

ONLINE PAYMENTS FRAUD DETECTION

Milestone 1: Project Initialization and Planning Phase

The "Project Initialization and Planning Phase" marks the project's outset, defining goals, scope, and stakeholders. This crucial phase establishes project parameters, identifies key team members, allocates resources, and outlines a realistic timeline. It also involves risk assessment and mitigation planning. Successful initiation sets the foundation for a well-organized and efficiently executed machine learning project, ensuring clarity, alignment, and proactive measures for potential challenges.

Activity 1: Define Problem Statement

Problem Statement: "Online payment fraud is a major issue impacting consumers and financial institutions alike. As the volume of online transactions continues to grow, so does the risk of fraudulent activities. Traditional fraud detection methods, which rely heavily on static rules and manual reviews, are proving inadequate against sophisticated and evolving fraud tactics. These outdated methods struggle to keep up with new fraud patterns and often result in high false positive rates, causing legitimate transactions to be flagged and frustrating customers.

To address these challenges, a machine learning-based system can be developed to enhance the detection accuracy of fraudulent transactions. This system will utilize advanced algorithms such as Random Forest, Decision Tree, ExtraTrees, SVM, and XGBoost to accurately classify transactions in real-time. The goal is to minimize false positives and negatives, adapt to emerging fraud patterns, and ensure data security throughout the detection process. By implementing this solution, we aim to protect financial institutions and their customers from significant financial losses and maintain trust in online payment systems."

Problem Statement Report: [Click here](#)

Activity 2: Project Proposal (Proposed Solution)

"Developing a predictive model using machine learning techniques that accurately estimates individual medical costs based on demographic and health-related features, thereby aiding healthcare providers and insurers in budgeting, risk assessment, and personalized patient care."

Project Proposal Report: [Click here](#)

Activity 3: Initial Project Planning

"Initial Project Planning involves outlining key objectives, defining scope, and identifying stakeholders for an online payments fraud detection system. It encompasses setting timelines, allocating resources, and determining the overall project strategy. During this phase, the team establishes a clear understanding of the dataset, formulates goals for analysis, and plans the workflow for data processing. Effective initial planning lays the foundation for a systematic and well-executed project, ensuring successful outcomes."

Project Planning Report: [Click here](#)

Milestone 2: Data Collection and Preprocessing Phase

The Data Collection and Preprocessing Phase involves executing a plan to gather relevant medical cost data from Kaggle, ensuring data quality through verification and addressing missing values. Preprocessing tasks include cleaning, encoding, and organizing the dataset for subsequent exploratory analysis and machine learning model development.

Activity 1: Data Collection Plan, Raw Data Sources Identified, Data Quality Report

The dataset for "Online Payments Fraud Detection" is sourced from Kaggle, a reputable platform known for its extensive collection of datasets in financial services and predictive analytics. This dataset includes transaction types, amounts, account details, and historical fraud patterns. Data quality is ensured through thorough verification processes, addressing missing values, handling outliers, and maintaining adherence to ethical guidelines. These steps establish a reliable foundation for developing predictive models to accurately detect and prevent fraudulent transactions.

Data Collection Report: [Click here](#)

Activity 2: Data Quality Report

The dataset for "Online Payments Fraud Detection" is sourced from Kaggle. It includes transaction types, amounts, account details, and historical fraud patterns. Data quality is ensured through thorough verification processes, including addressing missing values, handling outliers, and maintaining adherence to ethical guidelines. These measures establish a reliable foundation for predictive modeling, ensuring the data's integrity and effectiveness in detecting fraudulent transactions.

Data Quality Report: [Click here](#)

Activity 3: Data Exploration and Preprocessing

Data Exploration involves analyzing the transaction dataset to understand patterns, distributions, and outliers. Preprocessing includes handling missing values, scaling numerical features, and encoding categorical variables. These crucial steps enhance data quality, ensuring the reliability and effectiveness of subsequent analyses in the fraud detection project. Proper data exploration and preprocessing are fundamental to developing accurate and robust predictive models to identify and prevent fraudulent transactions.

Data Exploration and Preprocessing Report: [Click here](#)

Milestone 3: Model Development Phase

The Model Development Phase involves crafting a predictive model for online payments fraud detection. It encompasses strategic feature selection, evaluating and selecting models (Random Forest Classifier, Decision Tree Classifier, Extra Trees Classifier, Support Vector Classifier, XGBoost), initiating training with code, and rigorously validating and assessing model performance. This phase aims to build a robust model that accurately identifies fraudulent transactions, enhancing the security and reliability of online payment systems.

Activity 1: Feature Selection Report

The Feature Selection Report outlines the rationale for selecting specific features (e.g., transaction amount, transaction type, merchant category, user location, etc.) for the online payments fraud detection model. It evaluates their relevance, importance, and impact on predictive accuracy, ensuring the inclusion of key factors that influence the model's ability to detect and prevent fraudulent transactions effectively.

Feature Selection Report: [Click here](#)

Activity 2: Model Selection Report

The Model Selection Report details the rationale behind choosing Random Forest Classifier (RFC), Decision Tree Classifier (DTC), Support Vector Machine (SVM), and XGBoost (XGB) models for online payments fraud detection. It considers each model's strengths in handling complex relationships, interpretability, adaptability, and overall predictive performance. This ensures an informed choice aligned with project objectives, aiming to effectively detect and prevent fraudulent transactions in online payment systems.

Model Selection Report: [Click here](#)

Activity 3: Initial Model Training Code, Model Validation and Evaluation Report

The Initial Model Training Code involves implementing selected algorithms (Random Forest Classifier, Decision Tree Classifier, Support Vector Machine, XGBoost) on the dataset for online payments fraud detection. This lays the foundation for predictive modeling. The subsequent Model Validation and Evaluation Report rigorously assesses each model's performance using metrics such as accuracy, precision, and recall. This ensures the reliability and effectiveness of the models in identifying and preventing fraudulent transactions in online payment systems.

Model Development Phase Template: [Click here](#)

Milestone 4: Model Optimization and Tuning Phase

The Model Optimization and Tuning Phase involves refining machine learning models for peak performance. It includes optimized model code, comparing performance metrics, and justifying the final model selection for enhanced predictive accuracy and efficiency.

Activity 1: Hyperparameter Tuning Documentation

The Random Forest model was selected for its superior performance, exhibiting high accuracy during hyperparameter tuning. Its ability to handle complex relationships, minimize overfitting, and optimize predictive accuracy aligns with project objectives, justifying its selection as the final model.

Activity 2: Performance Metrics Comparison Report

The Performance Metrics Comparison Report contrasts the baseline and optimized metrics for various models, specifically highlighting the enhanced performance of the Random Forest model. This assessment provides a clear understanding of the refined predictive capabilities achieved through model optimization.

Activity 3: Final Model Selection Justification

The Final Model Selection Justification articulates the rationale for choosing Random Forest as the ultimate model. Its exceptional accuracy, ability to handle complexity, and successful optimized the model align with project objectives, ensuring optimal fraud detection's.

Model Optimization and Tuning Phase Report: [Click here](#)

Milestone 5: Project Files Submission and Documentation

For project file submission in GitHub , Kindly click the link and refer to the flow.

[CLICK HERE](#)

Milestone 6: Project Demonstration

For project demonstration video kindly refer GitHub [Click here](#)

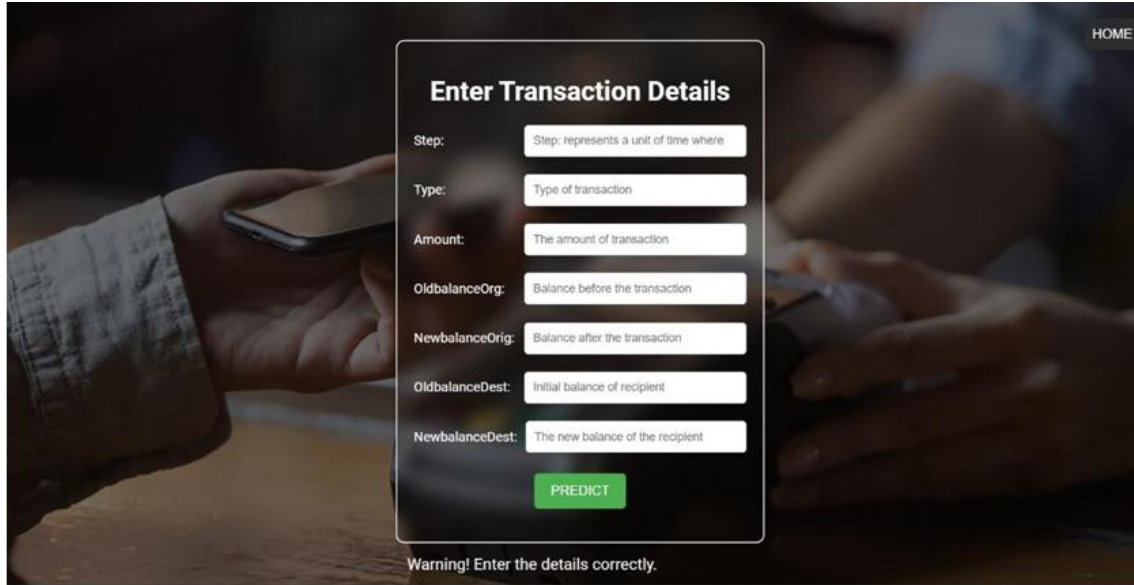
For same video access that from google drive [Click here](#)

The following images shows the output of my project:

Home Page:



Prediction Page:



The screenshot shows a web application interface for entering transaction details. The background is a blurred image of hands holding a smartphone. A dark overlay contains a form titled "Enter Transaction Details". The form has seven input fields, each with a label and a placeholder text. A green "PREDICT" button is at the bottom of the form. Below the form, a warning message is displayed. In the top right corner of the overlay, there is a "HOME" link.

HOME

Enter Transaction Details

Step: Step: represents a unit of time where

Type: Type of transaction

Amount: The amount of transaction

OldbalanceOrig: Balance before the transaction

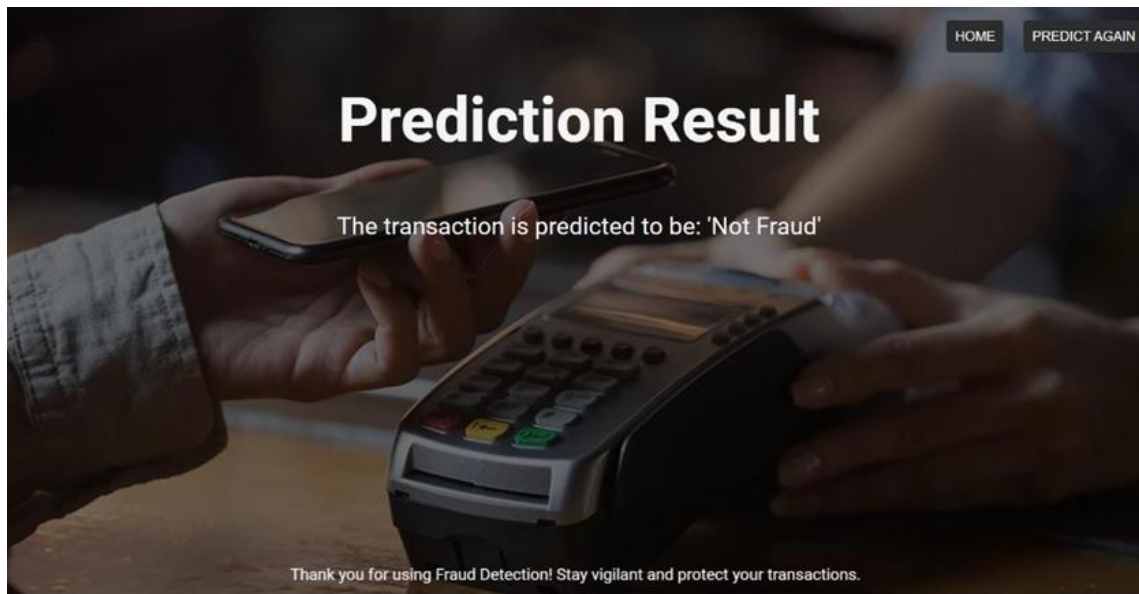
NewbalanceOrig: Balance after the transaction

OldbalanceDest: Initial balance of recipient

NewbalanceDest: The new balance of the recipient

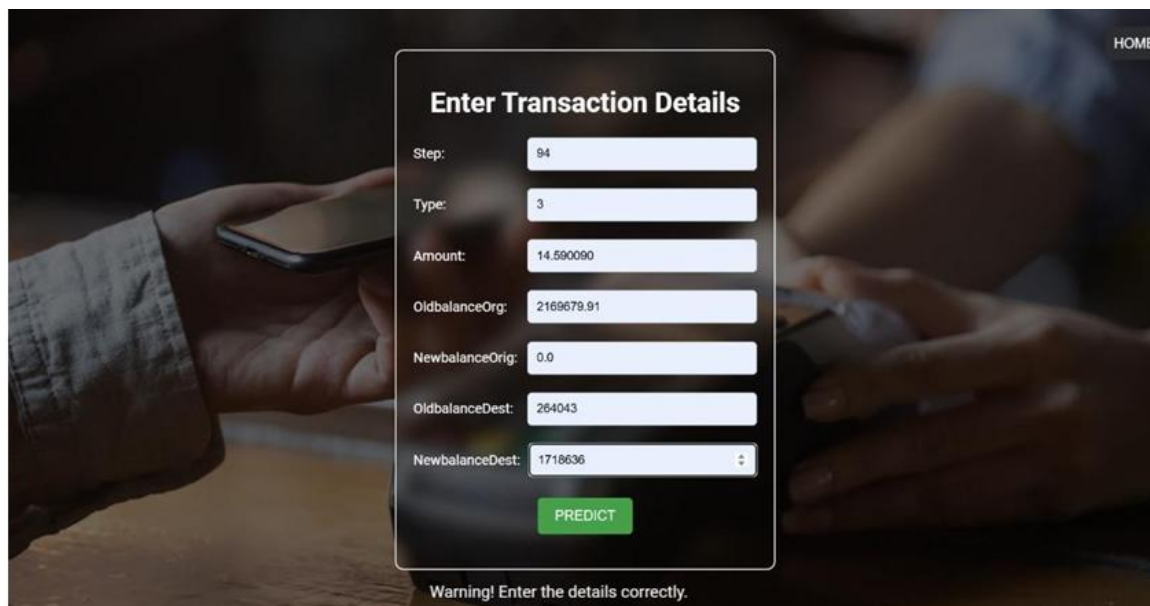
Warning! Enter the details correctly.

Result Page:



PREDICTIONS:

Prediction-1



HOME

Enter Transaction Details

Step:

Type:

Amount:

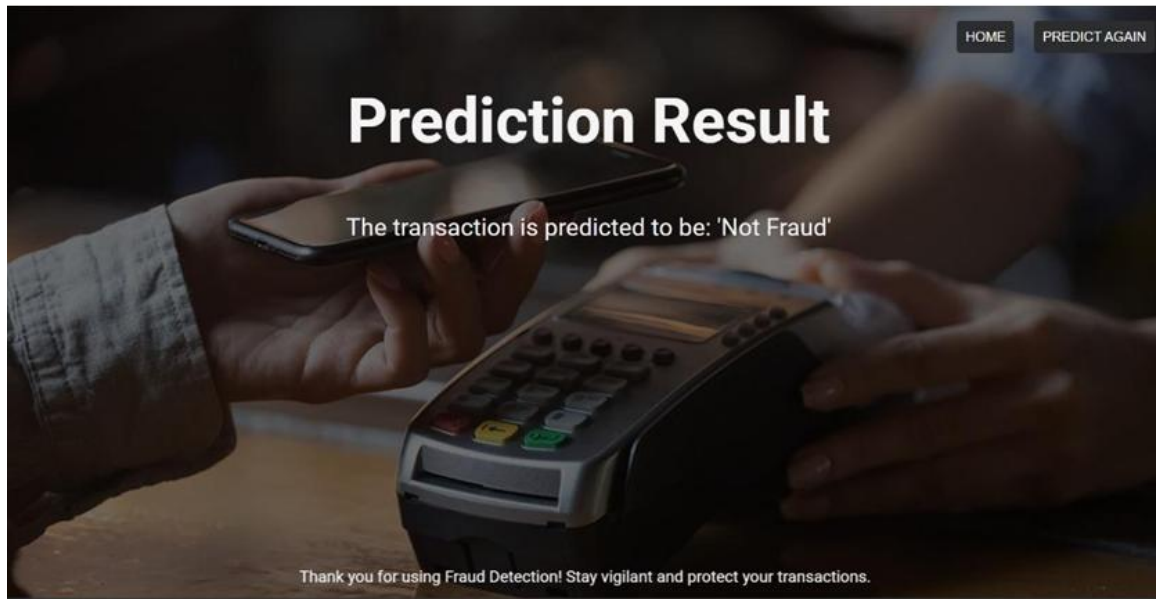
OldbalanceOrg:

NewbalanceOrig:

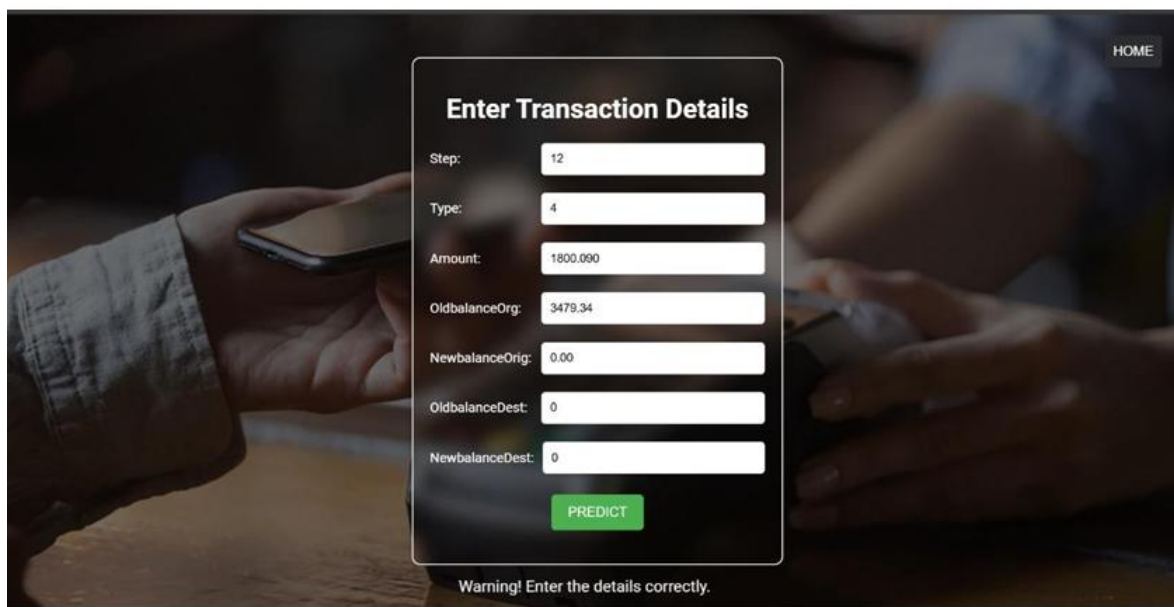
OldbalanceDest:

NewbalanceDest:

Warning! Enter the details correctly.



Prediction-2



The screenshot displays a web application interface for entering transaction details. The background is a blurred image of a person's hand holding a smartphone over a payment terminal. The main heading is "Enter Transaction Details" in white text. Below the heading, there are several input fields with labels and values: "Step:" with value "12", "Type:" with value "4", "Amount:" with value "1800.090", "OldbalanceOrig:" with value "3479.34", "NewbalanceOrig:" with value "0.00", "OldbalanceDest:" with value "0", and "NewbalanceDest:" with value "0". A green "PREDICT" button is located below the input fields. At the bottom, a warning message reads: "Warning! Enter the details correctly." In the top right corner, there is a "HOME" button.

