Phase-1 Submission

Student Name: LOKESH .J

Register Number: 410723104040

Institution: DHANALAKSHMI COLLEGE OF ENGINEERING

Department: COMPUTER SCIENCE AND ENGINEERING

Date of Submission: [29-04-2025]

1.Problem Statement

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

- ✓ **Increasing Fraud:** Credit card fraud is growing in volume and complexity, causing major financial losses and trust issues.
- ✓ **Weak Traditional Methods:** Rule-based systems are outdated, often inaccurate, and need AI to detect fraud more effectively and in real time.

2.Objectives of the Project

✓ Accurate Fraud Detection: Identify fraudulent credit card transactions with high accuracy using AI.

✓ Real-Time Monitoring: Enable instant analysis and detection of suspicious activities.

✓ Reduce False Positives: Minimize disruption to genuine users by lowering false alerts.

✓ Adaptive Learning: Continuously improve detection by learning from new fraud patterns.

3.Scope of the Project

- ❖ This project focuses on developing an AI-powered system to detect and prevent credit card fraud in real time. It involves analysing transaction data, identifying suspicious patterns, reducing false positives, and continuously improving through machine learning. The system aims to enhance security for financial institutions and provide a safer experience for users.

4.Data Sources

- ✓ Historical Transaction Data: Includes labelled records of legitimate and fraudulent transactions.

- ✓ User Behaviour Data: Patterns of typical user spending and transaction habits.

- ✓ Banking System Logs: Real-time transaction logs from financial institutions.

- ✓ External Threat Intelligence: Data from fraud reports, blacklists, and cybersecurity databases.

5.High-Level Methodology

- ✓ **Data Collection:** Gather transaction data from banks, institutions, or open sources, ensuring it includes both legitimate and fraudulent transactions with key features.
- ✓ **Data Cleaning:** Handle missing values, remove duplicates, correct inconsistencies, and ensure accurate fraud labels.
- ✓ **Exploratory Data Analysis (EDA):** Analyse data distribution, identify correlations, and visualize trends and anomalies.
- ✓ **Feature Engineering:** Create new features, encode categorical data, and scale numerical features.
- ✓ **Model Building:** Choose and train machine learning models, address class imbalance, and split data into training and testing sets.

- ✓ **Model Evaluation:** Evaluate performance using accuracy, precision, recall, F1-score, and ROC-AUC, and fine-tune hyperparameters.
- ✓ **Deployment:** Deploy the model in a real-time system, automate fraud alerts, and ensure low-latency processing.
- ✓ **Visualization & Interpretation:** Create dashboards to visualize performance metrics, flagged transactions, and model decision logic for stakeholders.

6.Tools and Technologies

1. Programming Language:

- Python

2. Libraries & Frameworks:

- Pandas, NumPy (data handling)
- Matplotlib, Seaborn, Portly (visualization)
- Scikit-learn, XG Boost, Light GBM (ML models)
- TensorFlow/Keres (optional - deep learning)
- Imbalanced-learn (class imbalance)

3. Tools & Platforms:

- Jupiter Notebook / Google Collab (development)
- Git & GitHub (version control)
- Flask / Fast API (deployment)
- Docker (optional - containerization)
- Power BI / Tableau (optional - dashboards)

4. Database:

- MySQL / PostgreSQL / MongoDB (data storage)

7.Team Members and Roles

S.NO	NAMES	ROLES	RESPONSIBILITY
1	LOKESH J	TEAM LEADER	DATA COLLECTING
2	BINAPALLI MANOJ	MEMBER	DATA CLEANING AND FEATURE ENGINEERING
3	GUNA SEKHER REDDY	MEMBER	MODEL EVALUVATION AND MODEL BUILDING
4	POORNA CHANDRA REDDY	MEMBER	VISUALIZATION AND INTERPRETATION
5	ERUGU PURUSHOTHAM	MEMBER	EXPLORATORY DATA ANALYSIS