Metaverse Fraud Prediction

By Joshua Beasley

Problem Statement

- With the rapid growth of the Metaverse, financial transactions in virtual environments have increased significantly

- Unlike traditional banking systems, transactions in the Metaverse lack stringent regulatory frameworks, making them prone to fraud

- What factors are most predictive of fraud in the Metaverse?

Predicting Fraud

- How can machine learning help predict fraud in the Metaverse?

- Identify patterns and detect anomalies to identify irregular transaction behaviors that deviate from the norm

- Dataset sourced from Kaggle containing Metaverse record transaction details

Data Wrangling

- Year analyzed: 2022
- ~78,600 observations with 14 features initially
- Dropped unhelpful features, checked for missing values
    - Dropped fields that gave away fraud too easily: Transaction Type, Risk Score, Anomaly
- Engineered a number of helpful features – increased to 48 total features
- **Target Variable: Fraud** (engineered binary feature using Transaction Type)

Data Preprocessing

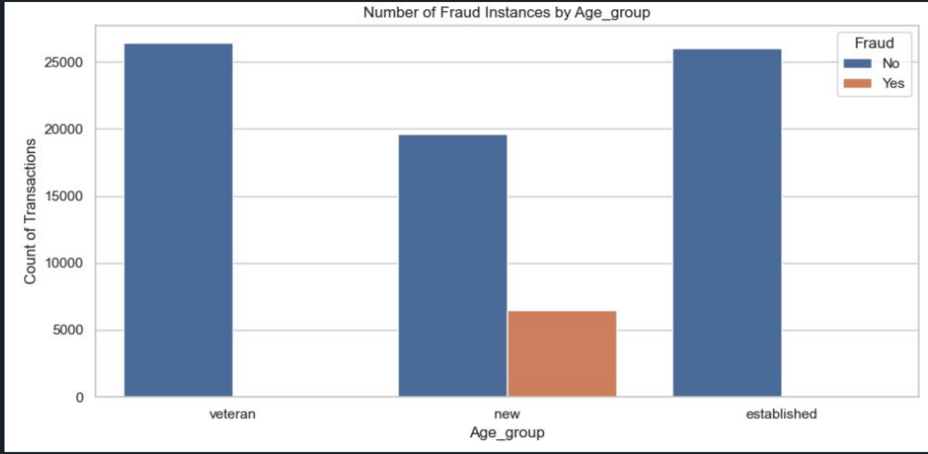
- Split into training/testing subsets
- Defined the preprocessor and pipeline
- Scaled numeric features and encoded categorical features

Correlation Insights

- Login Frequency and Session Duration had moderate negative correlations to Fraud
- Amount Per Login showed a moderate positive correlation with Fraud
- Amount Per Login and Login Frequency were strongly negatively correlated to themselves
    - Shows frequent logins are associated with smaller, routine transactions

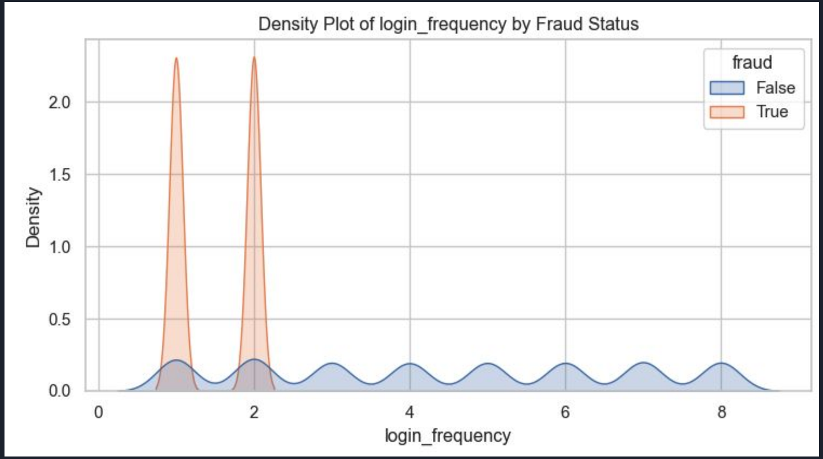
Fraud by Category

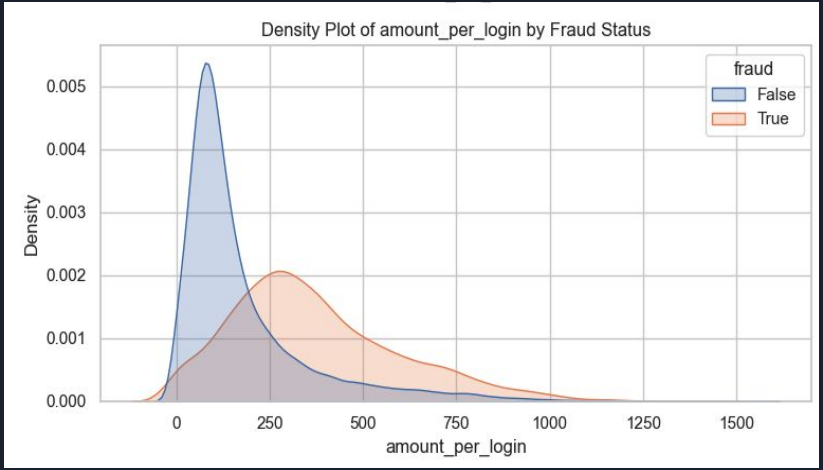
- No meaningful differences in fraud instances within categories, but with two exceptions: Purchase Pattern and Age Group
- Of the three age groups, the only one with fraud is “new”
- Of the three purchase patterns, the only one with fraud is the “random” purchase pattern



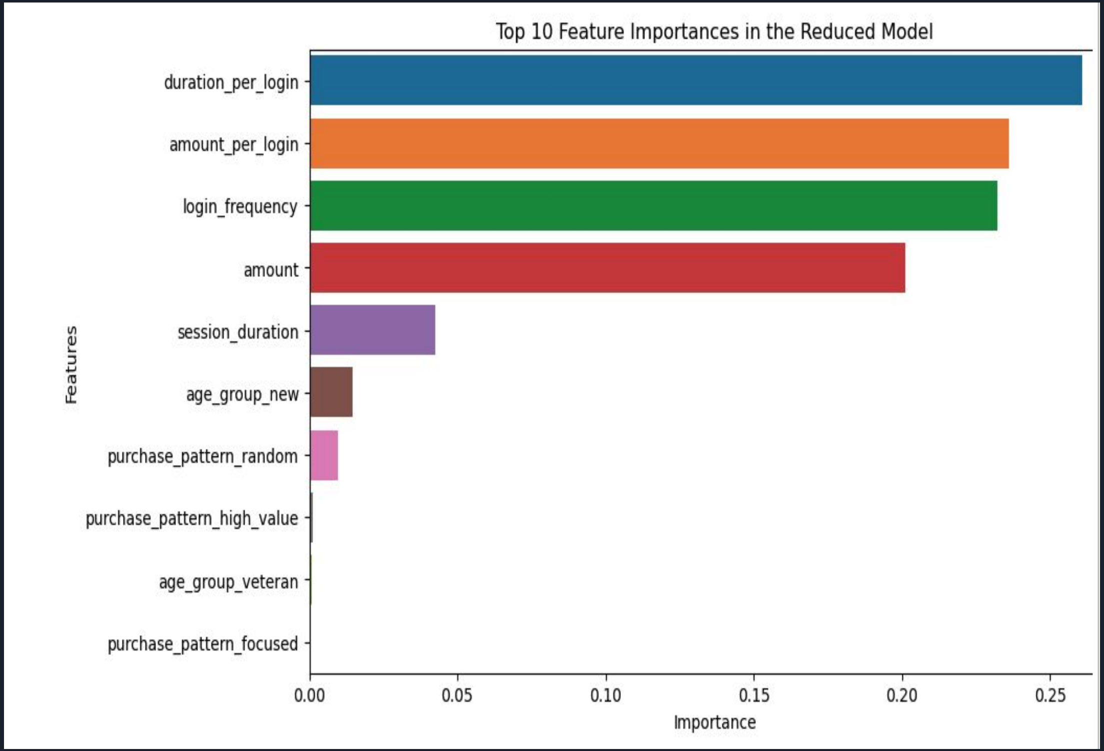
Login Frequency and Amount Per Login

- Login Frequency by Fraud Status: Fraud distribution shows two clear peaks on the left, compared to more uniform distribution of non-fraud
- Amount Per Login by Fraud Status: Non-fraud distribution shows peak at very low amount per login, while fraud distribution is flatter and to the right
- **TAKEAWAY: Fraudsters login less frequently (1-2X) for higher avg amounts per login compared to legit transactors**





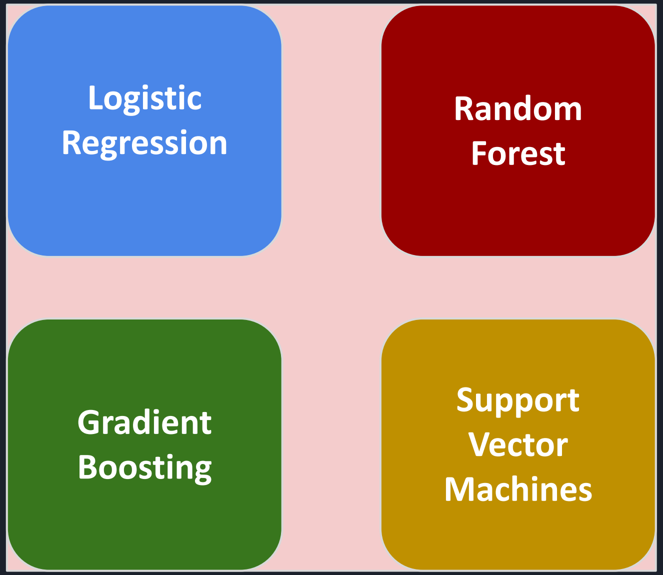
Most Impactful Features



Metrics for Evaluation

- **Precision**
  - Accuracy of positive predictions relative to all predicted positives – important for minimizing false positives
- **Recall (Sensitivity)**
  - True positive rate – crucial in fraud detection because it measures the model's ability to identify all potential fraudulent transactions, minimizing the risk of missing any true fraud cases
- **F1 Score**
  - Harmonic mean of precision and recall – balanced metric useful when requiring a trade-off between these two metrics
- **Confusion Matrix**
  - Provides a summary of prediction results on a classification problem

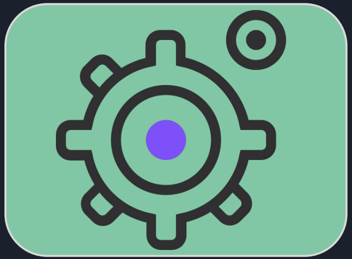
Model Selection

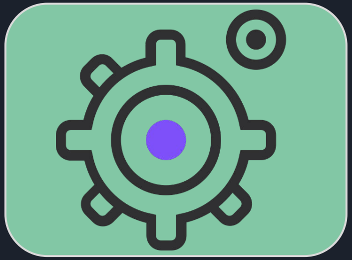


Hyper-Parameter Tuning

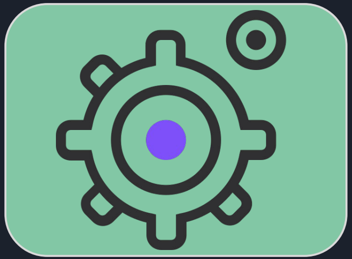
- Reduced features from full 48 to top 10 (identical results), then applied techniques to maximize recall (SMOTE, cost-sensitive learning, adjusting classification threshold)

- Discovered optimal parameters that maximized our recall (max_depth = 10, min_samples_leaf = 4, min_samples_split = 10, n_estimators = 300)

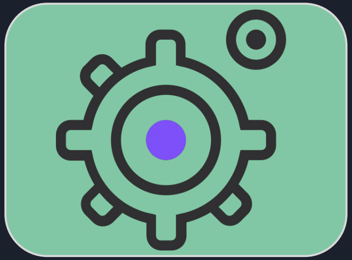




Best Model Results



- **Precision**: 25%
- **Recall**: 100% (1.0)
- **F1-Score**: 39%
- **Confusion Matrix**:
  - True Negatives: 10,621
  - False Positives: 3,848
  - False Negatives: 2
  - True Positives: 1249



Recommendations

1. **Implement fraud prediction model into the transaction processing system to enable real-time fraud detection**
   a. Immediate detection and action
   b. Reduced losses from delays
2. **Continuous model updates with new transaction data to adapt to evolving threats**
3. **Enhanced customer verification measures for transactions identified as high-risk**
   a. Two-factor authentication
   b. Manual reviews