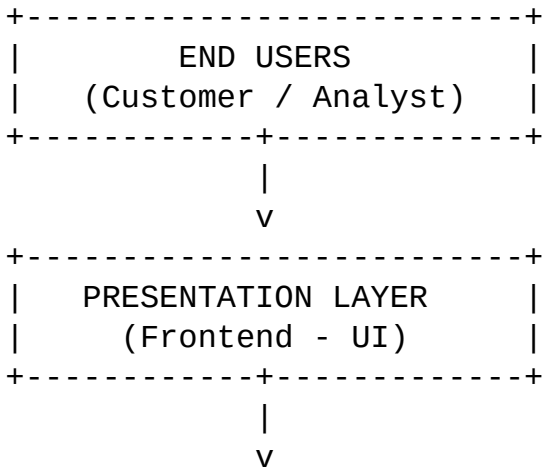
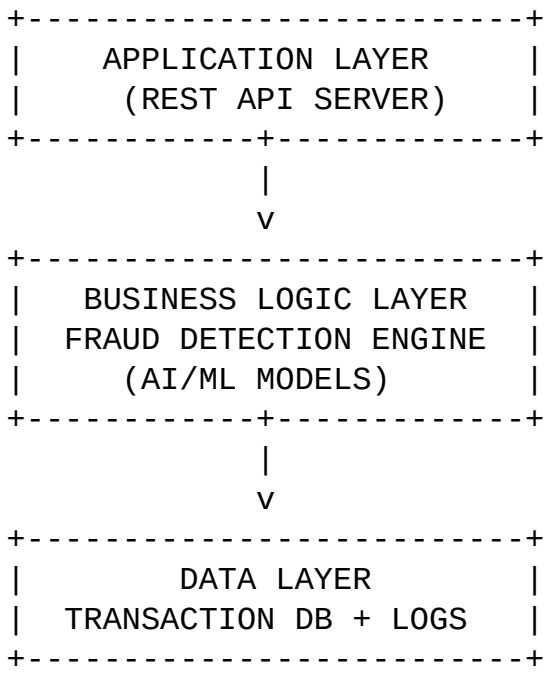
II. HOW END USERS ACCESS THE SYSTEM

A. USER ACCESS FLOW

- User opens the web application using a secure HTTPS connection.
- User logs in using valid credentials (Username and Password).
- System authenticates the user using JWT-based authentication mechanism.
- User performs a financial transaction or reviews a fraud alert notification.
- Frontend sends the request to the Application Layer using REST APIs.
- Application Layer validates input data and forwards request to Business Logic Layer.
- Fraud Detection Engine evaluates the transaction using AI/ML models and risk scoring algorithms.
- Data Layer retrieves transaction history and fraud logs for analysis.
- Fraud decision (Low / Medium / High Risk) is returned to Application Layer.
- Final result is displayed to the user on the dashboard interface.

B. PICTORIAL REPRESENTATION





C. COMPONENT INTERACTION FLOW

- STEP 1: User submits transaction from dashboard.
- STEP 2: Frontend converts action into structured API request.
- STEP 3: Application Layer validates input and checks authentication.
- STEP 4: Business Logic Layer analyzes transaction using AI/ML fraud detection models.
- STEP 5: Data Layer provides transaction history and fraud logs.
- STEP 6: Fraud decision generated (Approve / Block / Manual Review).
- STEP 7: Application Layer sends response back to Frontend.
- STEP 8: Frontend displays final risk status and notification.