Online Payments Fraud Detection System

Project Overview

The Online Payments Fraud Detection system is a proactive 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.

Scenarios Addressed:

1. Real-time Fraud Monitoring

The system continuously monitors transactions in real time, analyzing features like amount, location, device, and behavior to flag suspicious activities.

2. Fraudulent Account Detection

Machine learning models detect patterns indicative of fraudulent accounts or activities based on user behavior over time.

3. Adaptive Fraud Prevention

The system adapts and improves its fraud detection capabilities by learning from new data and adjusting algorithms against evolving fraud trends.

Technical Architecture

- Machine Learning Model

A RandomForestClassifier is trained on payment datasets to classify transactions as legitimate or fraudulent based on numerical and categorical features.

- Bac

A RESTful API built with Flask (Python) that serves the trained machine learning model. It receives transaction details via POST requests and returns a risk score and classification in milliseconds.

- Fro

A modern, responsive, and visually appealing web dashboard. It allows users to simulate transactions and instantly visualizes the transaction risk assessment, mimicking a real-time monitoring interface.

Online Payments Fraud Detection System

Project Value

Provides automated, low-latency transaction vetting to significantly reduce chargebacks and protect both merchants and customers from financial loss.