Online Payment Fraud Detection using Machine Learning

Team Members :-	
	Student 1 (Team Lead)
	Student 2
	Student 3
	Student 4
Team ID :-	LTVIP2026TMIDS55701

Project Overview:

Online Payment Fraud Detection using Machine Learning is a proactive, data-driven approach to identify and prevent fraudulent activities during online transactions. By leveraging historical transaction data, customer behavior patterns, and machine learning algorithms, this project aims to detect potential fraud in real time, ensuring secure and trustworthy online payment experiences for users and businesses alike. The goal is to provide timely alerts and actionable predictions to financial institutions, payment gateways, and e-commerce platforms to minimize the financial and reputational impact of online fraud.

Scenario 1: Real-time Fraud Monitoring

One of the primary use cases is the development of a real-time fraud monitoring system for online payment platforms. By analyzing transaction features such as transaction amount, type, and account balance changes, the system can flag suspicious transactions for immediate review, preventing fraudulent activities before they are completed.

Scenario 2: Fraudulent Account Detection

Machine learning models can detect patterns indicative of fraudulent accounts. By analyzing behavioral patterns over time — including unusual transaction types, sudden large transfers, and inconsistencies between old and new account balances — the system can identify and flag potentially compromised accounts, protecting legitimate users and businesses from financial harm.

Scenario 3: Adaptive Fraud Prevention

The system adapts and improves its fraud detection capabilities over time. By continuously learning from new transaction data and comparing multiple classification algorithms, it can stay ahead of evolving fraud techniques and provide ongoing protection for businesses and their customers against online payment fraud.

Technical Architecture:

The system is built on a 3-tier architecture comprising a Presentation Layer (HTML5/Bootstrap 5 web interface), a Logic Layer (Flask server managing data preprocessing and model inference), and a Data/Model Layer (Pickle-serialized ML model and CSV training dataset). User inputs transaction data through the web UI; the Flask backend performs Label Encoding and passes the feature vector to the trained classifier, which returns a real-time FRAUD or NOT FRAUD prediction displayed on the UI.

Pre-Requisites:

To complete this project, you must require the following software, concepts, and packages.

VS Code / Anaconda Navigator:

- Refer to the link to download VS Code: https://www.youtube.com/watch?v=mIVB-SNycKI
- Or download Anaconda Navigator from: https://www.anaconda.com/products/navigator

Python packages:

- Open Anaconda prompt as administrator and type "pip install numpy" and click enter.
- Open Anaconda prompt as administrator and type "pip install pandas" and click enter.
- Open Anaconda prompt as administrator and type "pip install scikit-learn" and click enter.
- Open Anaconda prompt as administrator and type "pip install matplotlib" and click enter.
- Open Anaconda prompt as administrator and type "pip install pickle-mixin" and click enter.
- Open Anaconda prompt as administrator and type "pip install seaborn" and click enter.
- Open Anaconda prompt as administrator and type "pip install Flask" and click enter.
- Open Anaconda prompt as administrator and type "pip install xgboost" and click enter.

Prior Knowledge:

You must have prior knowledge of the following topics to complete this project.

- ML Concepts — Supervised learning, classification algorithms
- Supervised learning: https://www.youtube.com/watch?v=QeKshry8pWQ&t;=3s
- Model Evaluation Metrics (Accuracy, Precision, Recall, F1-Score)
- Flask web framework basics: https://www.youtube.com/watch?v=lj4I_CvBnt0

- Python programming fundamentals and pandas/numpy data manipulation