

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

Date	31 January 2026
Team ID	LTVIP2026TMIDS48224
Project Name	Online Payments Fraud Detection using Machine Learning
Maximum Marks	4 Marks

Functional Requirements:

Following are the functional requirements of the proposed solution.

FR No.	Functional Requirement	Description
FR-1	User Authentication & Authorization	The system must authenticate users such as administrators and fraud analysts. Role-based access control must restrict actions to authorized users only.
FR-2	Data Collection & Storage	The system should collect real-time transaction data from payment gateways and securely store it in a centralized database. Data retrieval must be supported for analysis and reporting.
FR-3	Transaction Monitoring	Real-time monitoring of transactions to detect anomalies such as unusual amounts, locations, or behavior patterns. Suspicious transactions must be flagged.
FR-4	Machine Learning Models	Implement supervised and unsupervised ML models for fraud detection. Models must support continuous training and retraining with new data.
FR-5	Alerting & Notification	Automated alerts for suspicious transactions via email, SMS, or in-app notifications to analysts/administrators.
FR-6	Case Management	Provide a case handling system for analysts to review flagged transactions, record decisions, and assign cases for investigation.

Non-functional Requirements:

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

FR No.	Non-Functional Requirement	Description
NFR-1	Performance	The system must process high volumes of transactions in real-time with minimal response delay for fraud alerts.
NFR-2	Scalability	The architecture should support horizontal scaling to handle increased transaction loads without performance degradation.
NFR-3	Security	Ensure encryption of data in transit and at rest. Strong access control and audit trails must be maintained.
NFR-4	Availability	High system uptime with redundancy and failover mechanisms to minimize downtime.
NFR-5	Compliance	Must comply with regulations such as GDPR and PCI DSS. Regular audits and compliance reports are required.
NFR-6	Usability	Provide user-friendly interfaces for fraud analysts. Include user training and support.