Project Design Phase
Problem – Solution Fit Template

Date	31 January 2026
Team ID	LTVIP2026TMIDS55701
Project Name	Online Payment Fraud Detection using Machine Learning
Maximum Marks	2 Marks

Problem – Solution Fit:

The Problem-Solution Fit simply means that you have found a problem with your customer and that the solution you have realized for it actually solves the customer's problem. It helps entrepreneurs, marketers and corporate innovators identify behavioral patterns and recognize what would work and why.

Purpose:

1. Customer Segment(s): Financial institutions (banks, credit card companies), payment gateway operators, e-commerce platforms, and end consumers conducting online transactions.

2. Jobs-to-be-done / Problems: Detecting fraudulent online payment transactions with high accuracy and providing real-time actionable classification (FRAUD / NOT FRAUD) to prevent financial loss.

3. Triggers: Unusual transaction amounts, abnormal account balance changes, high-frequency transactions in a short period, or transaction types inconsistent with user history.

4. Emotions (Before/After): Before: Anxious and financially exposed due to reactive, rule-based fraud systems. After: Confident and secure due to real-time ML-powered detection and early alerts.

5. Available Solutions: Manual transaction review processes, basic threshold-based rule engines, or generic fraud screening tools that do not adapt to evolving transaction patterns.

6. Problem Root Cause: Lack of automated, adaptive tools that can simultaneously analyze transaction amount, type, account balances, and behavioral patterns to classify fraud in real time.

7. Your Solution: A machine learning model achieving up to 79% accuracy (SVM) with five algorithms compared, deployed as a Flask web application that classifies transactions as FRAUD or NOT FRAUD through a simple, easy-to-use web interface.

Template:

1. CUSTOMER SEGMENT(S) CS • Financial institutions / banks • Payment gateway operators • E-commerce platforms • Online consumers	**5. CUSTOMER CONSTRAINTS CC** • Limited ML expertise in fraud teams • High cost of enterprise fraud platforms • Lack of labeled real-time transaction data	**5. AVAILABLE SOLUTIONS AS** • Manual transaction review • Basic rule-based threshold filters • Generic fraud screening APIs (static)
2. JOBS-TO-BE-DONE / PROBLEMS JAP • Detect fraud transactions with high accuracy • Provide real-time FRAUD / NOT FRAUD alerts • Reduce false positive rate for genuine transactions	**9. PROBLEM ROOT CAUSE RC** • Lack of automated ML tools analyzing transaction amount, type, and account balance features simultaneously	**6. BEHAVIOUR BE** • Manual review of flagged transactions • Reactive rule adjustment post-incident • Delayed fraud resolution, customer disputes
3. TRIGGERS TR • Unusual transaction amounts or types • Abnormal account balance changes • High transaction frequency anomalies • BEFORE: Anxious, financially exposed	**10. YOUR SOLUTION SL** A Flask web application with ML model (79% accuracy — SVM) that processes 7 transaction features and classifies as "FRAUD" or "NOT FRAUD" in real time.	**8. AVAILABLE SOLUTION CH ONLINE:** No directly comparable open-source real-time fraud web app **OFFLINE:** Rule-based bank systems, manual fraud investigation teams

Fig. 4: Problem-Solution Fit Canvas for Online Payment Fraud Detection. This illustrates alignment between customer problems and ML-based web application solution.