Online Payment Fraud Detection

Ahmad Bin Tariq, Omer Faiz, Subhan Zia
Department of Computer Science,
National University of Computer and Emerging Sciences, Lahore

November 25, 2024

Abstract

Online payment fraud has become a critical challenge in the modern financial ecosystem. This project investigates techniques for detecting fraudulent transactions in a large-scale dataset of online payments. Using a combination of data preprocessing, feature engineering, and machine learning models, we aim to identify fraud with high accuracy. Our best-performing model, XGBoost, achieved a precision of 0.89, a recall of 0.87, and an F1-score of 0.88, showcasing its effectiveness for fraud detection. Future work includes expanding the dataset and exploring alternative algorithms.

1 Introduction

Online payment systems have revolutionized financial transactions but have also led to a surge in fraudulent activities. Accurately detecting fraudulent transactions is essential for financial security. This study explores machine learning techniques to classify transactions as fraudulent or non-fraudulent based on a dataset containing over 6 million records. We preprocess the data, address class imbalance, and train various models to identify fraudulent activities effectively.

2 Methodology

2.1 Data Preprocessing

- **Dataset Overview:** The dataset contains 6,362,620 rows and 8 columns, including transaction details such as amount, type, and account balances.
- **Data Cleaning:** Removed unnecessary columns (`nameOrig`, `nameDest`, `isFlaggedFraud`) and encoded categorical features.
- **Balancing Classes:** Used random undersampling to address class imbalance, ensuring equal representation of fraudulent and non-fraudulent transactions.

2.2 Feature Engineering

- **Visualization:** Generated heatmaps, boxplots, and pairplots to explore feature relationships.
- **Scaling:** Standardized numerical features to ensure a mean of 0 and a standard deviation of 1.
- **Dimensionality Reduction:** Retained only the most relevant features based on correlation analysis.

2.3 Model Training

The reduced dataset was split into training and testing sets (80-20 split). We evaluated five models: Logistic Regression, Random Forest, XGBoost, MLP, and Naive Bayes. XGBoost emerged as the best model with a cross-validation accuracy of 87.29%.

3 Experiments

3.1 Correlation Heatmap of Features

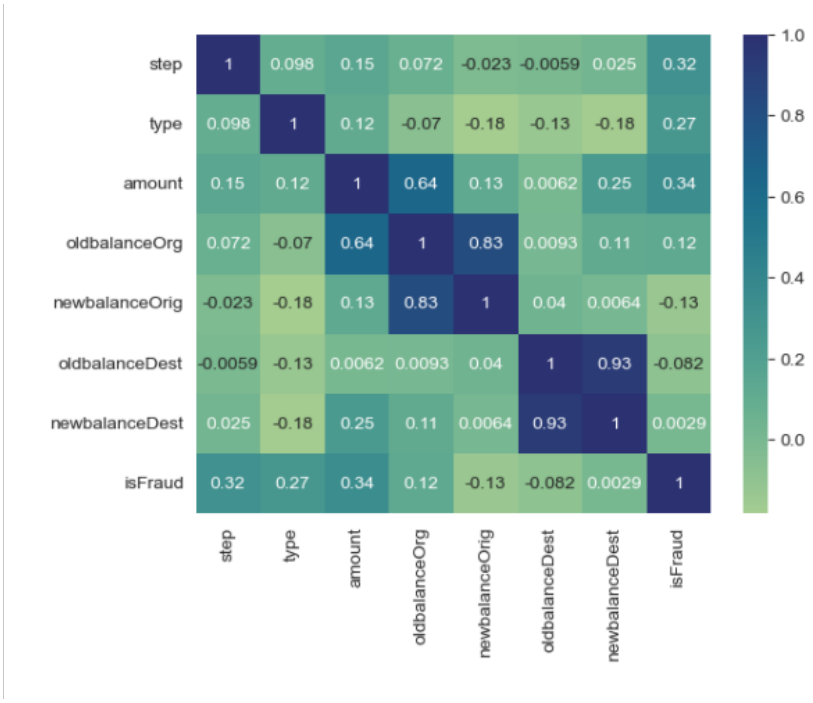

Figure 1: Correlation Heatmap of Features

We generate a correlation heatmap of the Balanced Data to visualize the relationships between different numerical features. The heatmap uses the 'crest' color map and annotates the correlation values on the plot.

3.2 ROC Curve for XGBoost Classifier

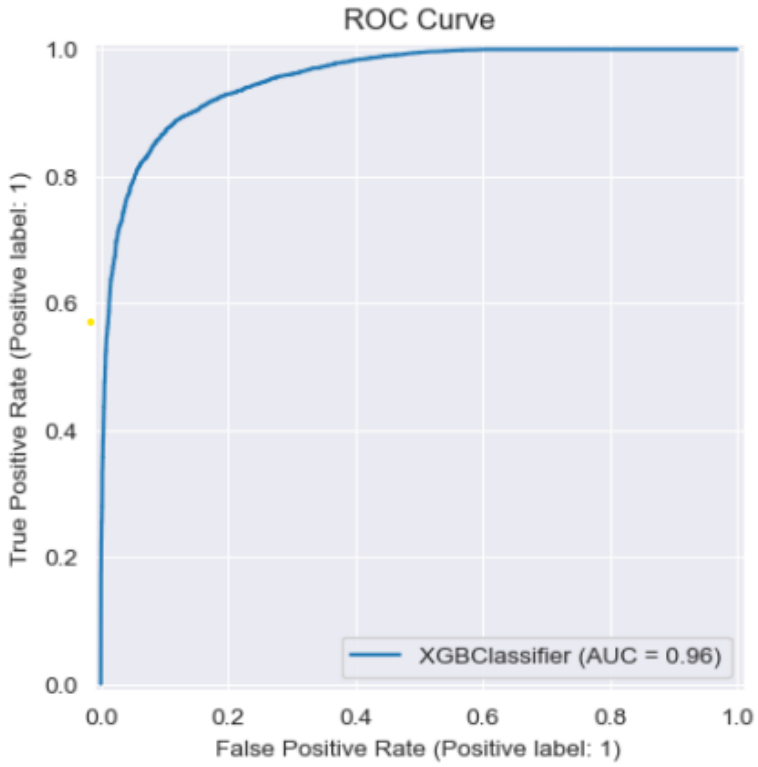

Figure 2: ROC Curve for XGBoost Classifier

ROC curve further demonstrate its effectiveness in distinguishing between non-fraud and fraud cases.

3.3 Pie Chart

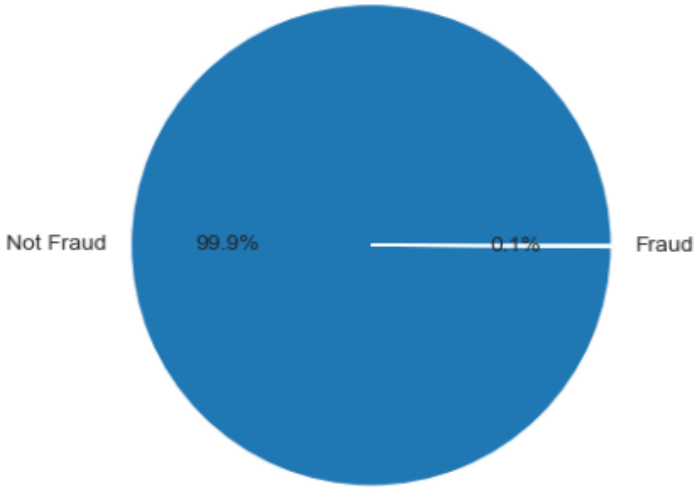

Figure 3: Pie Chart

The pie chart illustrates a significant imbalance in transaction data, with a vast majority (99.9 percent) classified as non-fraudulent and a tiny fraction (0.1 percent) as fraudulent. This imbalance poses challenges for building effective fraud detection models, as they must be highly sensitive to accurately identify rare fraudulent cases while minimizing false positives. To improve model accuracy and mitigate the potential financial impact of fraud, it's crucial to collect more data on fraudulent transactions to create a more balanced dataset and carefully balance sensitivity with specificity to avoid excessive false positives.

3.4 Boxplot for Data Distribution

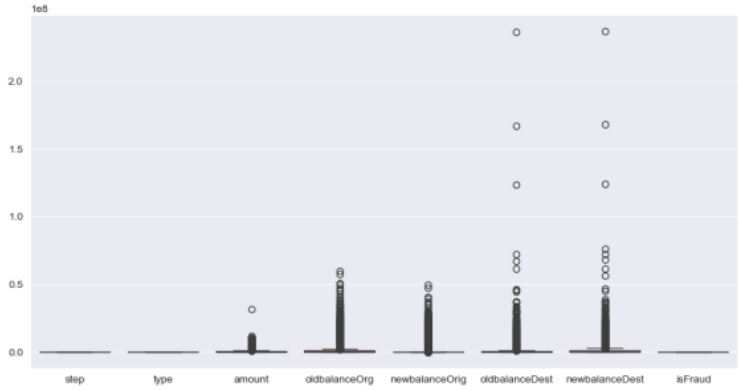

Figure 4: Visualizing Feature Distributions

We create a boxplot to visualize the distribution and detect any potential outliers in the Balanced Data

3.5 Visualizing Feature Distributions

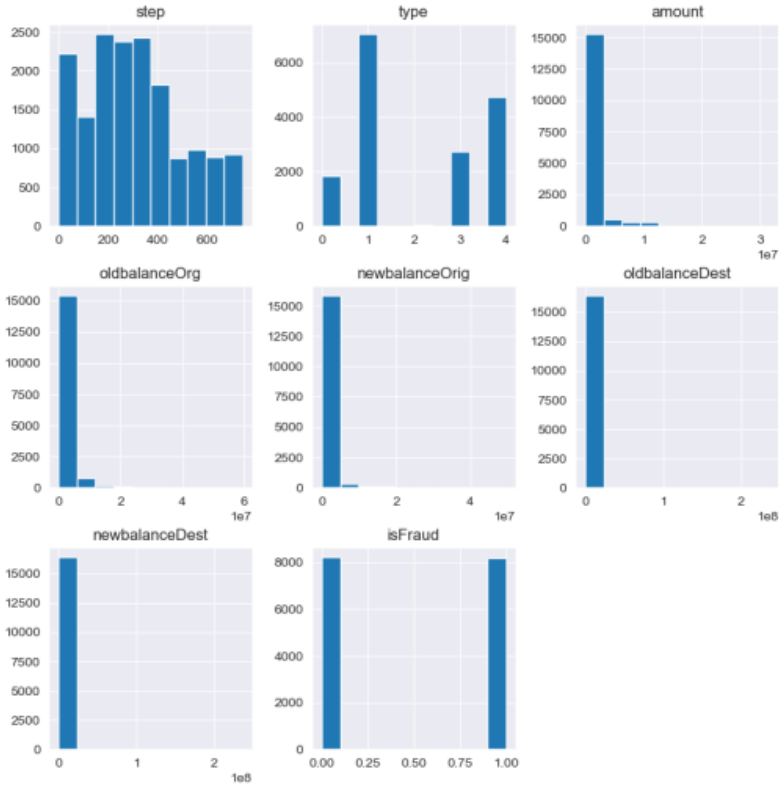

Figure 5: Visualizing Feature Distributions

We plot histograms for all numerical features in the Balanced Data to observe their distributions.

3.6 Pairplot of Features

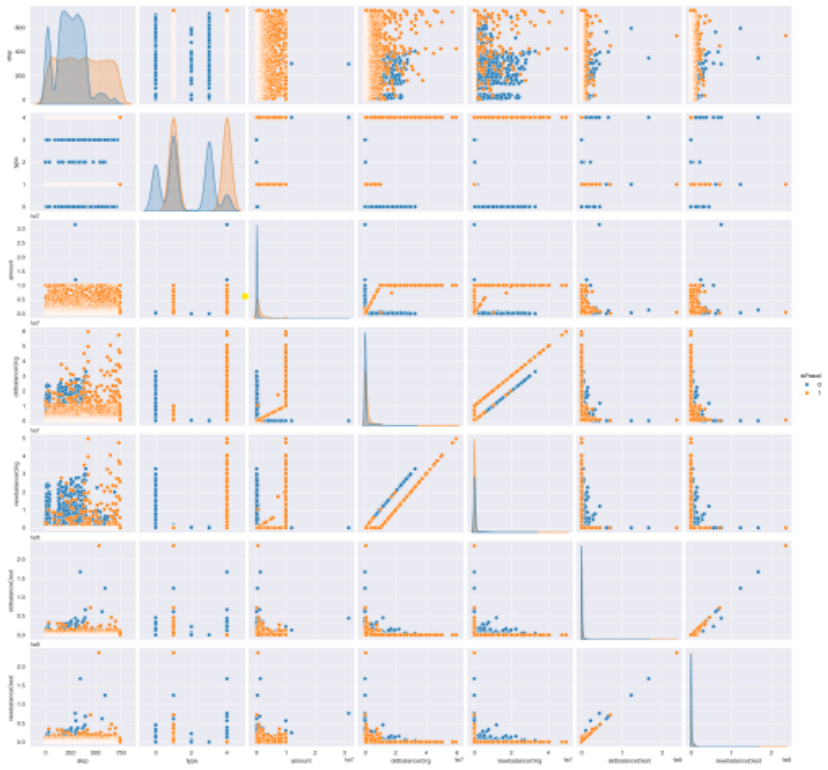

Figure 6: Pairplot of Features

We create a pairplot to visualize the relationships between features in the Balanced Data, colored by the 'isFraud' label. This helps in understanding how the features correlate with fraud vs. non-fraud transactions.

3.7 Heatmap for Reduced Data

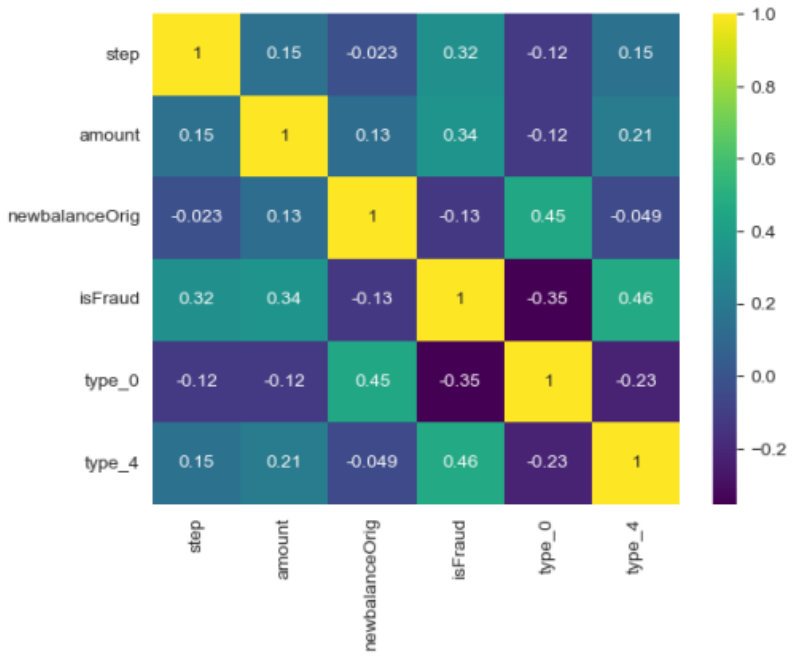

Figure 7: Heatmap for Reduced Data

• Visualized the correlation matrix of the reduced dataset using a heatmap. • Ensured the remaining features are minimally correlated and relevant for model training

4 Results & Discussion

The XGBoost model achieved the following metrics:

- Accuracy: 88.52%
- Precision: 89.32%
- Recall: 87.45%
- F1-Score: 88.38%
- AUC: 96%

4.1 Confusion Matrix

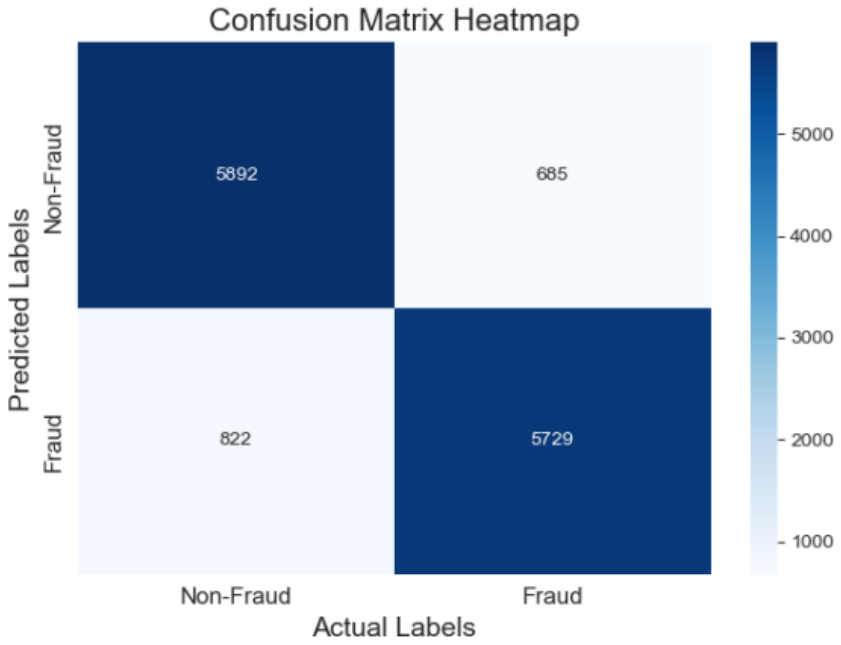

Figure 8: Confusion Matrix

The confusion matrix revealed a strong ability to distinguish between fraudulent and non-fraudulent transactions. Potential errors may stem from overlapping features between classes.

5 Conclusion and Future Work

This project demonstrates the feasibility of using machine learning for online fraud detection, with XGBoost outperforming other models. Future work includes exploring advanced techniques like deep learning, utilizing larger datasets, and incorporating real-time fraud detection systems.

References

[1] Dataset available at `https://www.kaggle.com/datasets`.

[2] Scikit-learn documentation for machine learning algorithms: `https://scikit-learn.org`.