Phase-1 Submission Template

Guarding transactions with AI-powered credit card fraud detection and prevention

Student Name: KANISH KUMAR.R

Register Number: 620123106047

Institution: AVS ENGINEERING COLLEGE

Department: ELECTRONIC COMMUNICATION ENGINEERING

Date of Submission: 30-04-2025

1. Problem Statement

With the rise of digital transactions, credit card fraud has become an increasingly serious issue. Millions of people fall victim to fraudulent transactions every year, leading to substantial financial losses for consumers and institutions alike. The goal of this project is to build an AI-powered system that can detect and prevent fraudulent credit card transactions in real-time, thereby safeguarding customers and enhancing trust in financial services.

2. Objectives of the Project

This project aims to create a predictive model capable of accurately identifying potentially fraudulent transactions. Key objectives include:

- Analyze transaction patterns to detect anomalies

- Build and evaluate machine learning models for fraud detection

- Minimize false positives while maximizing true fraud detection

- Provide insights into key features contributing to fraud

- Propose a preventive framework for real-time detection

3. Scope of the Project

The project focuses on analyzing transaction data to detect fraudulent activity. It includes model training, evaluation, and potential integration into financial platforms. Limitations include restricted access to real-time financial data and reliance on pre-available public datasets. The project will not include actual transaction blocking but will simulate detection scenarios.

4. Data Sources

The dataset used for this project is a public credit card transaction dataset available on Kaggle, containing anonymized transaction records. This dataset is static and publicly available, ideal for model training and evaluation.

5. High-Level Methodology

- Data Collection – Download the dataset from Kaggle.
- Data Cleaning – Handle missing values, check for duplicates, and normalize data.
- Exploratory Data Analysis (EDA) – Use statistical analysis and visualization (e.g., histograms, correlation maps).
- Feature Engineering – Create new features based on transaction patterns and timing.
- Model Building – Train classification models such as Logistic Regression, Random Forest, XGBoost, and Neural Networks.
- Model Evaluation – Evaluate using metrics like Accuracy, Precision, Recall, F1-score, and AUC-ROC.
- Visualization & Interpretation – Visualize performance metrics and feature importance using plots and dashboards.
- Deployment – Prototype a web-based fraud detection dashboard using Streamlit.

6. Tools and Technologies

- Programming Language – Python

- Notebook/IDE – Google Colab, Jupyter Notebook
- Libraries – pandas, numpy, seaborn, matplotlib, scikit-learn, XGBoost, TensorFlow
- Optional Tools for Deployment – Streamlit, Flask

7. Team Members and Roles

- Member 1: [R.KANISH KUMAR] Data Collection and Preprocessing
- Member 2: [S.HARISH] Exploratory Data Analysis and Visualization
- Member 3: [M.JEEVAN] Model Building and Evaluation
- Member 4: [S.JAYAVEL] Deployment and Presentation