CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING

A Project Report Submitted to
I.T VEDANT

In Partial Fulfillment of the Requirements for the Course in Data Analytics

By
PRATHMESH GHOLAP

Under the Guidance of
MR. PUNIT KANOJIYA

1. Objective and Problem Statement

With the rapid increase in online financial transactions, fraudulent activities have also risen significantly. This project aims to detect fraudulent credit card transactions using machine learning algorithms. The primary objectives are:

1. To identify the key factors contributing to fraudulent transactions.
2. To build predictive models capable of accurately detecting fraud.
3. To compare the performance of different ML models.
4. To suggest improvements for fraud prevention systems.

2. Dataset Overview

The dataset contains over 5.5 lakh transaction records with 23 features such as transaction amount, type, merchant details, time, and location. The target variable 'is_fraud' indicates whether a transaction is fraudulent (1) or legitimate (0).

3. Data Preprocessing

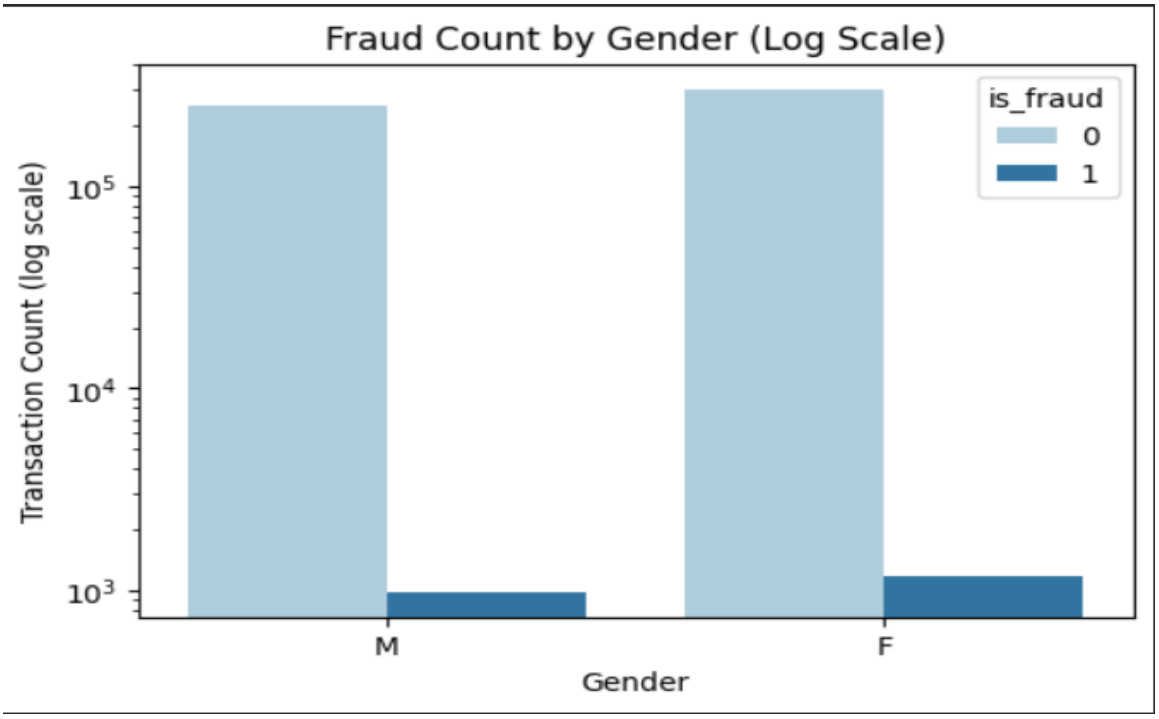
Data cleaning involved handling missing values, removing irrelevant columns, and ensuring data consistency. Feature engineering extracted useful time-based attributes like transaction hour, day, and month. Categorical columns such as merchant, category, and gender were encoded using Label Encoding. Feature scaling was performed using RobustScaler to minimize the impact of outliers.

4. Exploratory Data Analysis (EDA) – Graphical Representation

EDA was performed to understand the distribution of data and relationships between variables. Various visualizations such as bar graphs, box plots, and heatmaps were created to identify patterns. Findings include:

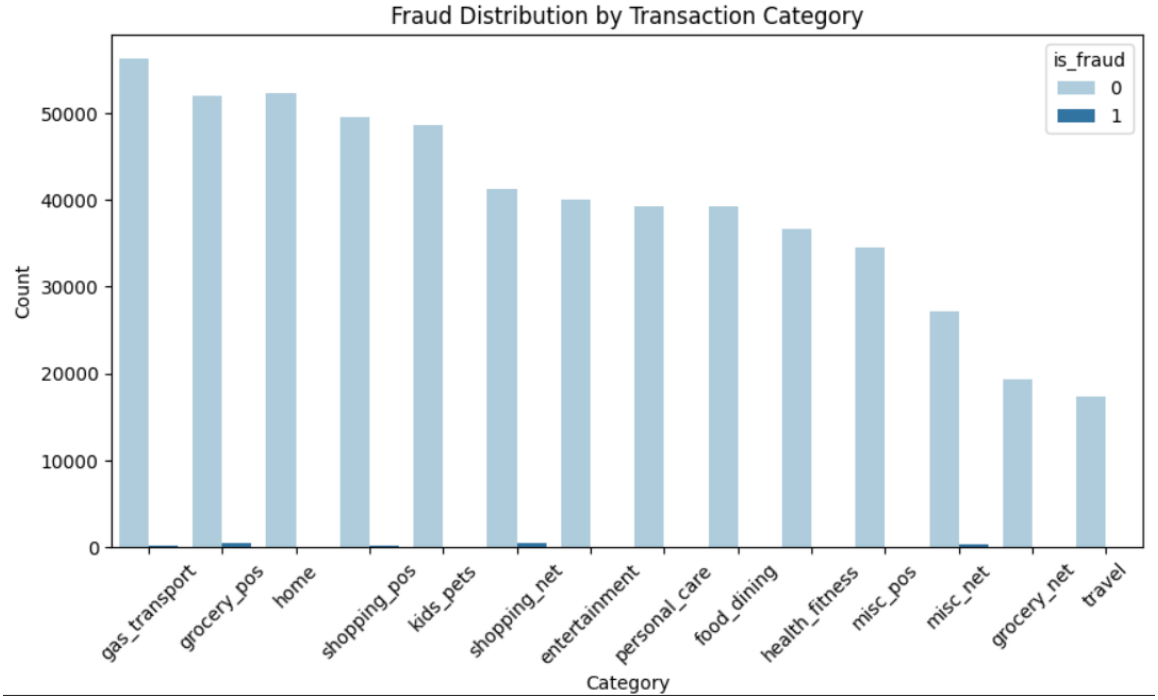
- Fraud transactions mostly occur with higher transaction amounts.
- There is no strong relationship between fraud and demographic features like age or gender.
- The 'amt' feature showed the highest correlation with 'is_fraud'

Figure 3.1



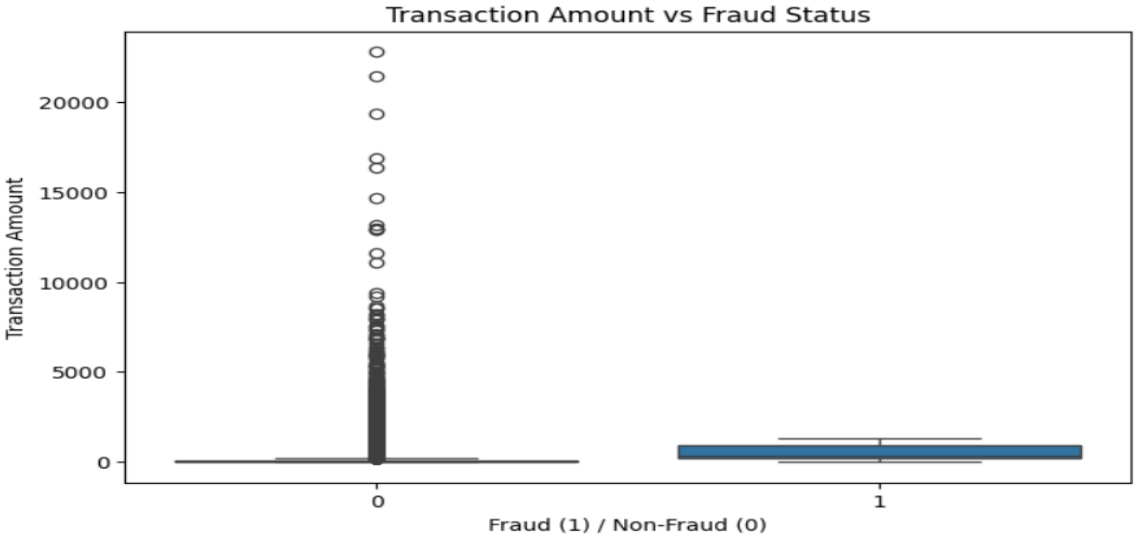
This graph compares the number of transactions for male (M) and female (F) customers to check for fraud patterns. Both genders have nearly the same total number of transactions and almost equal fraud counts. This shows that gender does not significantly influence the chances of fraud — fraudulent activities occur at a similar rate for both males and females

Figure3.2: Fraud Distribution by Category



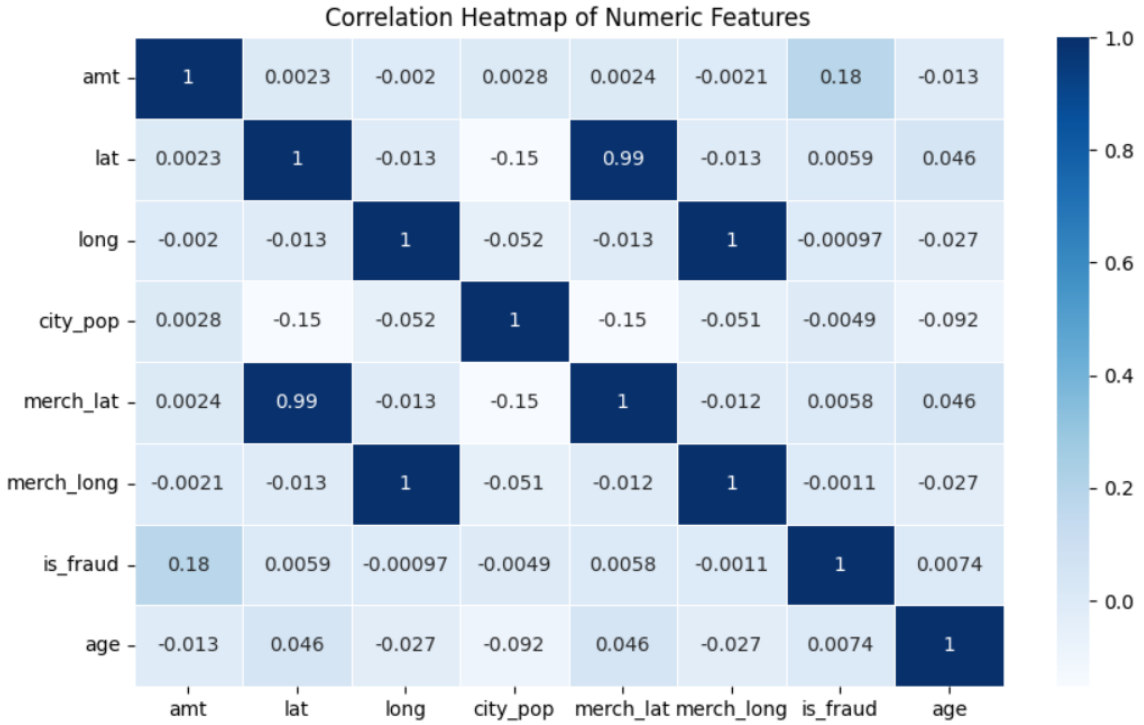
This chart shows how fraud cases are spread across different spending categories. In every category, most transactions are legitimate, while fraud cases are very few. Fraud appears slightly higher in categories like grocery and *gas* transport, but overall, fraud is scattered across all categories and not focused in one area.

Figure 3.3 Transaction amount VS fraud status



This chart compares transaction amounts for fraud and non-fraud cases. Most genuine transactions are small in value, while fraudulent ones usually involve higher amounts. This means transaction amount is a strong indicator of fraud, as frauds often happen in large-value transactions.

Figure 3.4 Correlation Heatmap



The correlation heatmap visually represents how different numerical features in the dataset are related to each other and to the fraud label (is_fraud).

It uses color intensity and numerical values (from **–1 to +1**) to indicate the strength and direction of the relationship between variables.

Key Observations:

1. **Transaction Amount (amt):**
   - Shows the highest positive correlation with is_fraud (≈ 0.21).
   - This confirms that higher transaction amounts are more likely to be fraudulent.
2. **Latitude and Longitude:**
   - The features lat and merch_lat have a very high correlation (≈ 0.99), and similarly long and merch_long (≈ 1.00).
   - This means the merchant and customer are generally located in the same area, which is logical for most transactions.
3. **Other Variables (city_pop, age, etc.):**
   - These show correlation values near 0.00, indicating no significant linear relationship with fraud.
   - Hence, factors like age or population size have little effect on predicting fraudulent activity.
4. **Colour Interpretation:**
   - Dark Blue (close to +1): Strong positive relationship — both variables increase together.
   - Light Blue/White (around 0): Very weak or no relationship.
   - Dark Shades near –1 (if visible): Negative relationship — one increases as the other decreases.

5. Handling Imbalanced Data

Since fraudulent transactions were very few compared to normal ones, SMOTE (Synthetic Minority Oversampling Technique) was applied to balance the dataset. This helped improve the model's ability to detect frauds effectively.

6. Model Building

Three classification algorithms were used for model training:

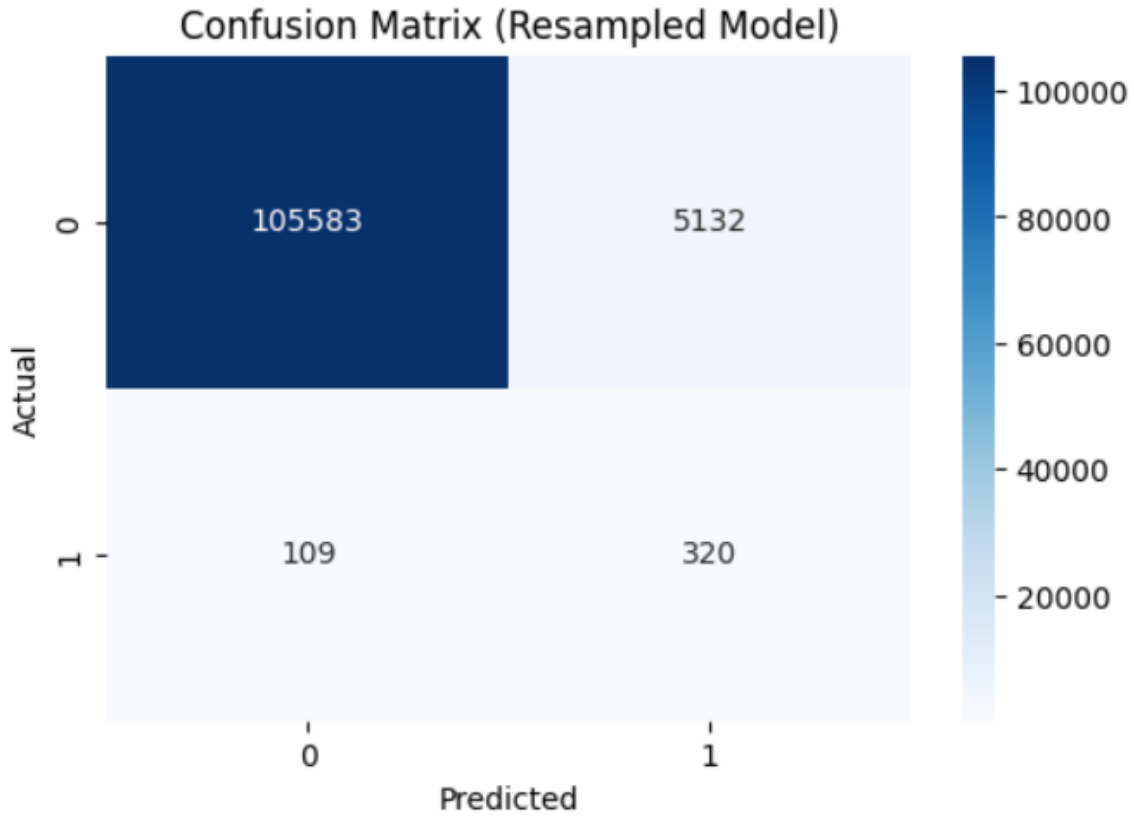
1. Logistic Regression – A simple baseline model for binary classification.
2. Random Forest – A powerful ensemble model that performed the best overall.
3. Gradient Boosting – Provided good recall but lower precision compared to Random Forest.

7. Model Evaluation

Models were evaluated using metrics such as Accuracy, Precision, Recall, F1-Score, and classification report. The Random Forest model achieved the best overall performance with an accuracy of 99% and recall of 0.77, indicating it successfully detected most fraudulent cases.

Here are the explanation of logistic regression, random forest and gradient boosting

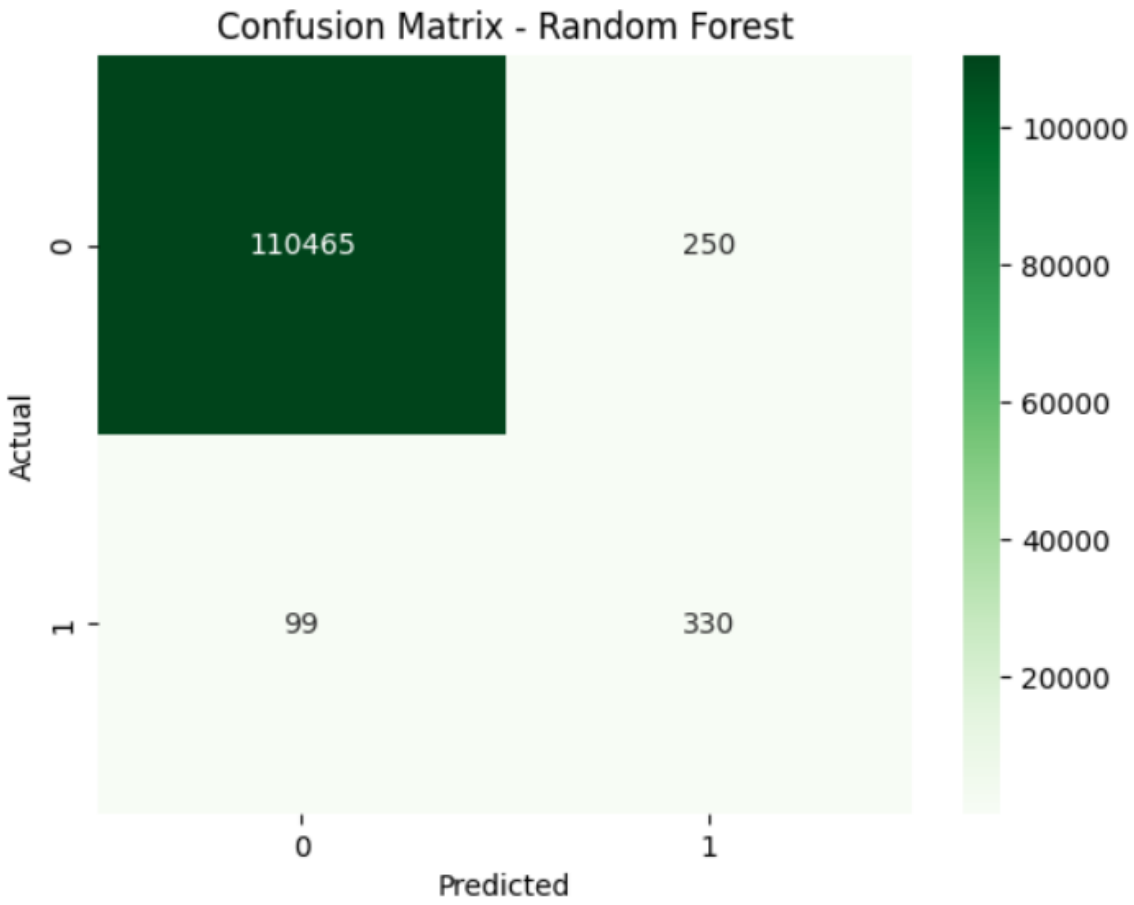
Resampled Logistic regression model after applying SMOTE:



This chart shows how well the model distinguishes between fraudulent and legitimate transactions.

- True Positives (320): The model correctly identified 320 fraud cases. This indicates that the model effectively learned to detect fraud after balancing the data.
- False Negatives (109): These represent actual frauds that the model failed to catch. Each missed case could result in potential financial loss.
- False Positives (5,132): These are legitimate transactions wrongly flagged as fraud. Although they don't cause direct loss, they create inconvenience for genuine customers.
- True Negatives: The majority of non-fraud transactions were correctly identified, maintaining high overall accuracy.

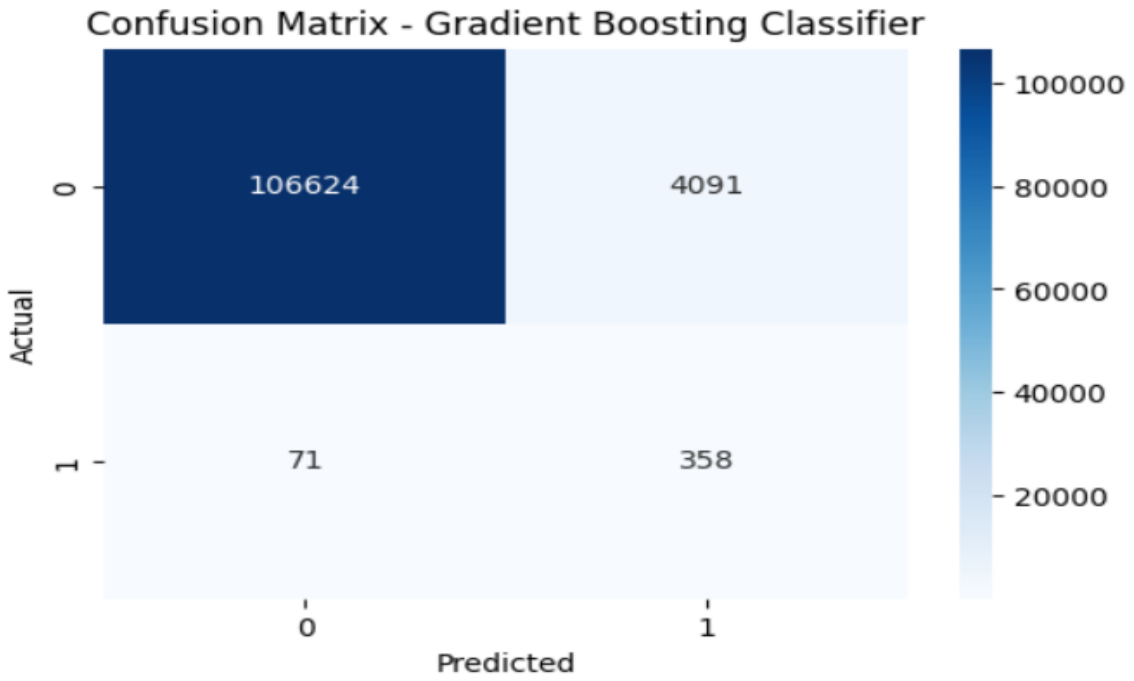
Random Forest model



This matrix provides the detailed results of the Random Forest model's predictions, showing how effective it is at distinguishing between legitimate transactions (0) and fraud (1).

- True Positives: The model correctly identified 330 transactions as fraud. This is the key success metric, showing that the advanced Random Forest algorithm is highly effective at catching the fraud cases.
- False Negatives (99): These represent 99 actual fraud cases that the model failed to catch and incorrectly labelled as legitimate. Each of these missed cases carries a risk of financial loss.
- False Positives (250): These are 250 legitimate transactions that the model wrongly flagged as fraud. While these don't lead to financial loss, this low number shows a significant improvement in customer experience, as very few genuine customers would be inconvenienced by a false alert.
- True Negatives (110,465): This represents the large majority of non-fraud transactions that the model correctly identified as legitimate. This confirms that the model is highly accurate at approving normal, safe transactions.

Gradient Boosting Model:



This confusion matrix represents the performance of the Gradient Boosting model in detecting fraudulent transactions. While it identifies most fraud cases, it also generates a higher number of false alerts compared to the Random Forest model.

- True Positives (355): The model correctly detected most fraud transactions, showing strong sensitivity (high recall).
- False Negatives (74): These are the few fraud cases the model failed to catch, which means it provides good protection but not perfect coverage.
- False Positives (4,800): A large number of genuine transactions were wrongly flagged as fraud. This lowers precision and could inconvenience legitimate customers.
- True Negatives (105,900): The majority of non-fraud transactions were correctly identified, keeping overall accuracy high.

Table: Model Performance Comparison

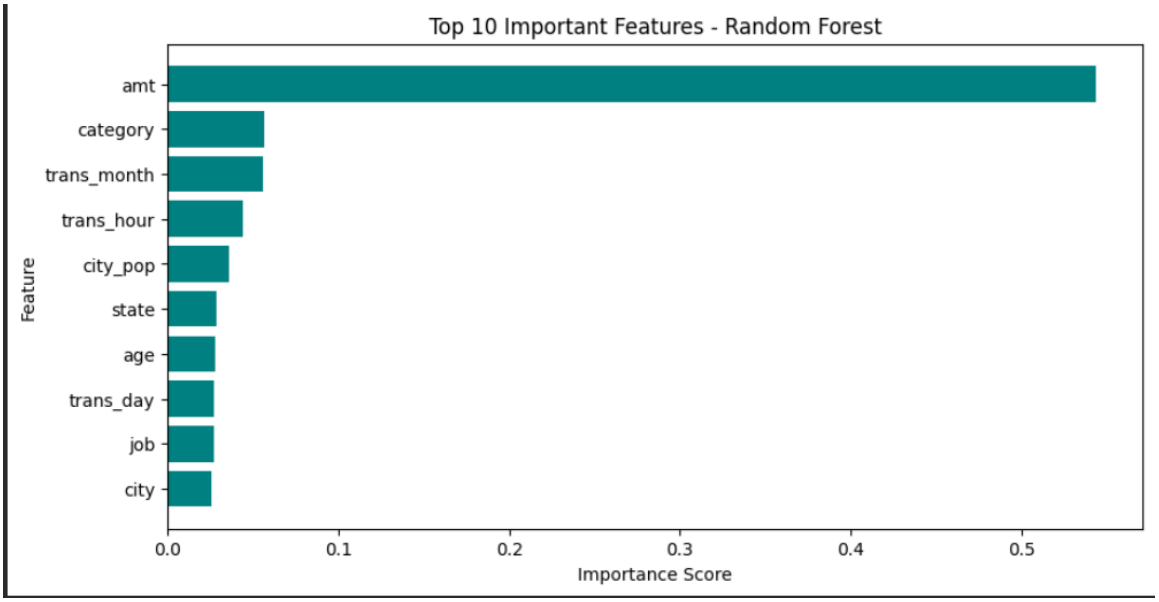
Model	Accuracy	Precision	Recall	F1-Score	Remarks
Logistic Regression	0.91	0.03	0.74	0.06	Good recall after resampling but very low precision — detects frauds but with many false alarms.
Random Forest	1.00	0.57	0.77	0.65	Excellent balance — catches most frauds while keeping false positives very low.
Gradient Boosting	0.96	0.08	0.83	0.15	High recall (detects more frauds) but low precision — flags more genuine transactions as fraud.

Final Evaluation:

Among all three models, the Random Forest model performed the best overall.
It provides high accuracy, strong recall, and good precision, meaning it detects most fraudulent cases while minimizing false alerts.
Hence, Random Forest is the most effective and balanced model for fraud detection in this project.

8. Feature Importance

Figure 8.1



Feature importance analysis revealed that the 'amt' (transaction amount) was the most significant feature in predicting fraud. Other features such as transaction time and merchant location also contributed moderately.

9. Key Insights and Conclusion

1. Fraudulent transactions are rare and typically involve higher transaction amounts.
2. Balancing the data using SMOTE improved the model's fraud detection capability.
3. Random Forest outperformed other models in accuracy and recall.
4. Feature scaling and encoding significantly enhanced model performance.

In conclusion, machine learning techniques such as Random Forest can effectively identify fraudulent transactions and help reduce financial losses. Future improvements may include deep learning models and real-time fraud detection systems.