

Project Design Phase-II
Solution Requirements (Functional & Non-functional)

Date	14 February 2026
Team ID	LTVIP2026TMIDS54062
Project Name	Online Payments Fraud Detection using Machine Learning

Functional Requirements:

Following are the functional requirements of the proposed solution.

FR No.	Functional Requirement (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	User Authentication	Login through Mobile Banking App Login through Internet Banking Biometric Authentication
FR-2	Transaction Monitoring	Capture real-time transaction data Track device and location details Maintain transaction history
FR-3	Fraud Detection Engine	Apply Machine Learning Model Calculate Risk Score Perform Rule-Based Validation
FR-4	Risk Classification	Categorize transactions as Low Risk, Medium Risk, High Risk Trigger alerts for suspicious activity
FR-5	Alert & Notification System	Send SMS alerts Send Email notifications Push notifications in mobile app
FR-6	Fraud Reporting & Card Blocking	One-click card block option Fraud reporting form Automated case generation
FR-7	Dashboard & Analytics	Real-time fraud monitoring dashboard Fraud trend visualization Risk segmentation charts

Non-functional Requirements:

Following are the non-functional requirements of the proposed solution.

FR No.	Non-Functional Requirement	Description
NFR-1	Usability	The system should have a simple and user-friendly interface for customers and administrators.
NFR-2	Security	All transaction data should be encrypted using secure protocols and multi-factor authentication.
NFR-3	Reliability	The system should detect fraud accurately with minimal false positives and false negatives.
NFR-4	Performance	Fraud detection decision should be completed within 2–3 seconds per transaction.

NFR-5	Availability	The system should operate 24/7 with minimal downtime.
NFR-6	Scalability	The system should handle high transaction volumes during peak hours.
NFR-7	Compliance	The system should comply with financial regulations and data protection standards.