PROJECT TITLE: HOSTEL MANAGEMENT SYSTEM

NAME: SARDAR ZAIN

REGISTRAION NO: SP23-BSE-013

TASK:

DOCUMENTATION AND CODING FOR ONLY LOGIN USECASE

Full Address Use Case (LOGIN)

Use Case: User Login

Use Case ID: UC-001
Primary Actor: User
Goal: Securely authenticate users and grant access to role-specific functionalities.
Scope: Authentication System

Description:

This use case describes the process by which a user (student, employee, or admin) logs into the system using valid credentials. Upon successful authentication, the user is redirected to a personalized dashboard with features and permissions tailored to their role.

Trigger:

The user clicks on the “Sign In” or “Login” button from the application or website.

Preconditions:

1. The user must be registered in the system.
2. The user must possess valid login credentials (email/ID and password).
3. The system and its authentication services must be operational.

Postconditions:

Success:

- The user is authenticated and redirected to their role-specific dashboard.
- The login timestamp and last login details are updated in the system logs.

Failure:

- The system displays appropriate error messages without granting access.

Main Flow (Normal Flow):

1. **User Accesses Login Interface:**
    - The user navigates to the login page via a URL or application.
2. **User Inputs Credentials:**
    - The user provides a valid username (email or ID) and password.
3. **System Validates Credentials:**
    - The system verifies if the username exists in the database.
    - If the username exists, the system compares the provided password against the stored hash.
4. **Successful Authentication:**
    - The user is logged in.
    - The system redirects the user to their respective dashboard (Student, Admin, or Staff).
    - The login event is logged with a timestamp.
5. **Access to Functionalities:**
    - The user is granted access to features and data as per their assigned role.

Alternative Flows (Invalid Inputs):

- **A1: Invalid Username:**

  - Condition: The entered username does not exist.
  - System Response: “User does not exist.”
- **A2: Invalid Password:**
  - Condition: The username exists but the password is incorrect.
  - System Response: “Your password is incorrect.”

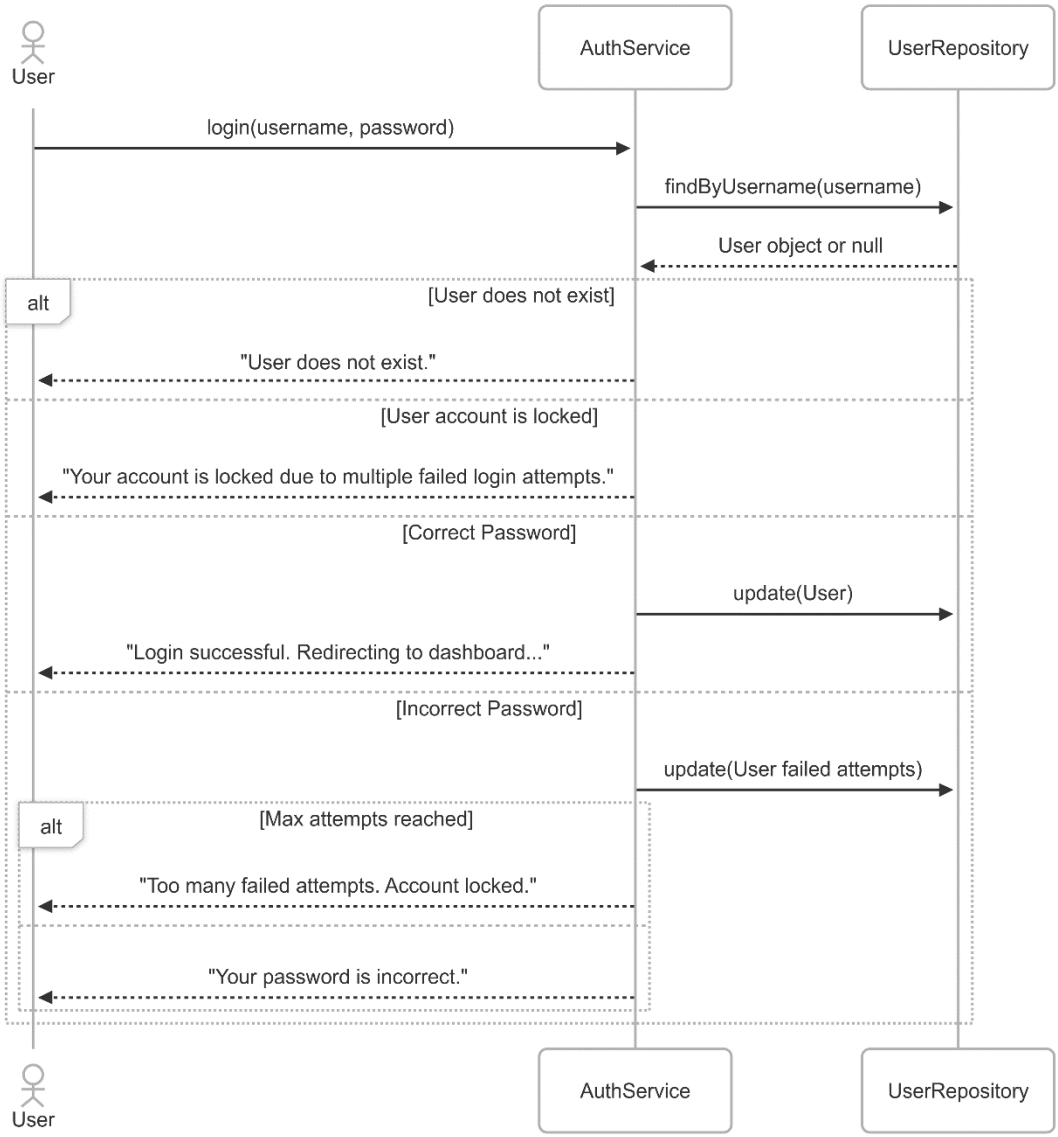
Exceptional Flows:

- **E1: Connection Timeout:**
  - Condition: The network connection times out during login.
  - System Response: The user is notified: “Connection timeout. Please check your internet connection and try again.”

Extension Points:

- **Account Lockout Mechanism (Security Extension):**
  - Trigger: Multiple consecutive failed login attempts (e.g., 5 attempts).
  - Action: The system temporarily locks the account and notifies the user via email.
  - Unlocking may require admin intervention or user action via email verification.

System sequence Diagram:



PROPOSED UI PROTOTYPES:

LOGIN: