Project Design Phase
Proposed Solution Template

Date	8 February 2026
Team ID	LTVIP2026TMIDS48224
Project Name	Online Payments Fraud Detection using Machine Learning
Maximum Marks	2 Marks

Proposed Solution Template:

Project team shall fill the following information in the proposed solution template.

Sl.No.	Parameter	Description
1. 1	**Problem Statement (Problem to be solved)**	In the rapidly growing digital payments ecosystem, fraudulent transactions are increasing due to sophisticated attack patterns. Traditional rule-based or manual verification methods are slow, inefficient, and unable to detect complex fraud behaviours in real time. Organizations need an automated way to identify fraudulent transactions instantly to prevent financial loss.
2. 2	**Idea / Solution Description**	This project presents a **Flask-based web application** integrated with a **Machine Learning model** trained on a Kaggle online payments fraud dataset. Users enter transaction details through a simple web form, and the system predicts in real time whether the transaction is **Fraud** or **Not Fraud** using a trained model (Random Forest/XGBoost).
3. 3	**Novelty / Uniqueness**	✓ Integration of ML model with a live Flask web interface for instant predictions. ✓ Use of high-accuracy models like Random Forest and XGBoost for fraud detection. ✓ Clear separation of modules: Training, Model, and Web App. ✓ Demonstrates real-time practical use of ML in payment security.
4. 4	**Social Impact / Customer Satisfaction**	The system highlights how technology can reduce financial fraud in digital transactions. By enabling instant fraud detection, it helps protect users and organizations from monetary loss and builds trust in online payment systems.

5. 5	**Business Model (Revenue Model)**	• Although developed as an academic project, future scope may include: • **API-based Fraud Detection Service** for payment gateways and fintech apps. • **SaaS Model** for banks and e-commerce platforms to integrate fraud detection.