**Dataset(Kaggle):**

This dataset was inspired by real-world transaction data but was generated synthetically to avoid privacy concerns. It includes key features that play a critical role in fraud detection, such as transaction amounts, device types, geographic locations, card type, and a "fraud" label indicating whether a transaction is suspicious.

Comprehensive Transaction Categories: Transactions span categories like Travel,retail (online and in-store), groceries, restaurants (fast food to premium), entertainment (streaming, gaming, events), healthcare, education, gas, and travel.

Geographic and Demographic Variety: The dataset includes data for European country (France,Germany) allowing for analysis with varying risk profiles.

**Data Preprocessing**

Data Cleaning & Preprocessing  
**Content:**

* Dropped irrelevant columns such as transaction\_id, customer\_id, and card\_number.
* Converted timestamp to datetime format and extracted features like transaction hour, weekday, and time of day.
* Extracted key details from JSON-like columns such as num\_transactions\_last\_hour, total\_amount\_last\_hour
* Table before cleaning:
* A screenshot of a computer

  AI-generated content may be incorrect.
* After cleaning
* A screen shot of a computer code

  AI-generated content may be incorrect.

**Feature Engineering**

**Content:**

* Removed weakly correlated features like transaction\_hour.
* Created new fraud indicators:
  + High Transaction Flag (num\_transactions\_last\_hour > threshold)
  + High Spending Flag (total\_amount\_last\_hour > threshold)
  + Long Distance Spending Flag (distance\_from\_home > threshold & amount > threshold)
  + Velocity-based Risk Score combining num\_transactions\_last\_hour & total\_amount\_last\_hour.

A screenshot of a computer screen

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

A green and black graph

AI-generated content may be incorrect.

Why Log Transformation:

* **Improves Model Learning**: Many ML models (XGBoost) work better with **normally distributed data**.
* **Reduces Outlier Effects**: Large fraudulent transactions don’t dominate smaller normal transactions.
* **Prevents Bias**: Helps models focus on relative differences rather than absolute size.

**Feature Scaling**

* Used Standard Scaling (Z-score normalization) for:
  + log\_amount, num\_transactions\_last\_hour, total\_amount\_last\_hour, velocity\_risk\_score.
* Ensured proper encoding of categorical variables (Label Encoding)

A screenshot of a computer

AI-generated content may be incorrect.

Before feature scaling

After feature scaling scaled values:

A screenshot of a computer

AI-generated content may be incorrect.

* + High performance on imbalanced datasets.
  + Strong feature importance analysis.
* Augmented with anomaly detection models (LOF & Isolation Forest) for hidden fraud detection.

| **Model** | **Pros** | **Cons** | **Why Not Selected?** |
| --- | --- | --- | --- |
| **Logistic Regression** | Simple & interpretable | Poor at detecting complex fraud patterns | Fraud is complex, requires non-linear models |
| **Random Forest** | Good accuracy, less overfitting | Slower than XGBoost | Works well, but XGBoost performs better |
| **XGBoost (Selected)** | **Handles imbalanced data well, fast, high accuracy** | Needs hyperparameter tuning | **Best choice for fraud detection** |

A screenshot of a graph

AI-generated content may be incorrect.

XGBoost model evaluation:

A screenshot of a graph

AI-generated content may be incorrect.

The model **is** highly confident **in** predicting legitimate transactions (very few false positives)**.**

However, the fraud precision **is** lower (72.69**%**), meaning some legitimate transactions are incorrectly flagged **as** fraud (false positives)**.**

Recall (No Fraud: 97.27**%**, Fraud: 95.28**%**)

The model captures 95.28**%** of actual fraud cases, meaning very few fraud cases are missed**.**

This **is** a great recall score **for** fraud detection, showing that the model **is** effective **in** capturing fraudulent transactions**.**

F1**-**Score (No Fraud: 98.44**%**, Fraud: 82.46**%**)

The fraud F1**-**score **is** 82.46**%**, which **is** a good balance of precision **and** recall**.**

Some false positives exist, but they might be acceptable to avoid missing real fraud cases**.**

Overall Accuracy (97.13**%**)

The model correctly predicts fraud**/**non**-**fraud **in** 97.13**%** of cases**.**

This **is** a strong performance but could be further improved by reducing false positives**.**

2️⃣ Confusion Matrix Analysis

Actual **/** Predicted No Fraud (0) Fraud (1)

No Fraud (0) 27,121 (**True** Negative) 759 (**False** Positive)

Fraud (1) 100 (**False** Negative) 2,020 (**True** Positive)

**False** Positives (759 cases)

These are legitimate transactions incorrectly flagged **as** fraud**.**

This might cause inconvenience to customers **and** increase manual review efforts **for** merchants**.**

We may need to adjust the risk score threshold **or** refine the model**.**

**False** Negatives (100 cases)

These are actual fraud cases that were missed**.**

This **is** a small number compared to the 2,020 correctly detected fraud cases, indicating that the model **is** effective **in** capturing fraud**.**

If reducing false negatives **is** a priority, we can fine**-**tune thresholds **or** add anomaly detection**.**

**ROC Curve & AUC Score Analysis**

AUC**-**ROC Score: 0.9402

This score (closer to 1 **is** better)**.**

It shows that the model **is** highly effective at distinguishing fraud **from** non**-**fraud**.**

Steep curve shape:

The model has high sensitivity at a low false positive rate**.**

A steep curve means most fraud cases are correctly identified before false positives increase**.**

Hybrid Model(XGboost,LOF and Isolation forest):

Model Evaluation:

A screenshot of a computer

AI-generated content may be incorrect.

A blue and white graph

AI-generated content may be incorrect.