Credit Card Processing System 28/8/25

Problem statement

People need a fast, secure and reliable way to process credit card payments. Current systems face issues like fraud, delays and limited reporting. The proposed Credit Card Processing System will provide secure transactions, fraud prevention, real-time settlement and comprehensive reporting.

SRS Document

1. Introduction

1.1 Purpose

The purpose of this document is to specify the functional and non-functional requirements of the Credit Card Processing System. It serves as a guide for developers, testers and stakeholders to design, implement and validate a secure and efficient credit card transaction processing solution.

1.2 Scope

The CCPS will enable merchants to accept credit card payments securely, authorize and settle transactions with banks/payment networks, detect fraudulent activities, provide transaction history and reports, ensure compliance with PCI DDS and financial regulations. This system will support e-commerce websites, point of sale (POS) systems and mobile payment solutions.

1.3 Overview

The CCPS will act as an intermediary between merchants and banks. Customers will initiate payments through applications which will connect to the CCPS for authorization, fraud checks and settlement. The system will also provide A merchant dashboard for reporting, APIs for integration and communication protocols.

2. General Description

- The system will run on a cloud-based infrastructure.
- The architecture will be modular with seperate transactions, fraud detection and reporting modules.
- Users include Customers who make payments, Merchants who accept payments and view reports and Administrators who manage and monitor the system.
- Interfaces: API's for integration, web dashboards
- Must comply with PCI DPS, support high transaction volumes and ensure 99.9% availability.

3. Functional Requirements.

- Accept and validate credit card details
- Authorize transactions with issuing banks
- Perform fraud checks
- Complete settlements and fund transfers
- Handle refunds and chargebacks

provide transaction reports
support secure merchant login and API authentication

Interface Requirements

- Web - based merchant dashboard (secure login, responsive)
- Uses API's like Bank / payment network APIs
- POS terminals and card readers
- HTTPS with TLS 1.3 encryption.

Performance Requirements

- Transaction authorization time should be less than 2 seconds.
- System throughput: 1000 transactions per second
- Availability: 99.9% uptime
- scalability: Must support 1M+ concurrent users.

Design Constraints.

- Must follow PCI DPI compliance for data handling
- AES 256 encryption, TLS 1.3 for transmission
- Database must support audit logs for 7 years
- ~~Ba~~ Compatible APIs

Non-functional Attributes.

- Security: End to end encryption, fraud detection, secure authentication.
- Reliability: Automatic failover, backup

recovery system

- Usability: Intuitive dashboard for responsive design.
- Portability: Cloud-based, accessible via and mobile devices.

8. Preliminary Schedule and Budget

Week 1-2: Requirement analysis & design

3-6: Development of transaction and module.

7-9: Fraud detection and settlement module.

10-12: Merchant dashboard and API integration

13-14: Testing

15: Deployment and user training

Budget:

Requirement analysis - ₹ 2,00,000

System Design - ₹ 4,00,000

Implementation - ₹ 3,50,00

Testing - ₹ 2,00,000

Deployment - ₹ 3,00,000

Total - ₹ 14,50,000