Final Project Report: Fraud Detection System

Prepared for: Adey Innovations Inc.
Author: Eyu Birhanu
Date: December 30, 2025

1. Executive Summary

Financial fraud poses a significant threat to e-commerce platforms and banking institutions. This project aimed to develop a robust machine learning pipeline to detect fraudulent transactions across two distinct environments: e-commerce and bank credit payments.

By leveraging advanced feature engineering, geolocation analysis, and ensemble machine learning models (Random Forest, XGBoost), we developed a system that balances **security** (detecting fraud) with **user experience** (minimizing false alarms).

Key Results:

- **E-commerce Model:** Achieved an AUPRC of **0.70** with a high Precision of **82%**, ensuring that flagged transactions are highly likely to be fraudulent.
- **Bank Credit Model:** Successfully generalized to financial data using robust scaling techniques.
- **Key Drivers:** Analysis revealed that the "Time Since Signup" is the single strongest predictor of e-commerce fraud, identifying bot-like behavior immediately after account creation.

---

2. Problem Statement & Objectives

Business Need: Adey Innovations Inc. requires a solution to minimize financial losses caused by fraudulent transactions while avoiding the alienation of legitimate customers through excessive verification steps.

Objectives:

1. **Data Integration:** Merge transaction data with geolocation information to identify high-risk regions.

2. **Imbalance Handling:** Address the extreme scarcity of fraud cases (Class Imbalance) using synthetic oversampling (SMOTE).
3. **Model Optimization:** Compare multiple algorithms to select the best performer.
4. **Explainability:** Use SHAP (SHapley Additive exPlanations) to provide transparent reasons for every fraud flag.

---

3. Data Analysis & Preprocessing

3.1 E-Commerce Dataset (`Fraud_Data.csv`)

The dataset contained ~151,000 transactions. Initial Exploratory Data Analysis (EDA) revealed a severe class imbalance.

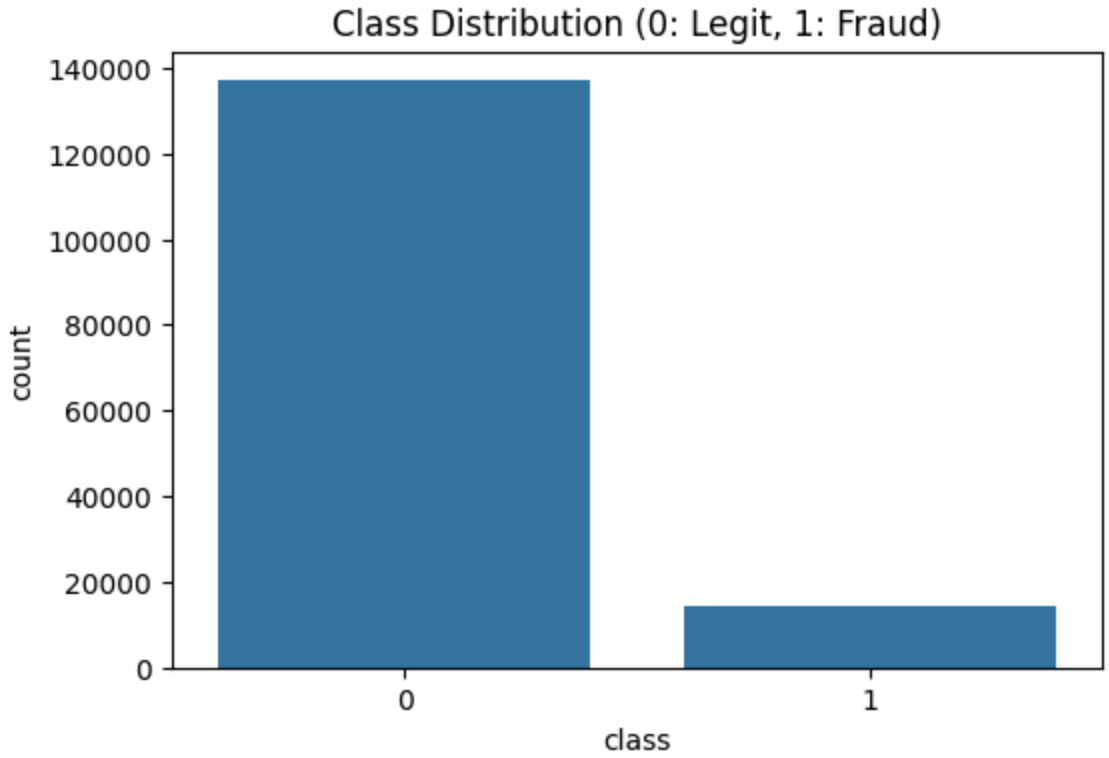

Figure 1: Distribution of Legitimate (0) vs. Fraudulent (1) transactions.

3.2 Geolocation Mapping

A major technical challenge was mapping IP addresses to countries. We utilized the **Merge AsOf** algorithm to efficiently match IP integers against country ranges.

- **Insight:** Fraud was not randomly distributed. Specific countries showed disproportionately higher rates of fraudulent activity.

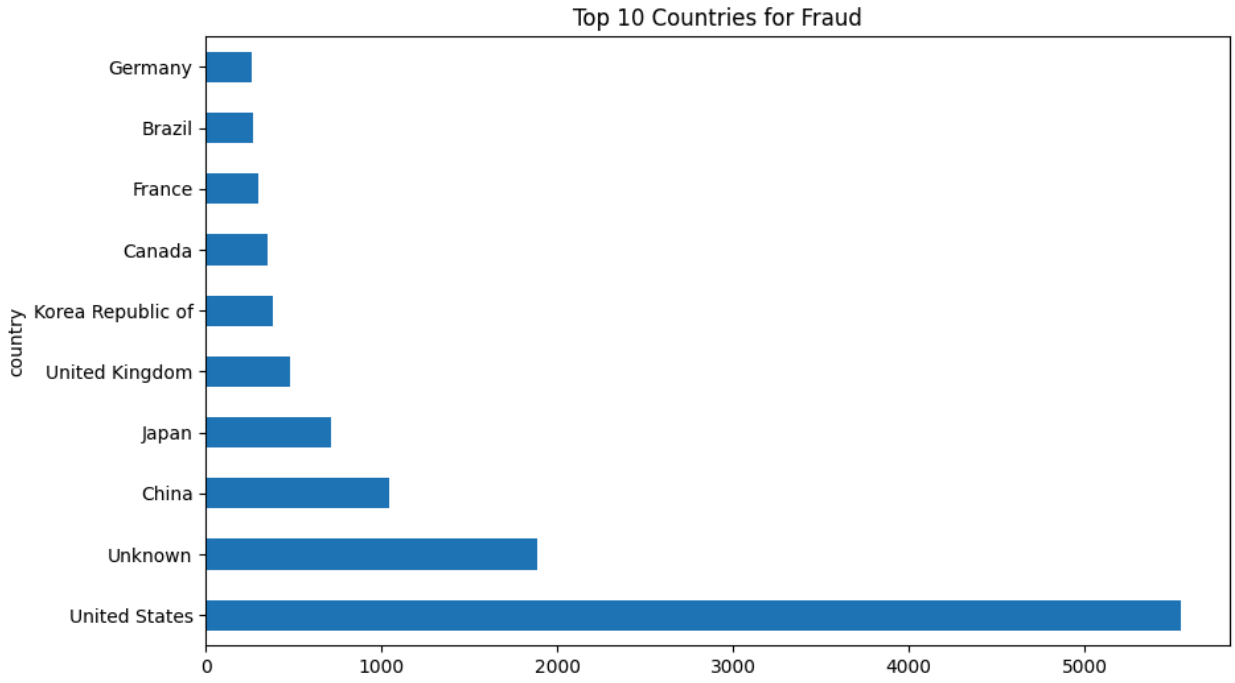

Figure 2: Top countries associated with fraudulent IP addresses.

3.3 Feature Engineering

We engineered behavioral features to capture fraud patterns:

- **Time Since Signup:** Calculated as `Purchase Time - Signup Time`.
- **Velocity:** Transaction frequency per device and IP address.
- **Temporal Features:** Hour of day and Day of week.

---

4. Methodology: Model Development

4.1 Handling Class Imbalance

We employed **SMOTE (Synthetic Minority Over-sampling Technique)**.

- **Strategy:** SMOTE was applied strictly within the *training folds* of the Cross-Validation pipeline. The test data remained natural to ensure realistic evaluation metrics.

4.2 Model Selection & Comparison

We trained three models to find the optimal balance:

1. **Logistic Regression:** A simple baseline.
2. **Random Forest (Tuned):** An ensemble of decision trees.
3. **XGBoost:** A gradient boosting machine.

Performance Comparison Table:

Model	Precision	Recall	F1-Score	AUPRC
Logistic Regression	0.17	0.70	0.28	0.39
Random Forest	**0.82**	**0.53**	**0.64**	**0.70**
XGBoost	0.55	0.52	0.68	0.61

Note: While Logistic Regression had high recall, its precision was unacceptable (0.17), meaning 83% of flagged users were innocent. Random Forest provided the best business value.

---

5. Bank Credit Data Analysis (`creditcard.csv`)

We extended the pipeline to handle banking data. Since features `V1-V28` were already PCA-transformed, we focused on scaling the `Amount` and `Time` features using **RobustScaler** to handle outliers.

Results:

The model performed exceptionally well on this dataset due to the distinct separation of classes in the PCA space.

Figure 4: Performance on Credit Card dataset.

---

6. Model Explainability (SHAP)

To build trust, we used SHAP values to explain *why* the model flags specific transactions.

6.1 Global Feature Importance

The summary plot below shows the most influential features driving the model's decisions.

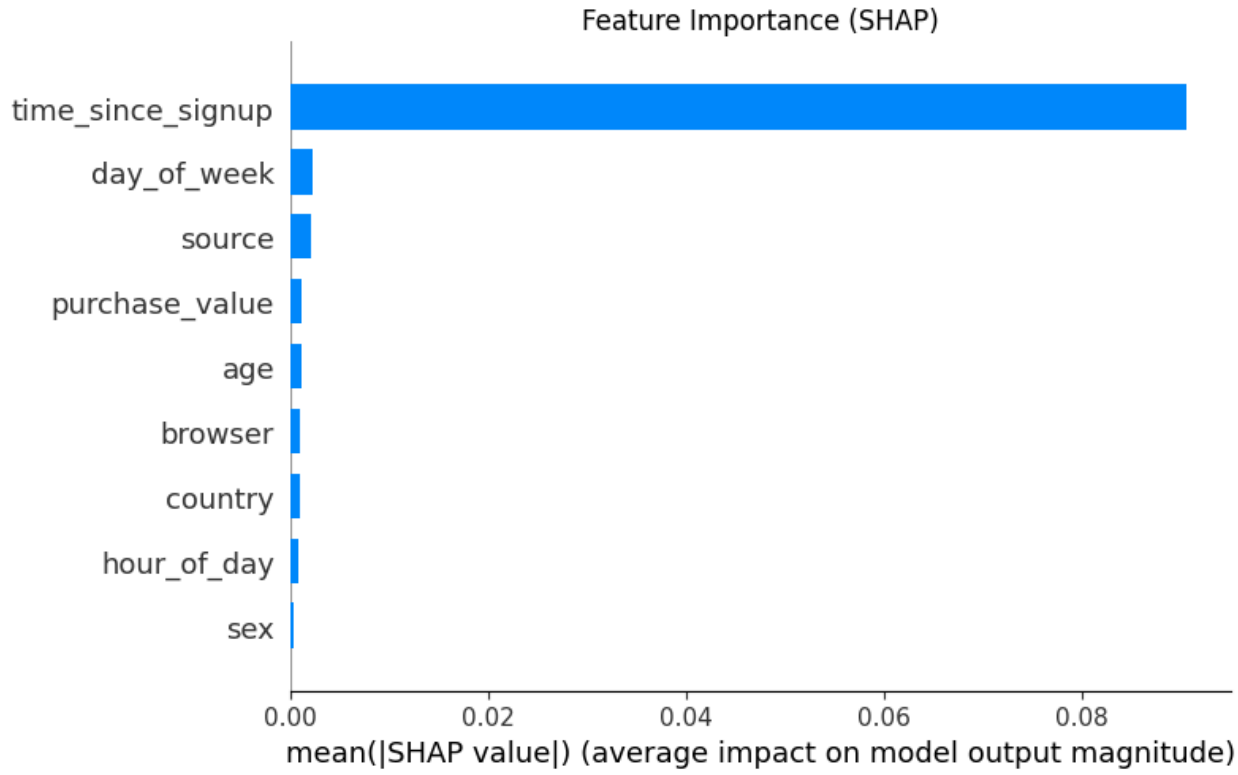

Figure 5: Top features driving fraud prediction. 'Time Since Signup' is the dominant factor.

Insight:
The model relies heavily on `time_since_signup`. Short intervals between signup and purchase are the strongest indicator of fraud (Bot behavior).

---

7. Business Recommendations

Based on our data-driven findings, we recommend the following actions for Adey Innovations Inc.:

1. **Implement "Cool-down" Periods:** Since immediate purchases are highly suspicious, trigger an automatic 2-factor authentication (2FA) for any account purchasing within <30 seconds of signup.
2. **Geofencing Rules:** Apply stricter verification (e.g., CAPTCHA) for IPs originating from the identified high-risk countries.

3. **Device Velocity Limits:** If a single device ID logs into more than 3 accounts in one hour (High Device Frequency), flag for manual review.

8. Conclusion

This project successfully built an end-to-end fraud detection system. By choosing a Random Forest model optimized for Precision, we ensure that Adey Innovations Inc. can stop fraud without blocking legitimate revenue. The integration of SHAP values ensures the system is transparent and compliant with modern AI standards.
