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

Date	30 January 2026
Team ID	LTVIP2026TMIDS90948
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 (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	Transaction Input	Capability to manually enter or upload transaction parameters (Type, Amount, Balances) through the UI.
FR-2	Real-time Prediction	Integration of the **XGBoost engine** to generate instant fraud probability scores upon data submission.
FR-3	Risk Classification	Automatic categorization of results into **Low, Medium, or High Risk** based on probability thresholds.
FR-4	Action Triggering	Providing specific recommended actions (e.g., "Freeze Account" or "Send OTP") based on the model's output.

Non-functional Requirements:

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

FR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	The Flask-based UI must be intuitive, requiring no technical knowledge to interpret the "Traffic Light" risk signals (Green, Yellow, Red).
NFR-2	**Security**	Transaction data must be handled securely; the system ensures that sensitive features like User IDs are dropped before processing to protect privacy.
NFR-3	**Reliability**	The system must consistently produce a high **F1-Score (99%)**, ensuring that legitimate transactions are not frequently blocked (minimizing False Positives).
NFR-4	**Performance**	The prediction logic (XGBoost + Pickle) must execute in **sub-millisecond time** to prevent delays in the user's payment experience.
NFR-5	**Scalability**	The architecture must be capable of handling a sudden surge in transaction volume (e.g., during holiday sales) without a drop in response time.