

**Project Initialization and Planning Phase**

|  |  |
| --- | --- |
| Date | 6 JUNE 2024 |
| Team ID | 739864 |
| Project Title | Online Fraud Detection Using ML |
| Maximum Marks | 3 Marks |

**Project Proposal (Proposed Solution) template**

This project proposal outlines a solution to address a specific problem. With a clear objective, defined scope, and a concise problem statement, the proposed solution details the approach, key features, and resource requirements, including hardware, software, and personnel.

|  |  |
| --- | --- |
| **Project Overview** |  |
| Objective | Develop a machine learning system to detect and prevent online fraud in real-time. |
| Scope | Implement a scalable fraud detection system that can analyze large volumes of transaction data to identify and flag potentially fraudulent activities. The project will cover data collection, model training, and integration with existing transaction systems. |
| **Problem Statement** |  |
| Description | Online fraud is a significant issue affecting financial institutions and customers, leading to substantial financial losses and undermining trust in online services. Fraudsters continually evolve their tactics, making traditional rule-based systems insufficient |
| Impact | Solving this problem will reduce financial losses, enhance customer trust, and improve the overall security of online transactions. It will also help in identifying new fraud patterns and adapting to emerging threats more quickly. |
| **Proposed Solution** |  |
| Approach | Utilize supervised machine learning techniques, such as logistic regression, decision trees, and neural networks, to analyze historical transaction data and identify patterns indicative of fraud. The solution will involve data preprocessing, feature engineering, model training, |



|  |  |
| --- | --- |
|  | and evaluation. Continuous monitoring and model retraining will be essential to maintain accuracy as fraud patterns evolve. |
| Key Features | Real-time Analysis: The system will process and analyze transactions in real-time to detect fraudulent activities as they occur.  Adaptive Learning: The model will continually learn from new data, improving its accuracy and ability to detect emerging fraud patterns. Scalability: Designed to handle large volumes of transactions without compromising performance. |

**Resource Requirements**

|  |  |  |
| --- | --- | --- |
| **Resource Type** | **Description** | **Specification/Allocation** |
| **Hardware** |  |  |
| Computing Resources | CPU/GPU specifications, number of cores | e.g., 2 x NVIDIA V100 GPUs |
| Memory | RAM specifications | e.g., 8 GB |
| Storage | Disk space for data, models, and logs | e.g., 1 TB SSD |
| **Software** |  |  |
| Frameworks | Python frameworks | e.g., Flask , sklearn , metrics |
| Libraries | Additional libraries | e.g., scikit-learn, pandas,  numpy |
| Development Environment | IDE, version control | e.g., Jupyter Notebook, Git , Google colab |
| **Data** |  |  |
| Data | Source, size, format | e.g., Kaggle dataset, 500 images , CSV |