Fraud Detection Project Report

1. Executive Summary

This report details the development of a high-performance fraud detection system. Starting from raw transactional data, we performed extensive exploratory data analysis (EDA), engineered domain-specific features, and evaluated multiple machine learning models. The project culminated in the selection of a Tuned Random Forest model as the production candidate, achieving an AUC-PR of 0.6470, a significant improvement over the baseline.

2. Data Analysis & EDA

The dataset is heavily imbalanced, with only a small fraction of transactions being fraudulent. This imbalance requires metrics like AUC-PR and F1-score for evaluation.

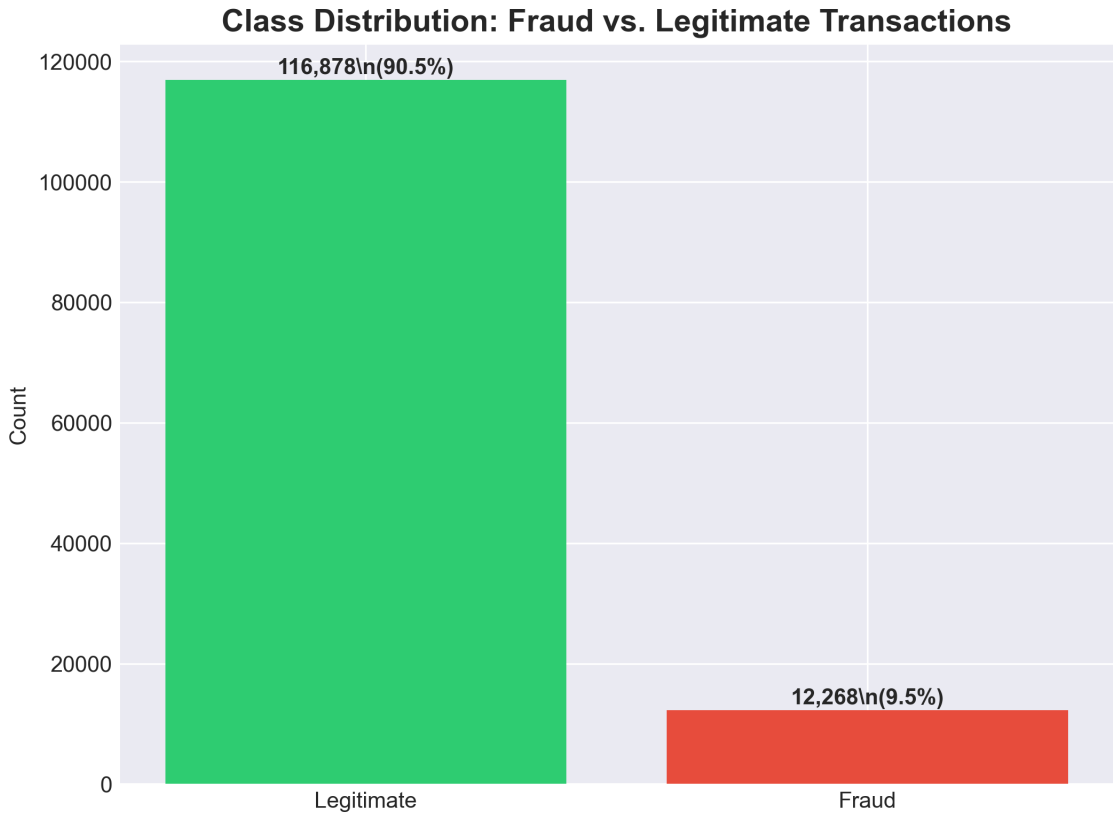

Figure 1: Class Distribution

Key insights from the EDA revealed that 'Time Since Signup' is a critical predictor. Fraudulent activity often occurs immediately after account creation, indicating automated attacks.

Fraud Detection Project Report

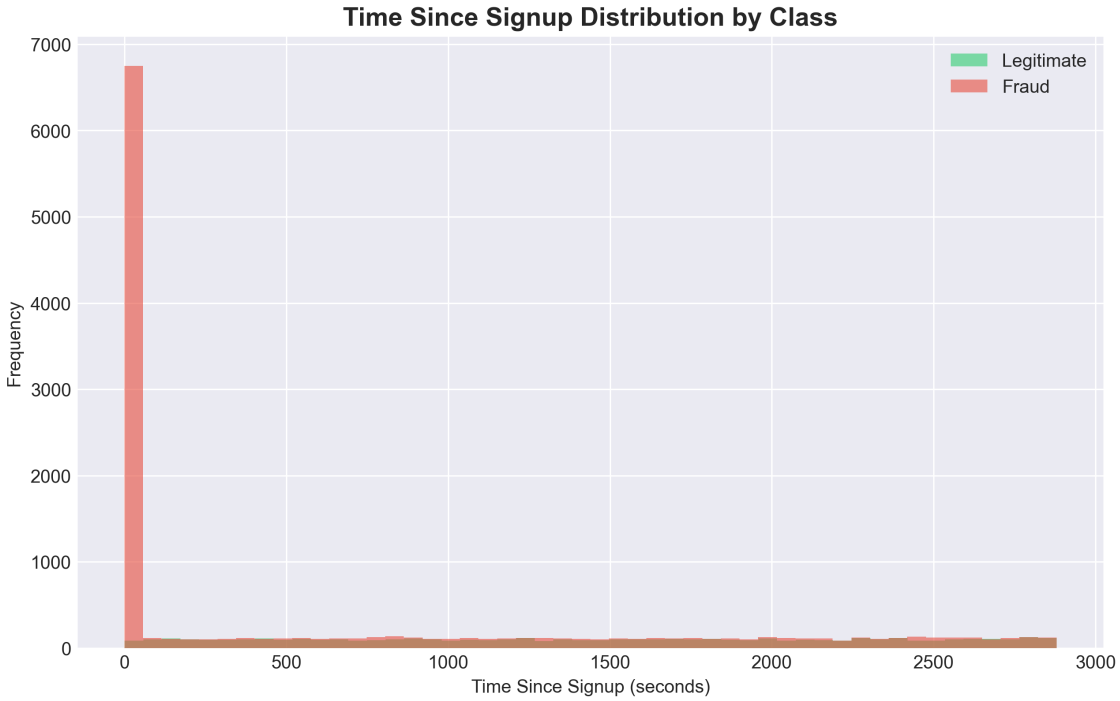

Figure 2: Time Since Signup (Seconds) by Class

Fraud Detection Project Report

3. Feature Engineering

Six key categories of features were developed:

1. Temporal Features: Capturing fraud-prone hours and days.
2. Velocity Features: Calculating time since signup (first transaction speed).
3. Geolocation Mapping: Converting IP addresses to countries to flag high-risk regions.
4. Device/IP Sharing: Detecting multiple users on the same infrastructure.

4. Model Performance & Selection

We compared a Logistic Regression baseline against Random Forest, XGBoost, and LightGBM. The Tuned Random Forest model was selected for its superior performance on imbalanced data.

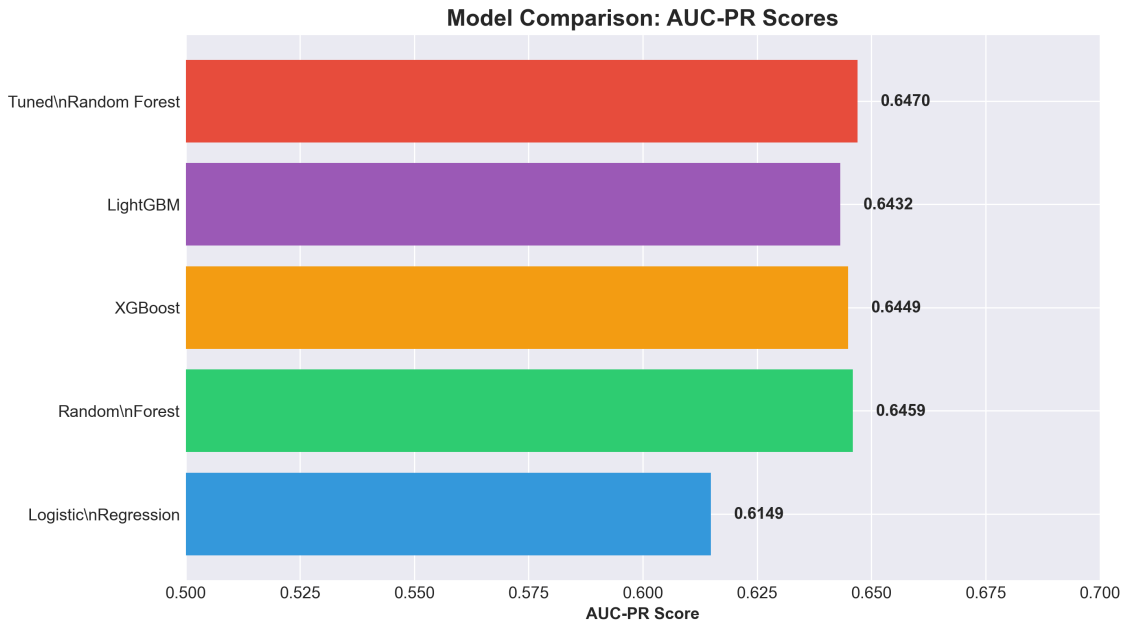

Figure 3: AUC-PR Comparison Across Models

Fraud Detection Project Report

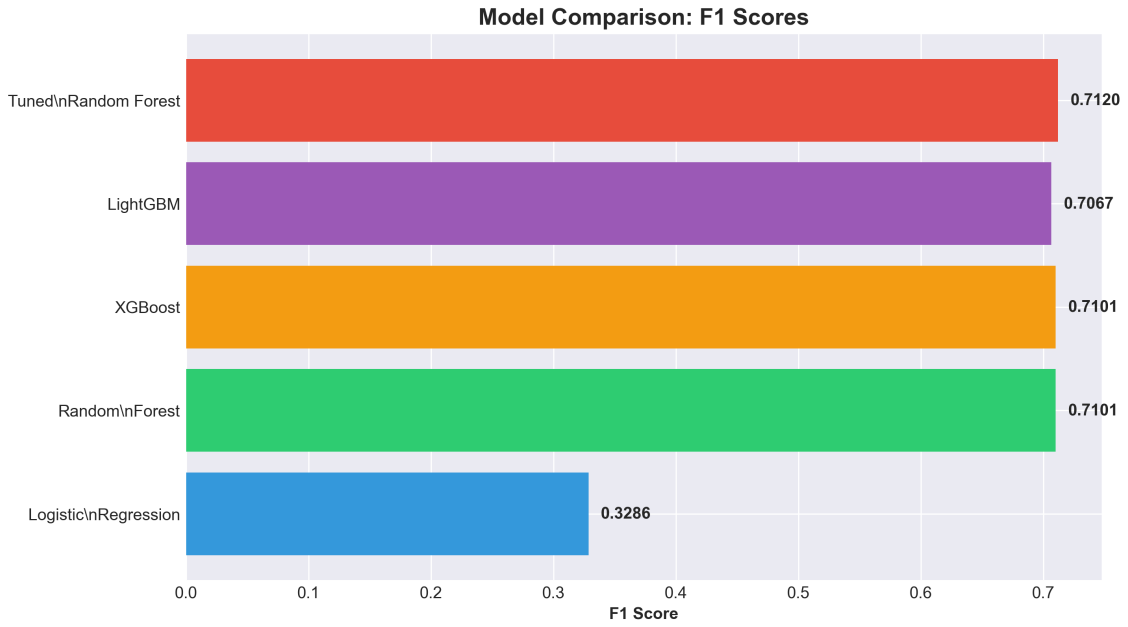

Figure 4: F1 Score Comparison

Fraud Detection Project Report

5. Model Interpretability (SHAP)

To ensure transparency, we utilized SHAP values to explain model predictions.

Global Results: The 'time_since_signup' feature is the most influential factor. Transactions occurring within seconds of signup are almost universally flagged as fraud.

Local Predictions: We analyzed True Positives (correctly blocked fraud), False Positives (legitimate users blocked), and False Negatives (missed fraud) to improve model refinement.

6. Business Recommendations

1. Implement a 15-minute 'Cooling Period' for new accounts.
2. Trigger Step-up Authentication (2FA) for transactions with low time-since-signup.
3. Monitor high-risk IP/Country combinations identified in the geolocation analysis.