# Project Initialization and Planning Phase

| | |
|---|---|
| Date | 15 July 2024 |
| Team ID | team-739735 |
| Project Title | Online Payments Fraud Detection |
| Maximum Marks | 3 Marks |

**Project Proposal (Proposed Solution):**

The proposal report aims to predict fraudulent online transactions using machine learning, boosting efficiency and accuracy.

| **Project Overview** | |
|---|---|
| Objective | The objective of this project is to build a machine learning model that can accurately identify potentially fraudulent transactions. This involves analyzing large datasets of transaction records, extracting relevant features, and applying advanced algorithms to distinguish between legitimate and fraudulent activities. |
| Scope | The project aims to comprehensively analyze and detect fraudulent online transactions based on transaction data, user behavior, and contextual factors. By integrating machine learning into online payment systems, the goal is to enhance security, reduce financial losses, and maintain customer trust. |
| **Problem Statement** | |
| Description | Inaccurate detection of fraudulent transactions due to evolving fraud techniques and lack of robust detection models hinders financial security and trust for online merchants and payment processors. This project addresses the need for advanced predictive models to enhance fraud detection capabilities, thereby ensuring secure and reliable online payment experiences for customers and businesses. |
| Impact | Addressing these challenges will lead to improved security and trust in online payment systems, reduced financial losses due to fraudulent activities, and enhanced customer satisfaction. By providing accurate and real-time fraud detection, the project aims to mitigate risks associated with online transactions. |

| Proposed Solution | |
|---|---|
| Approach | Implementing machine learning algorithms to analyze historical transaction data and user behavior to develop a predictive model for detecting fraudulent activities in real-time. This involves data preprocessing, feature engineering, model training and evaluation, and deploying the model within the online payment system to continuously monitor and flag suspicious transactions. |
| Key Features | • **Development of a machine learning-driven model** to detect fraudulent transactions based on transaction data and user behavior patterns.<br>• **Real-time detection capabilities** to identify and prevent fraudulent activities as they occur, ensuring immediate response to threats.<br>• **Continuous model refinement** through feedback loops and updated data to adapt to evolving fraud patterns and techniques. |

**Resource Requirements**

| Resource Type | Description | Specification/Allocation |
|---|---|---|
| **Hardware** | | |
| Computing Resources | CPU/GPU specifications, number of cores | T4GPUs |
| Memory | RAM specifications | 8 GB |
| Storage | Disk space for data, models, and logs | 1 TB SSD |
| **Software** | | |
| Frameworks | Python frameworks | Flask |
| Libraries | Additional libraries | scikit-learn, pandas, numpy, matplotlib, seaborn |
| Development Environment | IDE | Jupyter Notebook, VScode |
| **Data** | | |

| | | |
|---|---|---|
| Data | Source, size, format | Kaggle, 177MB, csv |