CS 331 (Software Engineering Lab)

Assignment 4

Automated Fraud Detection System

SHASHANK LODHI

I. CHOOSE AN APPROPRIATE SOFTWARE ARCHITECTURE STYLE

Selected Architecture Style: LAYERED ARCHITECTURE

- The Automated Fraud Detection System follows a Layered Architecture.
- The system is divided into logical layers where each layer has a defined responsibility.
- Each layer performs specific tasks and communicates only with adjacent layers.
- This ensures modularity, maintainability and structured interaction between components.

A. JUSTIFICATION BASED ON GRANULARITY AND RESPONSIBILITIES

1. PRESENTATION LAYER

- Provides user interfaces for Bank Customers, Fraud Analysts and System Administrators.
- Displays transaction status, risk alerts and reports.
- Collects user input such as transactions, approvals or reviews.
- Works for end-users and communicates with the Application Layer.

2. APPLICATION LAYER

- Acts as a controller layer.
- Coordinates transaction processing and risk evaluation.
- Invokes fraud detection services from the Business Logic Layer.
- Manages workflows such as Approve Transaction, Block Transaction and Flag for Manual Review.
- Works as a bridge between Presentation and Business layers.

3. BUSINESS LOGIC LAYER

- Core fraud detection engine resides here.
- Performs risk scoring and pattern analysis.
- Applies fraud detection rules and AI models.
- Classifies transactions into Low, Medium or Critical Risk.
- Makes final decision logic before passing result back to Application Layer.

4. DATA LAYER

- Stores transaction data and fraud logs.
- Maintains external fraud database references.
- Handles database queries securely.
- Provides data to Business Layer for analysis.

B. WHY LAYERED ARCHITECTURE IS BEST

SCALABILITY

- Fraud Detection Engine can scale independently.
- Database scaling can be handled separately.
- Suitable for cloud-based deployment.

MAINTAINABILITY

- Clear separation of concerns.
- Easy debugging and testing.
- New fraud detection techniques can be added without affecting UI.

PERFORMANCE

- Risk scoring optimized in Business Layer.
- Real-time monitoring enabled.
- Efficient transaction approval or blocking.

SECURITY

- Identity verification isolated.
- Secure database access.
- Real-time alerts prevent misuse.

II. APPLICATION COMPONENTS

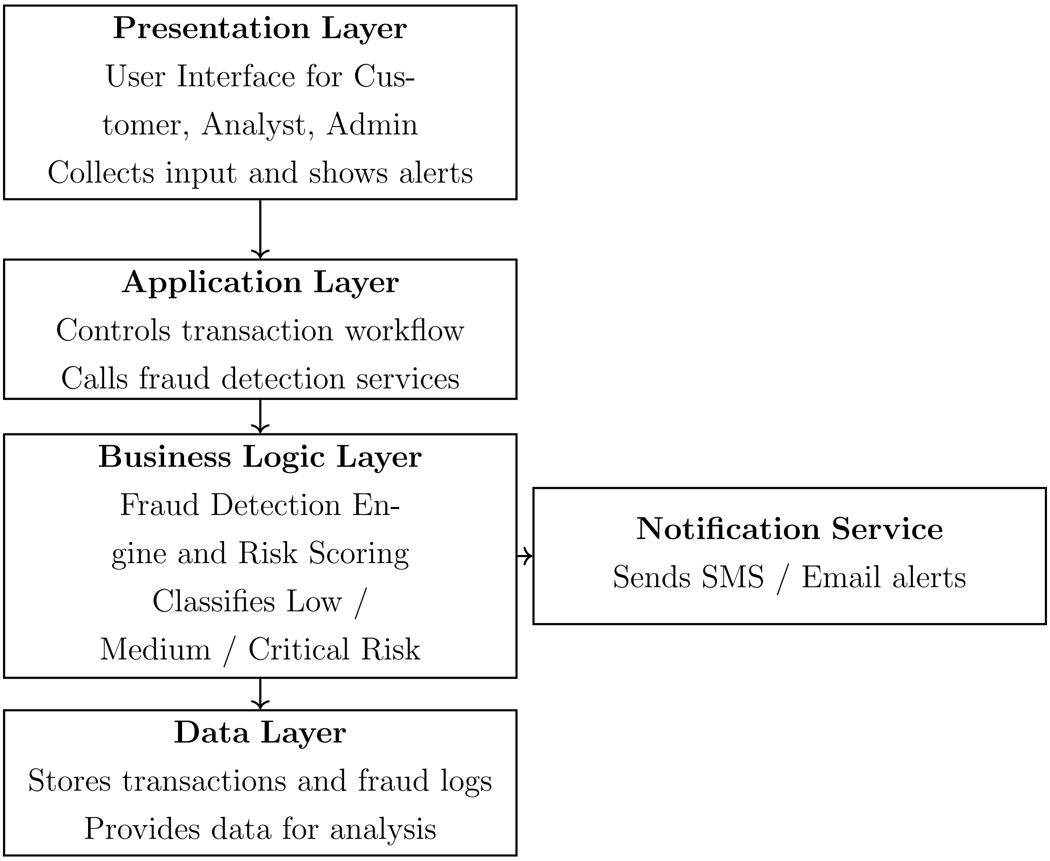
ACTOR COMPONENTS

- Bank Customer – Initiates transactions.
- Fraud Analyst – Reviews flagged transactions.
- System Administrator – Manages risk rules and AI models.
- Notification Service – Sends alerts via SMS or Email.
- External Fraud Database – Provides fraud reference data.

CORE APPLICATION COMPONENTS WITH FUNCTIONS

- **Monitor Transaction and Behavior:** Tracks user activity and transaction patterns.
- **Calculate Risk Score:** Computes risk value based on fraud rules and AI models.
- **Approve Transaction:** Allows transaction if risk is low.
- **Block Transaction:** Stops transaction if risk is critical.
- **Flag for Manual Review:** Sends medium-risk transactions to Fraud Analyst.
- **Send Real-Time Alert:** Notifies users and admins about suspicious activity.
- **Generate Compliance Audit:** Creates audit reports for regulatory purposes.
- **Manage Risk Rules and AI Models:** Updates fraud detection rules and machine learning models.

SYSTEM ARCHITECTURE DIAGRAM


Presentation Layer
User Interface for Customer, Analyst, Admin
Collects input and shows alerts
Application Layer
Controls transaction workflow
Calls fraud detection services
Business Logic Layer
Fraud Detection Engine and Risk Scoring
Classifies Low / Medium / Critical Risk
Notification Service
Sends SMS / Email alerts
Data Layer
Stores transactions and fraud logs
Provides data for analysis