04.07.2025

ONLINE PAYMENT FRAUD DETECTION

The project focuses on detecting fraudulent payments using machine learning techniques

Ekaterina Kuznetsova

Overview

The primary objective of this project is to develop a robust machine learning model capable of detecting fraudulent online payment transactions. With the growing number of online transactions, identifying fraudulent activity what is critical to ensuring financial security and preventing economic losses.

Dataset:

Source: Kaggle - Online Payments Fraud Detection Dataset

Details:

The dataset contains transaction-level information with labelled classes:

- Not fraud(0) for legitimate and fraud (1) transactions
- covering features such as transaction type
- amount
- balances before and after the transaction
- recipient of the transaction
- balances before and after the transaction

What are the benefits for businesses to detect fraud?

- **Predict Future Fraud Risk** - Machine learning models use past data to get better at catching new fraud patterns early
- **Detect and Prevent Fraud in Real Time to Reduce Revenue Losses** - the system uses pattern recognition and data analytics techniques to identify potential fraud rapidly
- **Keeping Customers protected and trusting the system** - proactive fraud prevention measures powered by advanced fraud analytics create a protective shield around customer assets
- **Resource Optimisation** - saves money by stopping the most significant fraud threats and less time is spent on manual investigations

Machine Learning Techniques used in Fraud Analytics:

- **Supervised learning -** predicts if a transaction is fraudulent based on past labelled data
- **Unsupervised learning -** detects new or unknown types of fraud (zero-day frauds) and identifies suspicious behaviour without needing prior fraud labels
- **Deep learning -** capture non-linear relationships and sequential behaviour in transactions
- **Natural language processing (NLP) -** analyses customer complaints, detects phishing or scam patterns in textual communication, extracts and classifies information from emails, chat logs, or social media

Implementation:

- Data Exploration & Visualisation: Understand data distributions, class imbalances and correlations.
- Model Development - Supervised Learning Technique:
  - Logistic Regression
  - **Random Forest** + using **SMOTE** (Synthetic Minority Over-sampling Technique) + **SMOTE-Tomek** (SMOTE + remove borderline noise (Tomek)
  - **XGBoost** + using **SMOTE** and **SMOTE-Tomek**
- Model Evaluation
- The best model used in the app Streamlit
- Conclusions & Insights

Why is SMOTE needed?

- You might have 98% legitimate and 2% fraudulent transactions.
- Most machine learning models are biased toward the majority class, so they might predict "not fraud" all the time and still get high accuracy —but poor fraud detection.

What does SMOTE do?

- SMOTE creates synthetic (new but realistic) examples of the minority class.

What is SMOTE-Tomek?

It is a hybrid technique that combines:

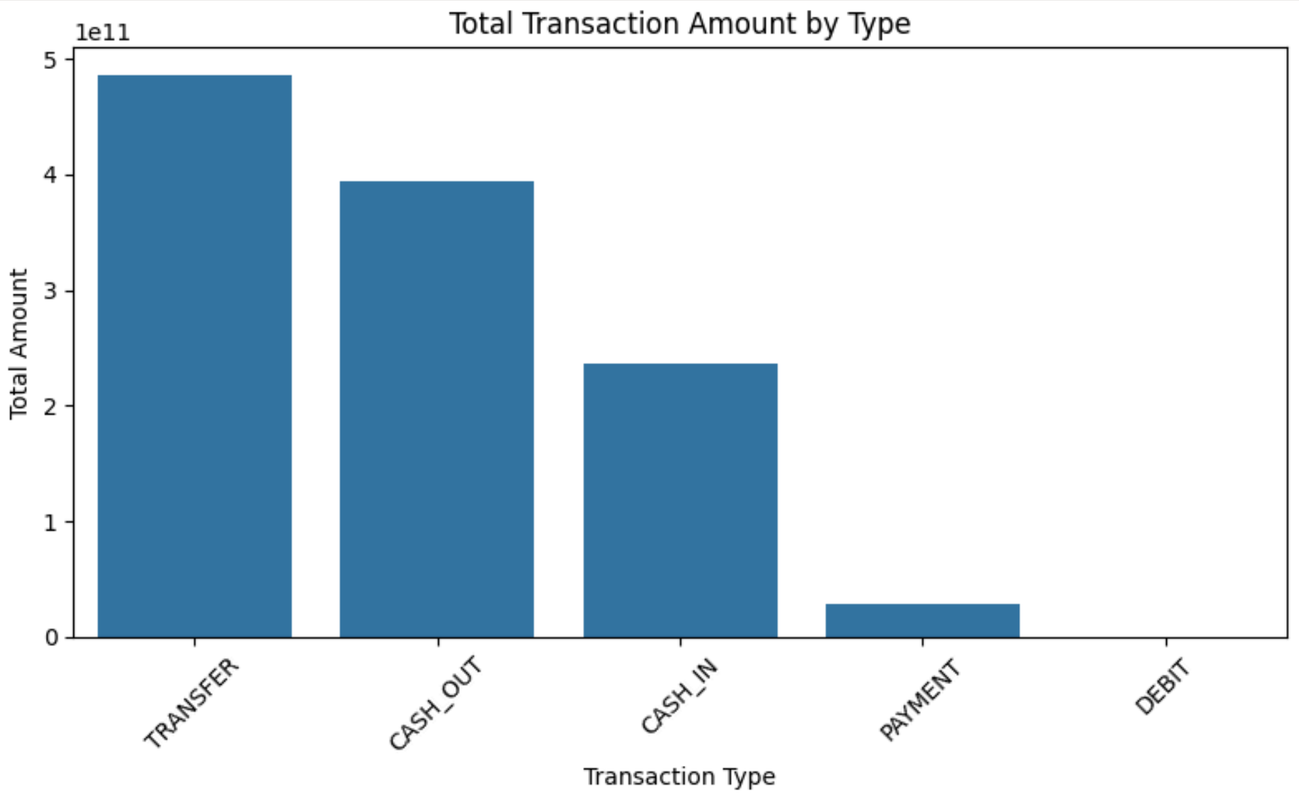
- **SMOTE** (Synthetic Minority Over-sampling Technique) – to generate synthetic minority class samples (like fraud cases), and
- **Tomek Links** – to clean the boundary between classes by removing overlapping or ambiguous majority class samples.

What does SMOTE-Tomek do?

- SMOTE creates synthetic minority samples to balance the dataset.
- Tomek Links are then used to remove noisy or overlapping majority samples, improving class separation.

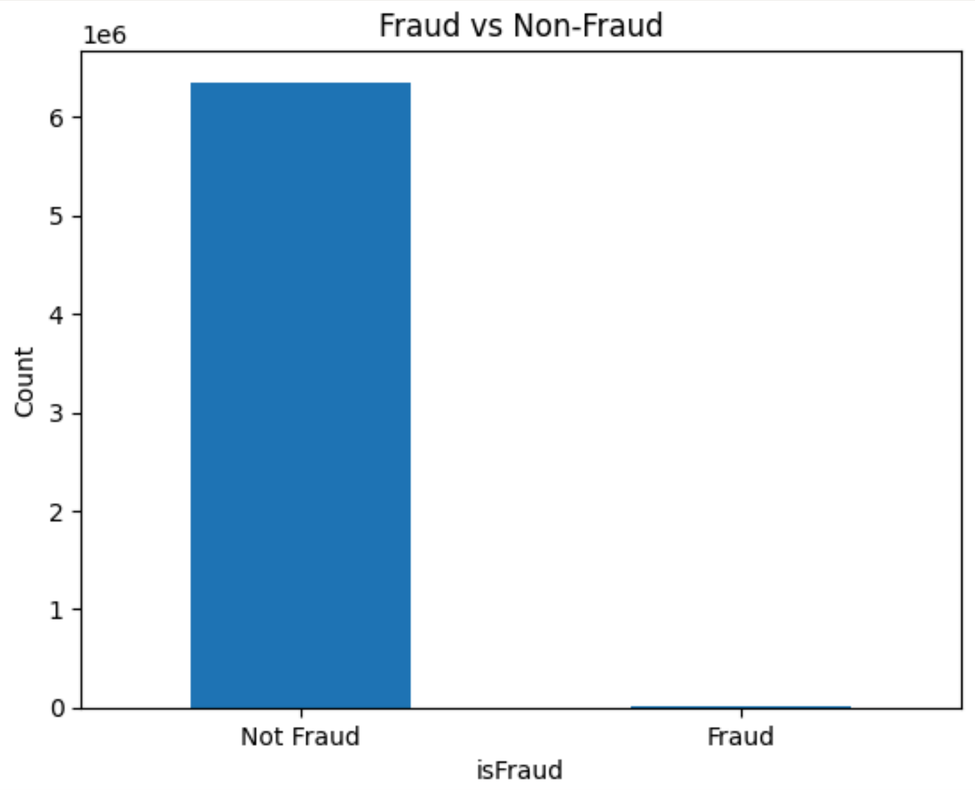
Together, SMOTE-Tomek provides: better class balance, cleaner class boundaries and improved model generalisation

Data Exploration & Visualisation




```
type
CASH_OUT    2237500
PAYMENT     2151495
CASH_IN     1399284
TRANSFER     532909
DEBIT         41432
Name: count, dtype: int64
```

Data Exploration & Visualisation

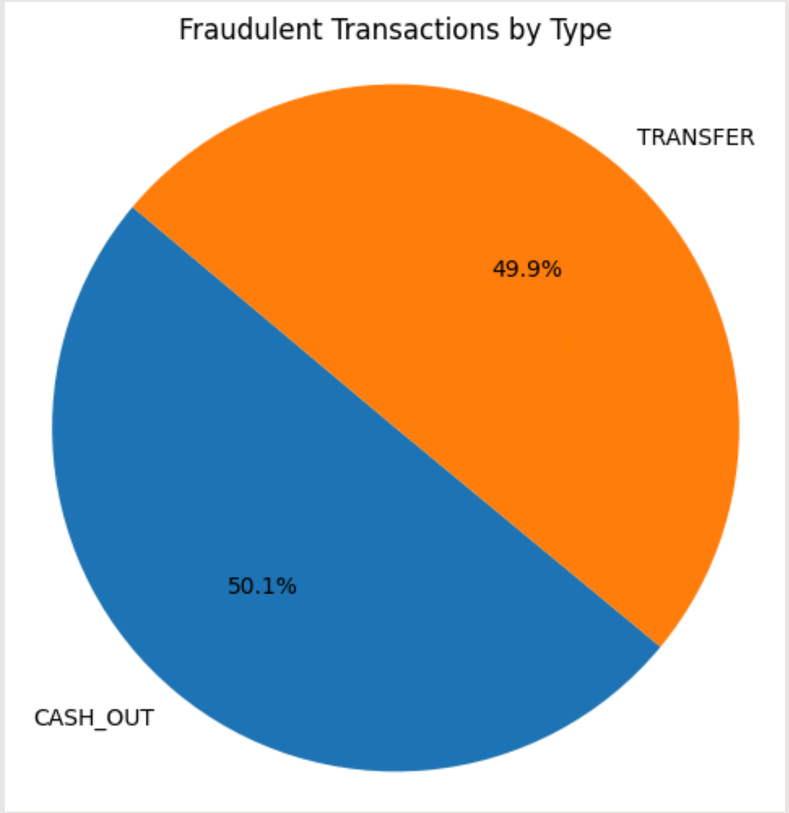



```
Class distribution:
isFraud
0    6354407
1       8213
Name: count, dtype: int64
isFraud
0    99.870918
1     0.129082
Name: proportion, dtype: float64
```

The system had a detection to flag fraudulent transactions but it didn’t recognise them

```
Missed frauds (not flagged): 8197
Total frauds in dataset: 8213
Percentage of frauds missed by flag: 99.81%
```

Fraudulent transactions



	step	type	amount	nameOrig	oldbalanceOrg	\
6062115	502	CASH_OUT	4758180.79	C1958197086	4758180.79	
3828477	282	CASH_OUT	481.90	C1550404479	481.90	
4573909	328	TRANSFER	975389.94	C891486597	975389.94	
6055689	499	TRANSFER	558136.45	C1925386760	558136.45	
1030680	84	CASH_OUT	2627070.50	C771703338	2627070.50	

	newbalanceOrig	nameDest	oldbalanceDest	newbalanceDest	isFraud	\
6062115	0.0	C350442116	0.00	4758180.79	1	
3828477	0.0	C1582825770	0.00	481.90	1	
4573909	0.0	C951633995	0.00	0.00	1	
6055689	0.0	C1909453139	0.00	0.00	1	
1030680	0.0	C1350764838	463083.63	3090154.12	1	

	isFlaggedFraud
6062115	0
3828477	0
4573909	0
6055689	0
1030680	0

```
type
CASH_OUT    4116
TRANSFER    4097
Name: count, dtype: int64
```

Model XGBoost

```
[[1270849      55]
 [    385    1235]]
              precision    recall  f1-score   support

           0       1.00      1.00      1.00   1270904
           1       0.96      0.76      0.85      1620

    accuracy                           1.00   1272524
   macro avg       0.98      0.88      0.92   1272524
weighted avg       1.00      1.00      1.00   1272524
```

True Negatives (legit transactions correctly predicted as legit)
False Positives (legit transactions incorrectly predicted as fraud)
False Negatives (fraud transactions missed by the model)
True Positives (fraud transactions correctly detected)
-Class 0: non-fraud transactions
-Class 1: fraud transactions

SMOTE

```
 [[1585363    3239]
 [     18    2035]]

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00   1588602
           1       0.39      0.99      0.56      2053

    accuracy                           1.00   1590655
   macro avg       0.69      0.99      0.78   1590655
weighted avg       1.00      1.00      1.00   1590655
```

SMOTE-TOMEK

```
  [[1268138    2743]
  [     11    1632]]
 Classification Report:
               precision    recall  f1-score   support

           0       1.00      1.00      1.00   1270881
           1       0.37      0.99      0.54      1643

    accuracy                           1.00   1272524
   macro avg       0.69      1.00      0.77   1272524
weighted avg       1.00      1.00      1.00   1272524
```

Model Random Forest

```
[[1270852      52]
 [    332    1288]]
              precision    recall  f1-score   support

           0       1.00      1.00      1.00   1270904
           1       0.96      0.80      0.87      1620

    accuracy                           1.00   1272524
   macro avg       0.98      0.90      0.94   1272524
weighted avg       1.00      1.00      1.00   1272524
```

True Negatives (legit transactions correctly predicted as legit)

False Positives (legit transactions incorrectly predicted as fraud)

False Negatives (fraud transactions missed by the model)

True Positives (fraud transactions correctly detected)

-Class 0: non-fraud transactions

-Class 1: fraud transactions

SMOTE

```
[[1587482    1120]
 [     66    1987]]
              precision    recall  f1-score   support

           0       1.00      1.00      1.00   1588602
           1       0.64      0.97      0.77      2053

    accuracy                           1.00   1590655
   macro avg       0.82      0.98      0.88   1590655
weighted avg       1.00      1.00      1.00   1590655
```

SMOTE - TOMEK

```
 [[1270031     850]
 [     41    1602]]
Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00   1270881
           1       0.65      0.98      0.78      1643

    accuracy                           1.00   1272524
   macro avg       0.83      0.99      0.89   1272524
weighted avg       1.00      1.00      1.00   1272524

Accuracy Score: 0.9992998167421597
```

Major Obstacle

- trying to use hyperparameters for Random Forest - it took a long time but didn’t help at all
- trying to find some interesting information fast without digging into the dataset
- still a lot of questions about transactions and recipients without answers but it wasn’t part of the project

Conclusion & Insights

- Most of my ideas on what to look for during the project was experience at my previous company
- Interesting to work with imbalanced data and find new tools to get better results
- A big dataset gives a lot of options to explore, however doesn’t answer all questions
- The time of transactions could help with detecting fraudulent behaviour better or finding the pattern
- There are still some options left to discover

THANK YOU