





Phase-1 Submission

Student Name: S. Yalini Nachiyar

Register Number: 410723104097

Institution: Dhanalakshmi college of

engineering

Department: CSE

Date of Submission: 30.04.2025

1. Problem Statements

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

2. Objectives of the Project

To develop a machine learning model capable of accurately detecting fraudulent credit card transactions.

To analyze transaction patterns and identify key indicators of fraud.

To create a real-time or near-real-time fraud detection system.

To visualize key insights for understanding fraud trends and model performance.

3. Scope of the Project

Features to be analyzed: Transaction features such as amount, time, location, merchant, user behavior, etc. - Anomaly detection based on transaction patterns. - Real-time classification of transactions as fraudulent or genuine.

4. Data Sources

- Dataset Name: Credit Card Fraud Detection - Source: Kaggle (<u>creadit card</u> <u>fraud detection</u>)- Type: Public dataset - Nature: Static dataset with anonymized features representing transactions made by European cardholders in 2013.







5. High-Level Methodology

- Data Collection —Data Collection: Download the dataset from Kaggle. - Load it into the working environment (Google Colab / Jupyter Notebook)
- **Data Cleaning** Handle missing values if any (although the Kaggle dataset is already clean). Remove duplicate entries if present. Normalize/scale features where necessary.
- Exploratory Data Analysis (EDA) Use visualizations (e.g., histograms, heatmaps, box plots) to explore class imbalance and feature distribution. Analyze relationships between features and the fraud label.
- **Feature Engineering** Derive new features like transaction velocity or user behavior metrics. Apply PCA or dimensionality reduction if needed.
- **Model Building** Derive new features like transaction velocity or user behavior metrics. Apply PCA or dimensionality reduction if needed.
- **Model Evaluation** Derive new features like transaction velocity or user behavior metrics. Apply PCA or dimensionality reduction if needed.
- Visualization & Interpretation--- Visualize model results, feature importances, and fraud detection rates using matplotlib/seaborn/Plotly.
- **Deployment** - Build a demo web app using Streamlit or Flask to simulate real-time fraud detection. Allow user input for live model predictions.

6. Tools and Technologies







- Programming Language –Python
- Notebook/IDE –Google Colab, Jupyter Notebook
- *Libraries* –pandas, numpy, seaborn, matplotlib, plotly, scikit-learn, XGBoost, TensorFlow/Keras
- Optional Tools for Deployment Streamlit, Flask, FastAPI

7. Team Members and Roles

S NO	TEAM MEMBERS	ROLES
1.	Nirosha.M	Exploratory Data Analysis
2.	Poorna kala.G	Data collection
3.	Nithyashree.S	Data Cleaning
4.	Yalini Nachiyar.S	Model Building & visualization

S