Online Payments Fraud Detection System

Detailed Project Documentation

1. Introduction

This project focuses on detecting fraudulent online transactions using Machine Learning. It analyzes transaction features and predicts whether a transaction is fraudulent or legitimate.

2. Problem Statement

With the growth of digital payments, online fraud has increased significantly. Manual fraud detection methods are inefficient. An automated ML-based solution is required.

3. Objectives

- Build a fraud detection model using ML algorithms.
- Compare multiple models and select the best performer.
- Deploy the model using Flask for real-time prediction.

4. System Architecture

Dataset → Data Preprocessing → Exploratory Data Analysis → Model Training → Model Evaluation → Model Saving → Flask Integration → User Prediction Interface.

5. Modules Description

- Data Preprocessing: Cleaning and handling missing values.
- EDA: Visualization using Matplotlib and Seaborn.
- Model Training: Logistic Regression, Random Forest, etc.
- Deployment: Flask web application.

6. Technologies Used

Python, Pandas, NumPy, Scikit-learn, Matplotlib, Seaborn, Flask, HTML, CSS.

7. Model Evaluation

Models evaluated using Accuracy, Precision, Recall, and F1-Score. Random Forest showed best performance.

8. Results

The final model successfully predicts fraudulent transactions with high accuracy and provides real-time results through the web interface.

9. Advantages

- Automated fraud detection.
- High accuracy.
- Fast prediction time.

10. Limitations

- Requires large dataset for better performance.
- May produce false positives.

11. Future Enhancements

- Cloud deployment (AWS/Heroku).
- Real-time streaming fraud detection.
- Deep learning-based improvements.