INTELLIGENT FRAUD DETECTION & RISK SCORING SYSTEM

Software Requirement Specification

Business Analyst Project Report
Prepared By: Soundarya S
Role: Business Analyst
Date: October 2025
Version: 1.0

SOFTWARE REQUIREMENT SPECIFICATION (SRS)

PROJECT: INTELLIGENT FRAUD DETECTION & RISK SCORING SYSTEM

DOMAIN: FINTECH

---

1. Introduction:

1.1 Purpose

This SRS provides a detailed description of the functional, non-functional, technical, and integration requirements for the Intelligent Fraud Detection & Risk Scoring System. It serves as a single source of truth for developers, QA testers, architects, and stakeholders.

1.2 Scope

The system must evaluate every transaction in real time, calculate a risk score, alert customers, trigger OTP/Face ID authentication when required, block high-risk transactions, and log incidents for fraud analysis.

1.3 Intended Users

- Business Analyst
- Development Team
- QA / Testing Team
- Product Owner
- Fraud Analysts
- Compliance Team
- Architects

1.4 Definitions

Term	Definition
Risk Score	Numerical value (0–100) used to classify transaction risk
Fraud Queue	List of transactions assigned for manual fraud review
OTP	One-Time Password
NFR	Non-Functional Requirement
High Risk	Score 80–89
Very High Risk	Score ≥ 90

2. Overall Description

2.1 Product Perspective

The system acts as a middleware layer between:

- Core Banking System
- Notification Systems (SMS/Email/Push)
- Authentication Service (OTP/FaceID)
- Fraud Management Dashboard
- Complaint Management System

It processes transactions BEFORE approval.

2.2 Product Functions

The system will:

- Analyze transaction data
- Apply fraud rules
- Generate risk score
- Trigger OTP/FaceID
- Block transactions
- Send alerts
- Log all actions
- Provide dashboard insights

2.3 Constraints

- Real-time performance < 1 second
- Integration dependency on SMS/Email gateways
- GPS/IP data availability
- Compliance with RBI guidelines

2.4 Assumptions

- Customer contact details are up-to-date
- Core banking supports real-time APIs
- Network connectivity is stable

3. Functional Requirements

(Direct extension of your FRD — formatted for SRS)

3.1 Transaction Evaluation Module

- FR-01: System must analyze every transaction in < 1 second.
- FR-02: Must capture amount, device ID, IP, GPS, ATM location, customer history.
- FR-03: Must calculate risk score using rule engine.

3.2 Risk Scoring Engine

Rule	Condition	Score
Amount Rule	> 50,000	+20
Amount Rule	> 1,00,000	+40
Device Mismatch	New device	+25
Location Mismatch	>100 km	+20
International IP	Outside India	+30
Odd Time	12AM–4AM	+15
Velocity Rule	>3 txns/min	+25
Past Fraud	History	+30
Wrong OTP	3 fails	+10

FR-04: Final risk score = total of triggered rules (max 100).

3.3 Decision Engine

Low Risk (0–59)

- Auto approve

Medium Risk (60–79)

- Approve + send warning notification

High Risk (80–89)

- Hold transaction
- Trigger OTP/Face ID
- If fails → block

Very High Risk (≥ 90)

- Block transaction
- Alert customer

- Add to Fraud Queue
- Auto-create complaint

3.4 Notification Module

FR-10: Send SMS/Email/Push within 5 seconds.

FR-11: Alert must include:

- Amount
- Location
- Time
- Device info
- “Not Me” button

3.5 Customer Response Module

FR-12: If customer clicks “Not Me”:

- Block card immediately
- Stop all outgoing transactions
- Auto-create fraud complaint
- Notify Fraud Analyst
- Update dashboard

3.6 Fraud Queue Module

FR-13: Show flagged transactions with:

- Risk score
- Reason codes
- Customer history
- Location map
- Device info

3.7 Logging & Audit Requirements

FR-14: Log every failure, OTP attempt, alert, action.

FR-15: Maintain audit logs for minimum 6 months.

4. System Architecture:

4.1 High-Level Architecture Components

- Transaction Input Layer
- Risk Scoring Engine
- Decision Engine
- Alert & Notification Service
- Authentication Service
- Fraud Queue & Dashboard
- Logging Layer
- Integration Layer

5. Data Requirements:

Field	Type	Purpose
transaction_id	String	Unique ID
customer_id	String	Customer identity
amount	Decimal	Amount
device_id	String	Device identifier
ip_address	String	User IP
gps_location	String	GPS coordinates
atm_location_id	String	ATM location code
risk_score	Integer	Final score
reason_code	String	Why flagged
timestamp	Datetime	Time of transaction

6. Integration Requirements:

6.1 External Systems

- Core Banking API
- OTP/FaceID Authentication API

- SMS/Email Gateway
- Complaint Management System
- Fraud Dashboard System

6.2 Data Flow

Transaction → Risk Engine → Decision Engine → Alerts → Queue → Dashboard

7. Non-Functional Requirements (NFR):

7.1 Performance

- Must handle 10,000 transactions/minute
- Risk scoring < 1 second

7.2 Security

- AES-256 encryption
- Masking of sensitive fields
- Audit logging

7.3 Availability

- 99.9% uptime
- Failover support

7.4 Compliance

- Must follow RBI fraud prevention guidelines

8. Acceptance Criteria (High-Level):

- Risk score must be 100% accurate based on rules
- High-risk transactions must NEVER pass without OTP/Face ID
- Alerts must reach user within 5 seconds
- User clicking “Not Me” must instantly block card
- Fraud Queue must refresh in real time
- OTP failures must be logged properly

9. Conclusion: This SRS defines the complete functional and non-functional behaviour of the Intelligent Fraud Detection & Risk Scoring System. It will be used by development, QA, and business teams to deliver a secure and efficient fraud prevention platform.