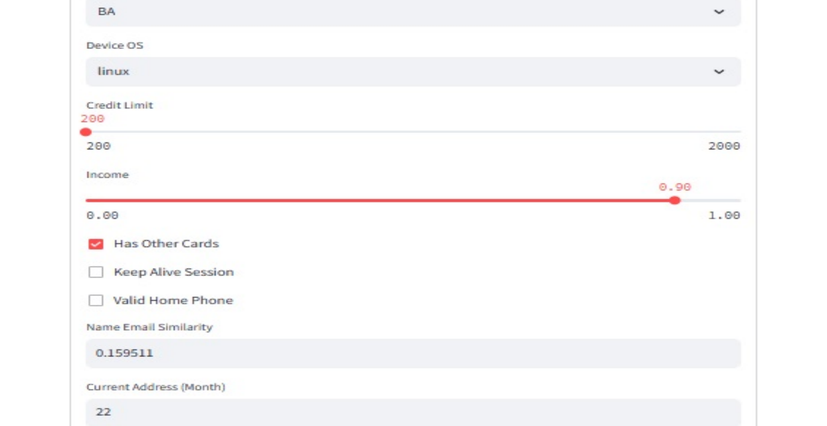
Results: Stage 2

Model Comparison for this Dataset on Test Set

Sample Class (Fraud: Non-Fraud)	Classifier	5 Fold CV Score	Recall (Fraud)	ROC_AUC Score
1:1	XGBClassifier	0.783	0.785	0.784
1:1	AdaBoostClassifier	0.785	0.776	0.785
1:1	LGBMClassifier	0.782	0.783	0.781
1:1	**VotingClassifier**	**0.787**	**0.784**	**0.785**
1:1	**StackingClassifier**	**0.787**	**0.784**	**0.785**
1:2	XGBClassifier	0.797	0.649	0.763
1:2	AdaBoostClassifier	0.797	0.622	0.758
1:2	LGBMClassifier	0.794	0.613	0.753
1:2	VotingClassifier	0.799	0.636	0.761
1:2	StackingClassifier	0.799	0.637	0.761
1:3	XGBClassifier	0.820	0.542	0.730
1:3	AdaBoostClassifier	0.819	0.515	0.724
1:3	LGBMClassifier	0.816	0.496	0.717
1:3	VotingClassifier	0.821	0.527	0.728
1:3	StackingClassifier	0.821	0.532	0.730

Results: Stage 3

Best Model Performance for this Dataset on Test Set



User Interface

Discussion

- We discovered that the stacking classifer was computationally intensive, running with $O(n)^2$ complexity.
- Interpretability Challenge: Understanding voting and stacking classifiers poses difficulties, and attempts to use Shap and ELI5 with a stacking classifier were unsuccessful.
- Voting and stacking classifiers performed slightly better when compared to LightGBM, XGBoost & AdaBoost on this dataset.

Future Work

- Conduct further exploration of the stacking classifer or implement oversampling techniques to see if model performance improves.
- Extend SHAP explainability features by adding LIME(Local Interpretable Model-Agnostic Explanations) allowing users to compare the features.
- Provide a feedback loop with financial institutions to aid model improvement.

References:
April 13, S. G., & 2022. (n.d.). New Fraud on the Block Causes Bank Losses to Rise. Www.bankinfosecurity.com. https://www.bankinfosecurity.com/new-fraud-on-block-causes-bank-losses-to-mount-a-18867
Akshaya, V., Sathyapriya, M., Ranjini Devi, R., & Sivanantham, S. (2022). Detecting Credit Card Fraud Using Majority Voting-Based Machine Learning Approach. Intelligent Systems and Sustainable Computing, 327–334. https://doi.org/10.1007/978-981-19-0011-2_30