COER UNIVERSITY
FORMERLY KNOWN AS UETR

UNIVERSITY OF OPPORTUNITIES

PROJECT PRESENTATION

AI- POWERED FRAUD DETECTION IN FINANCIAL TRANSACTION

Team- Binary Bytes

Team Members

Anil Yadav- AI&ML /2nd year

Anshul Verma- AI&ML /2nd year

Anirudh Raturi- AI&ML /2nd year

Abhishek Bhatt- AI&ML /2nd year

Introduction

Problem Statement: Credit card fraud has become one of the most significant challenges in the financial industry. With millions of transactions happening every minute, detecting fraudulent activities in real-time is crucial to prevent financial losses and protect customer trust.

Why It's Important

- Fraudulent transactions cost financial institutions and consumers billions of dollars every year.
- Manual monitoring is slow and prone to human error, leading to increased false positives and false negatives.

Key Goal: Our goal is to develop an AI-powered system that detects fraudulent transactions in real-time, ensuring quick responses to suspicious activities and minimizing financial damage.

Scope and Features

Scope

- Real-time detection of credit card fraud.
- Focus on minimizing false positives for better user experience.
- Handle various types of financial fraud (credit card, identity theft).

Key Features

- Transaction pattern analysis to identify suspicious behaviors.
- Anomaly detection to flag unusual activities.
- Automatic alerts for real-time fraud notification and action.

Data Collection and Preprocessing

Data Sources

- **Kaggle Credit Card Fraud Dataset:** A publicly available dataset that contains historical transaction data labeled as fraudulent or non-fraudulent.
- **Simulated Data:** Generated additional data using tools like Faker to create realistic transaction scenarios for testing our model.

Preprocessing Steps

- **Data Cleaning:** Identified and handled missing values, removed outliers, and corrected inconsistencies to ensure data quality.
- **Normalization:** Scaled transaction amounts and other numerical features to ensure consistent model performance across varying ranges.
- **Feature Engineering:** Created new features such as:

1. Transaction time
2. Transaction amount

Fraud Detection Algorithm

Models Used

Logistic Regression and for classification.

Training Approach

- Train-Test Split for model evaluation.
- Hyperparameter Tuning to optimize performance.

Key Metrics

- Precision: Accuracy of fraud detection (99.92 %).
- Recall: Ability to capture fraud cases.
- F1 Score: Balances precision and recall.

Future Real-time Detection SystemPlanning

System Components

- Transaction Data Stream: Real-time data input to monitor and detect suspicious transactions.
- Fraud Detection API: Built using Flask/Django, the API processes transaction data and assigns fraud risk scores.

Decision Logic

Twilio SMS Alerts: Automatically sends SMS notifications to admins or users when fraudulent transactions are detected, using Twilio.

Technologies Used

- Message Queues (e.g., Kafka, RabbitMQ) to process large transaction volumes.
- Flask for API development and integration.
- Twilio for real-time SMS alerts.

Alerting and Reporting System

Fraud Alerts

Twilio SMS Integration: Sends instant SMS alerts to admins and users when suspicious transactions are flagged.

Reporting Dashboard:

- Transaction Overview: Displays total transactions, flagged fraud cases, and false positives.
- Fraud Trends: Visualizes patterns and anomalies over time, helping to improve the detection system.
- Performance Metrics: Shows the system's accuracy, precision, recall, and F1 score for continuous monitoring and improvement.

Security and Deployment

Security

- Data Encryption: Protect sensitive transaction details.
- Secure API: Use HTTPS for safe communication.

Deployment

AWS/Heroku: Cloud hosting for handling large-scale transactions.

Testing and Validation

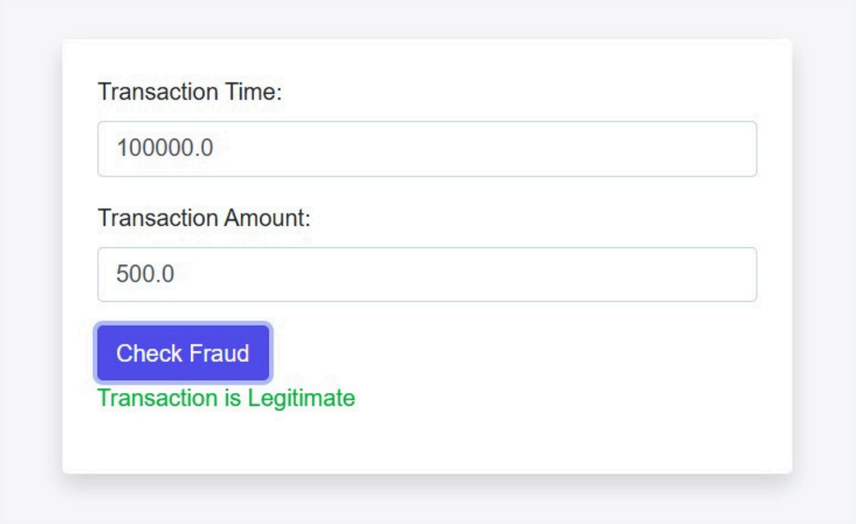
Testing Process

- Mock Transactions: Simulated transactions are run through the system to verify fraud detection accuracy.
- Performance Testing: Ensures the system can handle high transaction volumes without lag or errors.

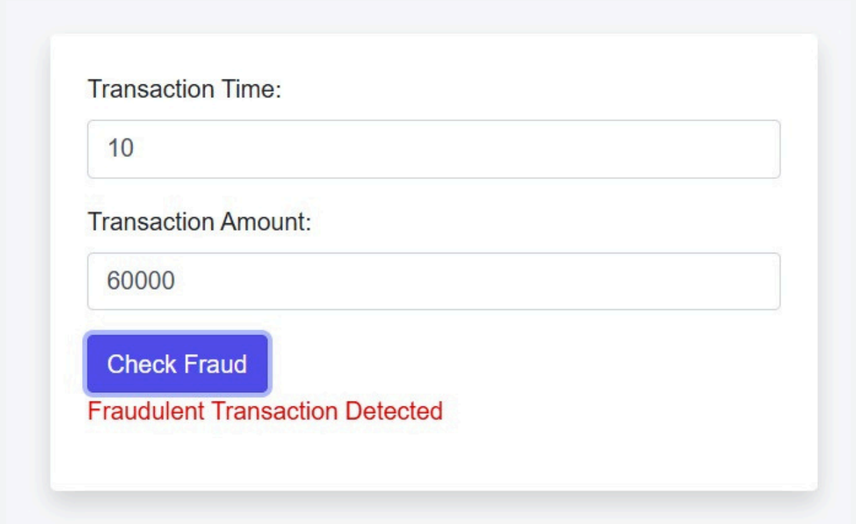
Validation Metrics

- Accuracy: Percentage of correctly identified fraud cases.
- False Positives: Focus on minimizing the number of legitimate transactions flagged as fraudulent.
- Model Tuning: Regularly fine-tuning the model to improve detection rates and reduce errors.

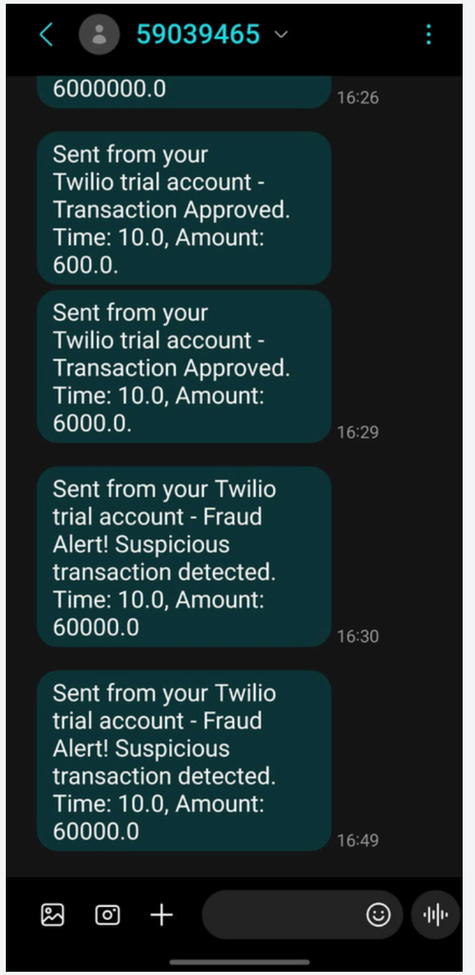
Fraud Detection in Action



(i) When the transaction is legit



(ii) When the transaction is fraud



THANK YOU