Problem 1: Anomaly Detection

Question: Develop an AI model that detects fraudulent blockchain transactions using synthetic transaction data.

Technologies Used: Python, Scikit-Learn, Flask, Pandas, Numpy

Algorithm Selection: Isolation Forest and One-Class SVM

Building Endpoint: Designed two endpoints POST and GET using REST API and Flask

A REST API endpoint, `POST /detect_fraud` implemented This endpoint takes input as blockchain data and gives probability of the transaction as fraud or not(between 0 or 1)

A REST API endpoint GET /status gives the current training status and overall health of the model

Model Training: For model training, i have taken features as [‘amount’, ‘timestamp’, ‘gas_fee’, ‘transaction_count’, ‘wallet_age’] as input to train **Unsupervised Machine Learning Algorithm**

Unsupervised learning is a machine learning technique that analyzes unlabeled data to find patterns and relationships and Unsupervised algorithms does not contain target variable

Isolation Forest: Isolation Forest is a ml algorithm that uses binary trees to identify outliers and anomalies in data.

One-Class SVM: One-Class SVM is an unsupervised learning algorithm primarily used for anomaly detection

Files Contains

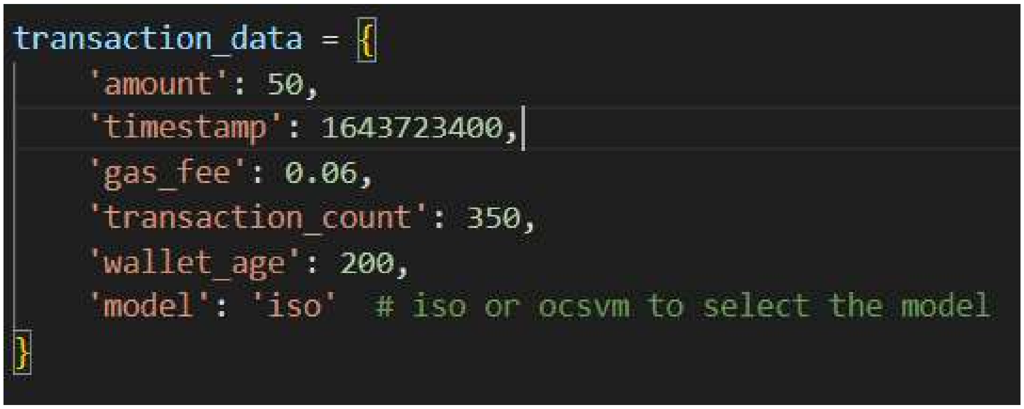
data_generator.py: contains cryptocurrency transaction data it simulates transaction details such as transaction IDs, sender and receiver addresses, transaction amounts, timestamps, gas fees, transaction counts, and wallet ages.

model_training.py: it trains and evaluates fraud detection models using Isolation Forest and One-Class SVM on synthetic transaction data. The models classify transactions as fraudulent or non-fraudulent based on key transaction features.

app.py: It is a Flask-based API provides fraud detection services using Isolation Forest and One-Class SVM. It loads a dataset, trains models, and exposes an endpoint for fraud prediction.

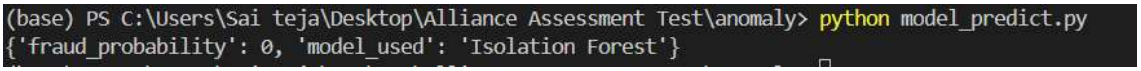
model_predict.py: it takes json as input and formulates output

Input:



```
transaction_data = {
    'amount': 50,
    'timestamp': 1643723400,
    'gas_fee': 0.06,
    'transaction_count': 350,
    'wallet_age': 200,
    'model': 'iso'  # iso or ocsvm to select the model
}
```

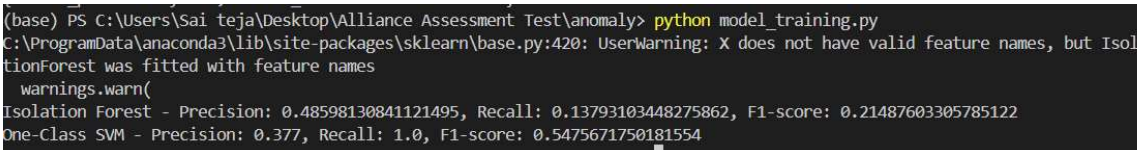
Output:



```
(base) PS C:\Users\Sai teja\Desktop\Alliance Assessment Test\anomaly> python model_predict.py
{'fraud_probability': 0, 'model_used': 'Isolation Forest'}
```

How To Run: To Run this code firstly to run **python app.py** it will run later in another terminal run **python model_predict.py** it will gives output

End Result: I achieved Precision, Recall and F1–score for models



```
(base) PS C:\Users\Sai teja\Desktop\Alliance Assessment Test\anomaly> python model_training.py
C:\ProgramData\anaconda3\lib\site-packages\sklearn\base.py:420: UserWarning: X does not have valid feature names, but Isol
tionForest was fitted with feature names
  warnings.warn(
Isolation Forest - Precision: 0.48598130841121495, Recall: 0.13793103448275862, F1-score: 0.21487603305785122
One-Class SVM - Precision: 0.377, Recall: 1.0, F1-score: 0.5475671750181554
```

And for clear elaboration i have written **anomaly_detection.ipynb**