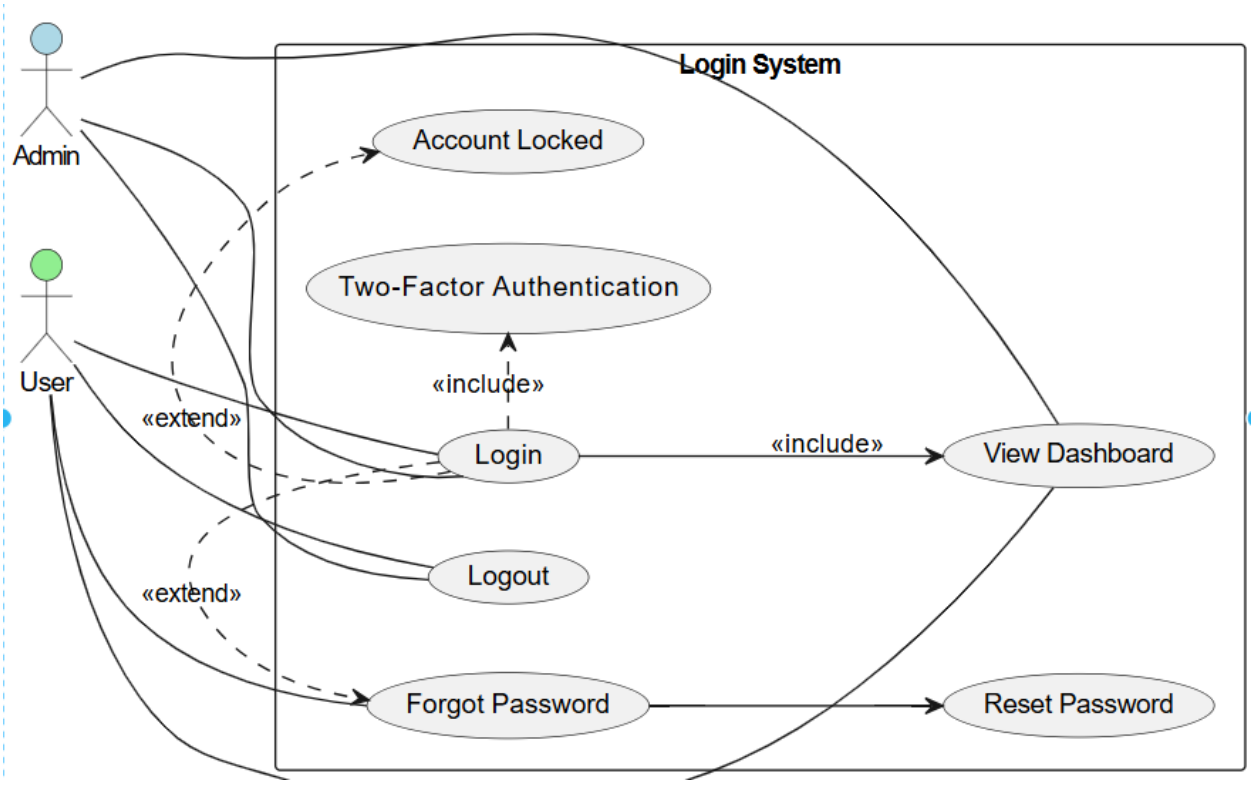
Name:SARINA AMJAD

REG NO:SP22-BSE-095

SYSTEM NAME:TRANSPORT SYSTEM

MODULE: LOGIN

1:USECASE DIAGRAM



FULLY DRESSED USECASE:

Fully Dressed Use Case: Login

A fully dressed use case provides a comprehensive, structured description of all functionalities, scenarios, and requirements for the "Login" process. Here is a detailed use case for a typical login system:

Use Case Name: Login

Primary Actor: User (could be Buyer, Seller, Admin, etc.)

Stakeholders and Interests:

User: Wants secure, quick access to their account.

System: Needs to authenticate users and protect against unauthorized access.

Admin: May monitor login attempts for security.

Preconditions:

The user has previously registered and has valid credentials.

The login page/interface is accessible.

Postconditions:

Success: User is authenticated and redirected to the main/dashboard page.

Failure: User remains on the login page with an appropriate error message.

Main Success Scenario (Basic Flow):

User navigates to the login page.

User enters their username and password.

User clicks the "Login" button.

System validates the credentials:

Checks if the username exists.

Verifies if the password matches the stored password.

If credentials are valid:

System creates a session for the user.

System redirects the user to the main/dashboard page.

User gains access to authorized features.

Extensions (Alternate Flows):

4a. Invalid Username or Password:

System displays an error message: "Invalid username or password."

User can retry login.

2a. Forgot Password:

User clicks "Forgot Password" link.

System prompts for email/username.

System sends password reset instructions to user's email.

4b. Account Locked (e.g., after multiple failed attempts):

System notifies user that the account is locked.

System may prompt user to contact support or unlock via email.

4c. Two-Factor Authentication (if enabled):

System prompts user for a second authentication factor (e.g., OTP).

User enters the OTP.

System verifies OTP before granting access.

4d. Third-Party Authentication:

User selects "Login with Google/Facebook/etc."

System redirects to third-party authentication.

Upon success, system logs in the user.

Special Requirements:

Passwords must be encrypted in storage and during transmission.

Login attempts should be logged for security auditing.

System should prevent brute-force attacks (e.g., by rate-limiting or CAPTCHA).

User sessions must expire after inactivity.

Frequency of Use: Multiple times per day, depending on user.

Business Rules:

Users must have unique usernames.

After a defined number of failed login attempts, the account is temporarily locked.

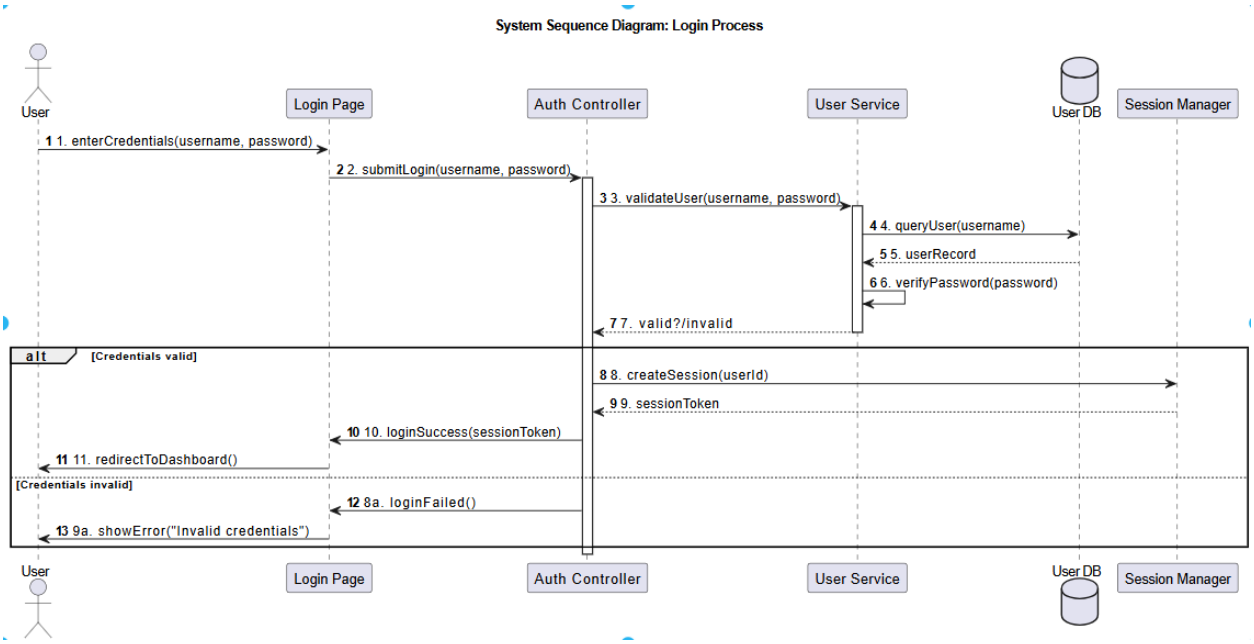
Open Issues:

Should the system support biometric authentication?

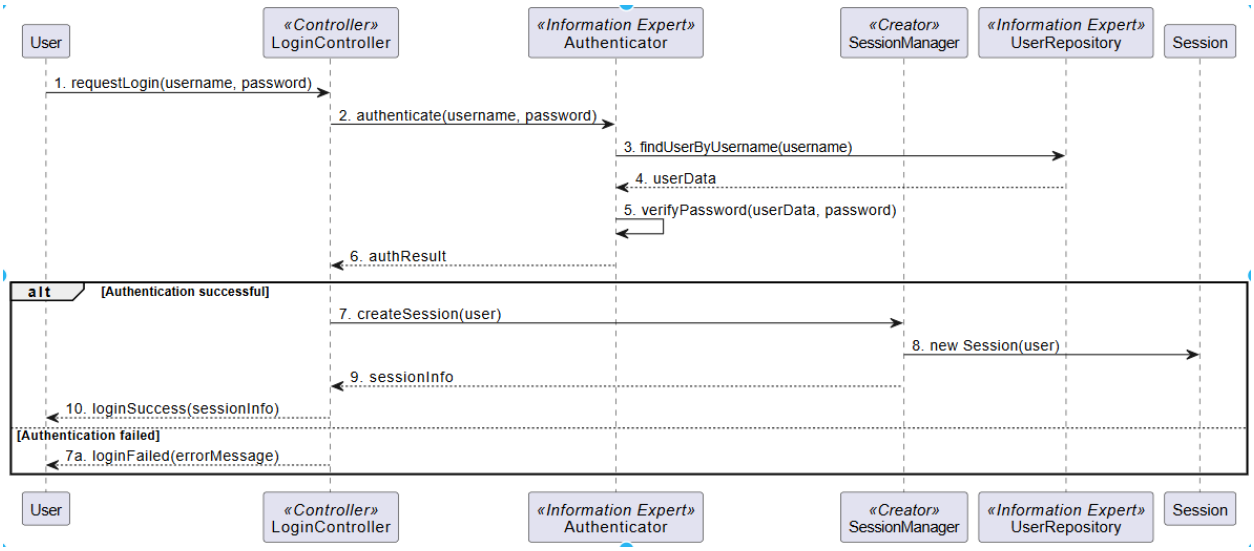
What is the exact lockout policy after failed attempts?

This use case covers all main and alternative flows, security considerations, and system requirements for a robust login process, as typically depicted in UML use case diagrams and related documentation

2.SYSTEM -STATE DIAGRAM:



3.COMMUNICATION DIAGRAM:



4.CLASS DIAGRAM: