PROJECT X: Automated Attendance System

Sophie Bohol
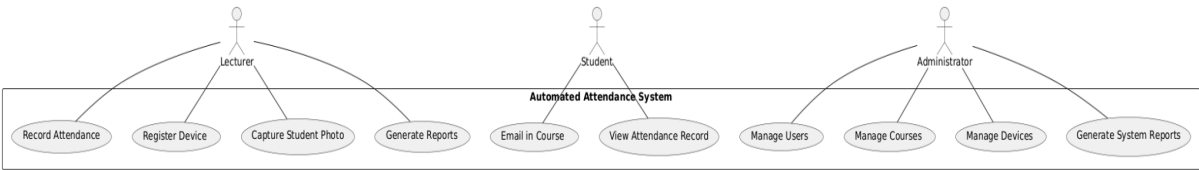
Jhomarie Avenido

Cloe Den Mabanding
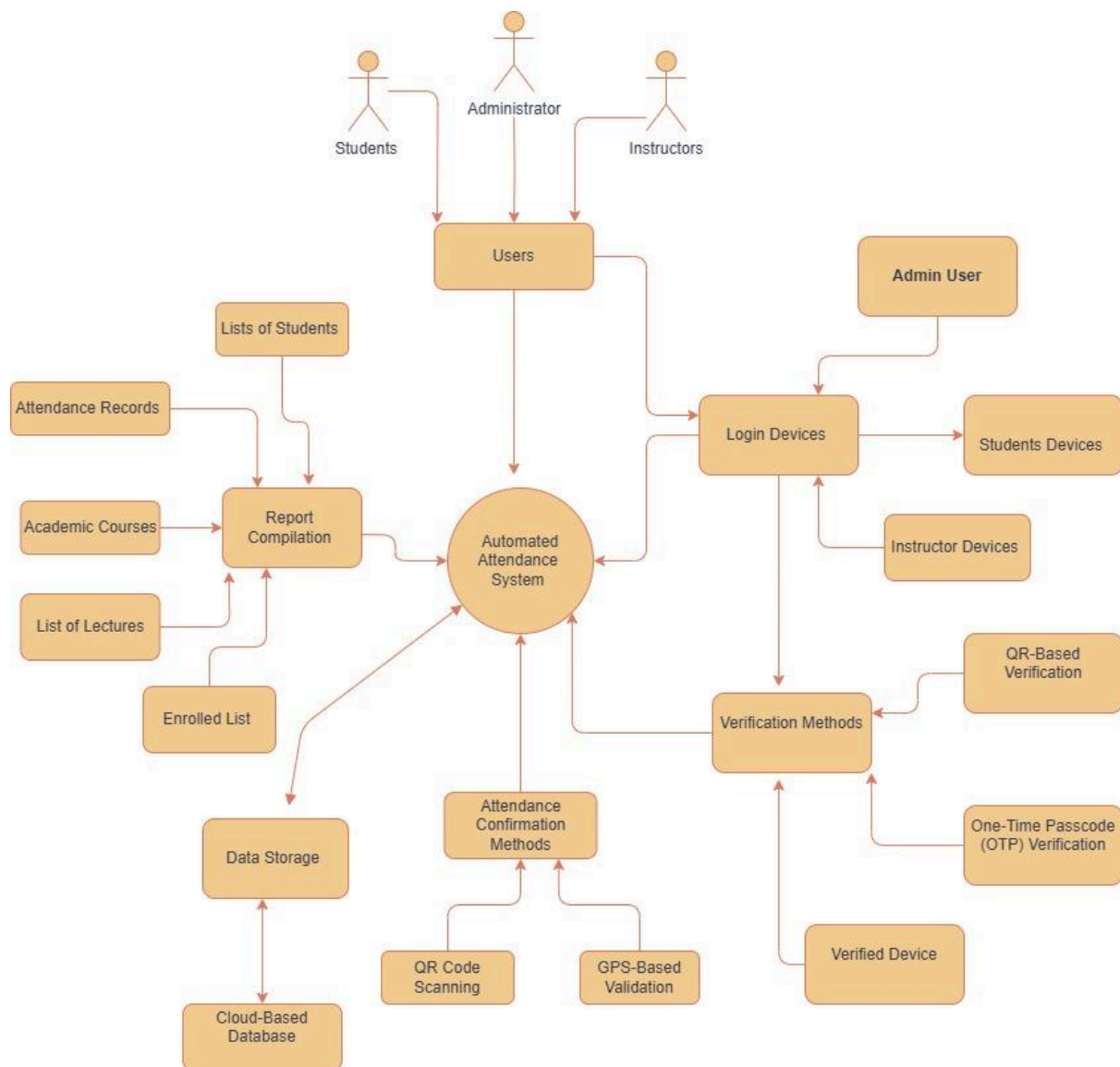
Maureen Portillo

BAMP

Use Case Diagram

Lecturer

Student

Administrator

Automated Attendance System

- Record Attendance
- Register Device
- Capture Student Photo
- Generate Reports
- Email in Course
- View Attendance Record
- Manage Users
- Manage Courses
- Manage Devices
- Generate System Reports

Conceptual Diagram

Frontend (Client Side)

- Mobile App (React Native) Main interface for users
- Camera Module (Captures student photos)

Backend (Server Side)

- REST API (Node.js/ Express) Manages system interactions
- Authentication Module (Manages login/logout)
- Attendance Processing Module (Records student attendance)

- Report Generation Module (Generates reports)

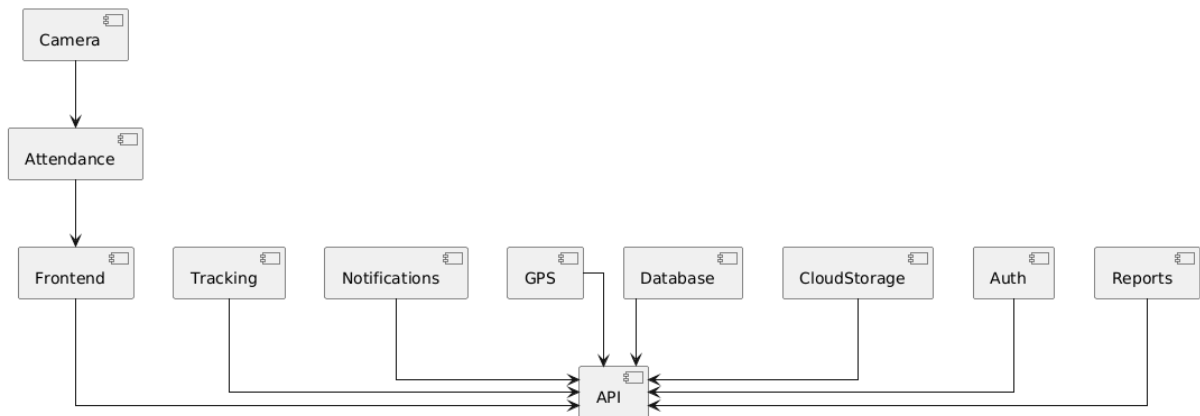- Device Tracking Module (Locates registered devices)

Database (Cloud-Based Mongodb)

- User & Role Management (Students, Lecturers, Admins)

- Course & Enrollment Data (Tracks student enrollment)

- Attendance Records (Stores attendance data)
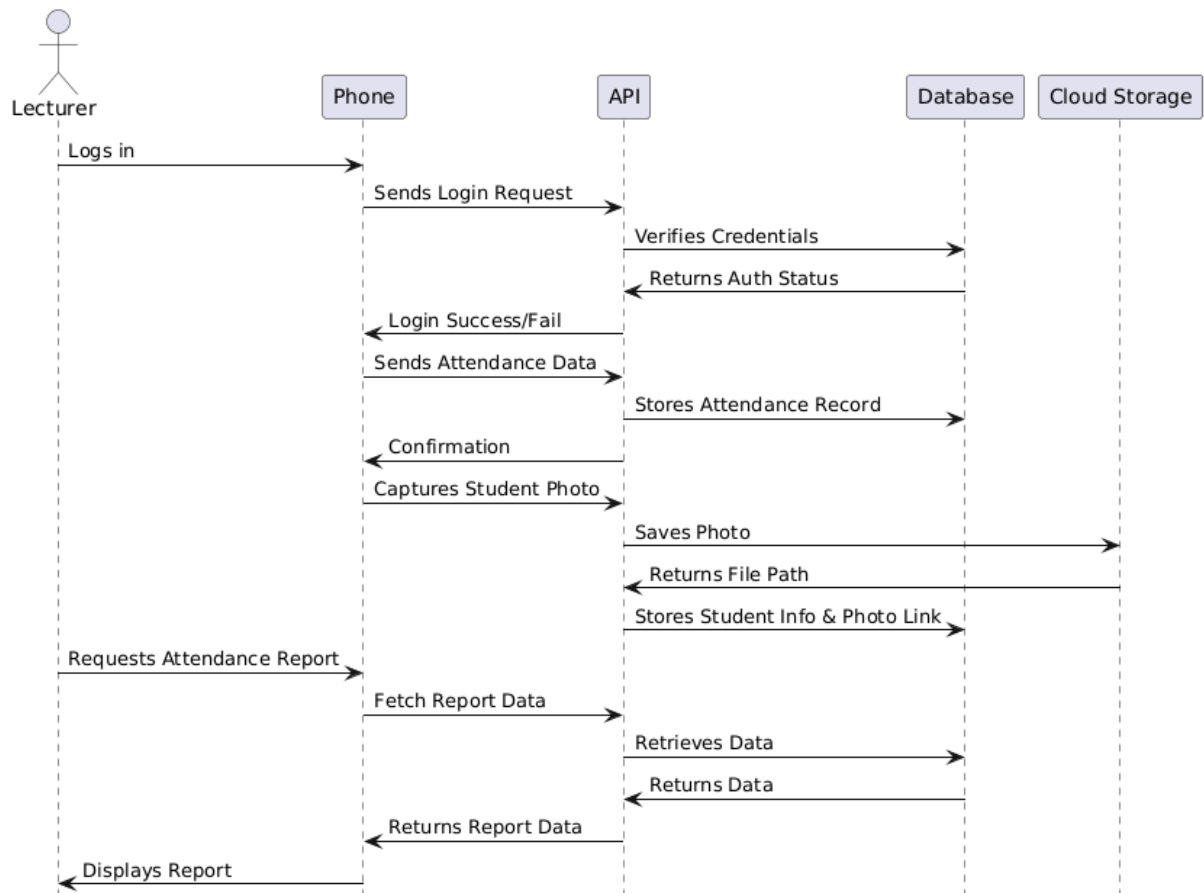
- Photo Storage (Stores student photos)

External Services (Enhancements)

- Cloud Storage (AWS S3, Firebase Storage - Stores images)

- GPS Tracking API (Google Maps API - Locates lecturers)

- Notification Service (Twilio, Firebase Cloud Messaging - Sends reminders)

Component Diagram

Sequence Diagram

Lecturer — **Phone** — **API** — **Database** — **Cloud Storage**

- Lecturer → Phone: Logs in
- Phone → API: Sends Login Request
- API → Database: Verifies Credentials
- Database → API: Returns Auth Status
- API → Phone: Login Success/Fail
- Phone → API: Sends Attendance Data
- API → Database: Stores Attendance Record
- API → Phone: Confirmation
- Phone → API: Captures Student Photo
- API → Cloud Storage: Saves Photo
- Cloud Storage → API: Returns File Path
- API → Database: Stores Student Info & Photo Link
- Lecturer → Phone: Requests Attendance Report
- Phone → API: Fetch Report Data
- API → Database: Retrieves Data
- Database → API: Returns Data
- API → Phone: Returns Report Data
- Phone → Lecturer: Displays Report

Use Case Scenario #1: Automated Attendance System

Scenario: Device Registration

Actors:

- Administrator
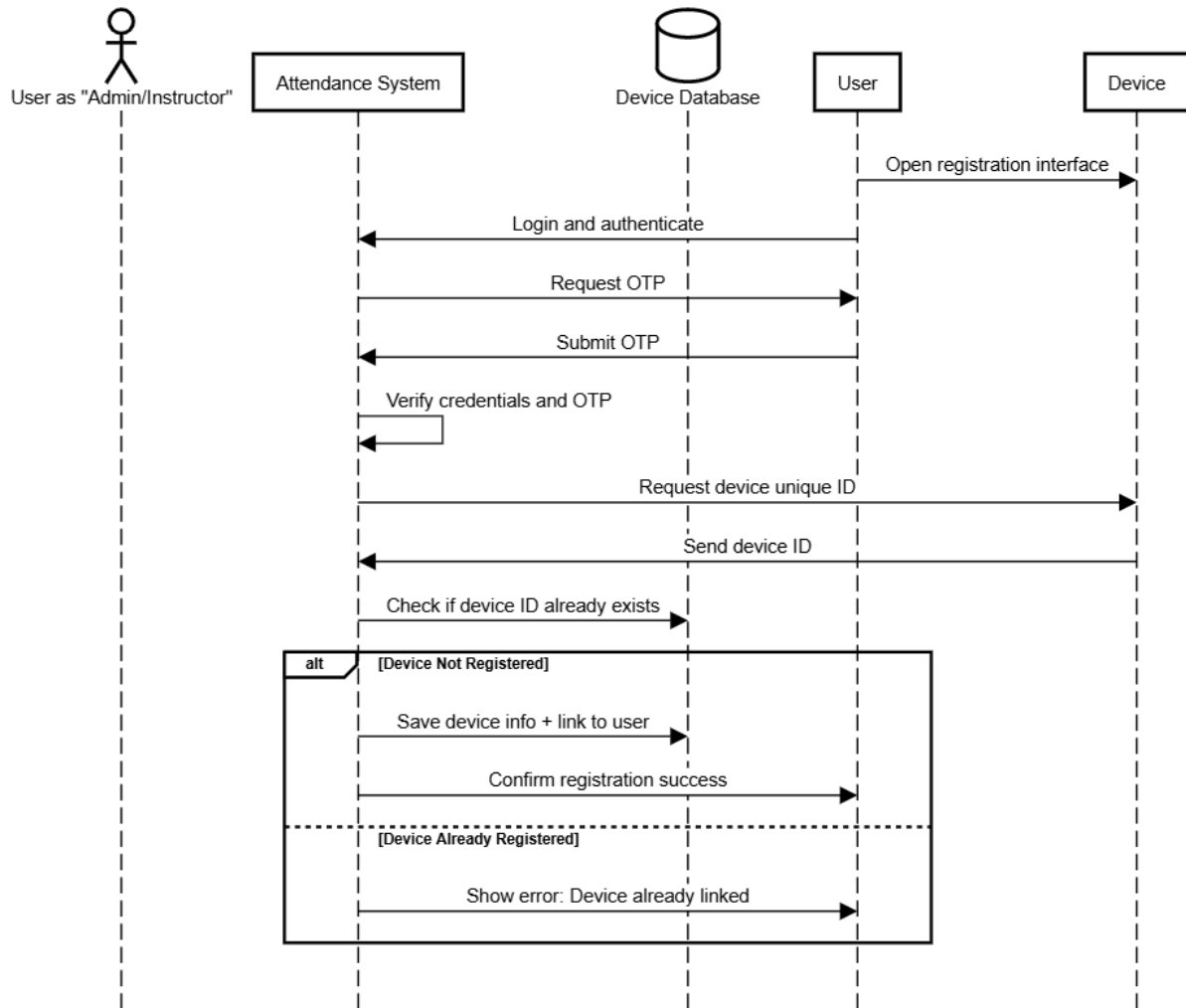- Instructor

Preconditions:

- The user (Administrator or Instructor) must be authenticated.
- The user must have an active system account with the appropriate role.
- The device must have internet access and GPS enabled.

Main Flow:

- The user (Admin or Instructor) logs into the system.
- The user selects the "Register Device" option.
- The system verifies the user's identity through OTP or system credentials.
- The system scans and retrieves the device's unique ID (e.g., IMEI or device fingerprint).
- The user confirms and names the device for easy identification.
- The system validates the device location via GPS to ensure it's within the allowed zone.
- The system stores the device information and links it to the user's profile.
- The system displays a confirmation message that the device has been successfully registered.

Alternative Flow (Device Already Registered):

- If the device is already registered under another account, the system notifies the user and blocks duplication.

Actors/Participants: User as "Admin/Instructor", Attendance System, Device Database, User, Device

- User → Device: Open registration interface
- User → Attendance System: Login and authenticate
- Attendance System → User: Request OTP
- User → Attendance System: Submit OTP
- Attendance System: Verify credentials and OTP
- Attendance System → Device: Request device unique ID
- Device → Attendance System: Send device ID
- Attendance System → Device Database: Check if device ID already exists

alt

[Device Not Registered]
- Attendance System → Device Database: Save device info + link to user
- Attendance System → User: Confirm registration success

[Device Already Registered]
- Attendance System → User: Show error: Device already linked

Use Case Scenario #2: Automated Attendance System

Scenario: Course Enrollment and Management

Actors:

- Administrator
- Instructor
- Student (for view-only access)

Preconditions:

- The user must be authenticated.
- The user must have the appropriate role (Admin or Instructor).
- The course and student data must be available in the system.

Main Flow:

- The Admin or Instructor logs into the system.
- The user navigates to the "Courses" section.
- The user selects one of the following actions:

  - Create a new course (name, code, instructor, schedule)
  - Update course details (schedule, instructor)
  - Delete an existing course

- To enroll students:

  - The user selects the course and clicks "Enroll Student"
  - The user selects the student(s) from a list or inputs their ID
  - The system validates student existence and adds them to the course

- To remove students:

  - The user selects the course and opens the enrolled student list
  - The user removes one or more students
  - The system updates the enrollment records

- The system logs the changes and displays a success confirmation.

Alternative Flow (Invalid Student ID):

● If the entered student ID does not exist in the system:

  ○ The system displays an error message
  ○ The enrollment action is cancelled

Alternative Flow (Duplicate Enrollment):

● If the student is already enrolled in the course:
  ○ The system warns the user and prevents duplicate enrollment
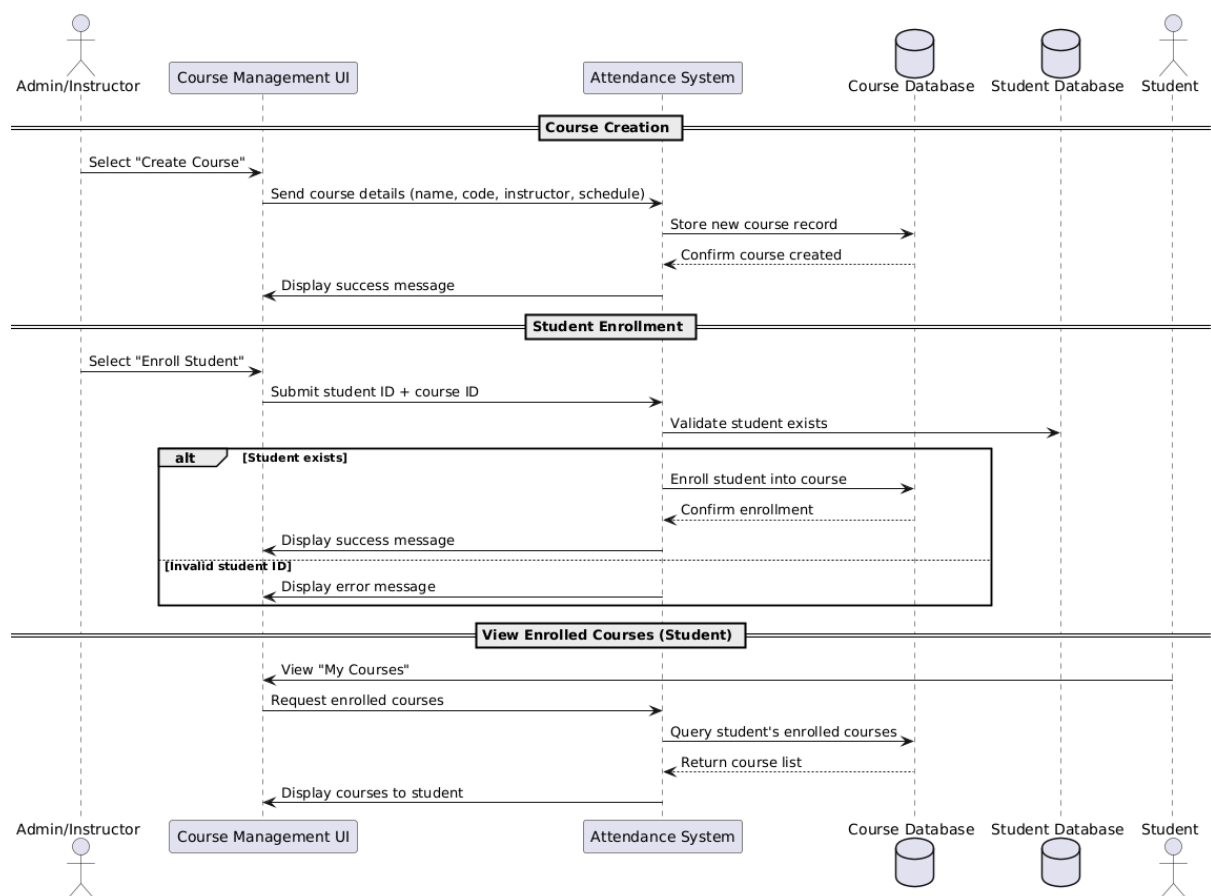
Use Case Scenario #3: Automated Attendance System

Scenario: Record Roll Call Attendance

Actors:

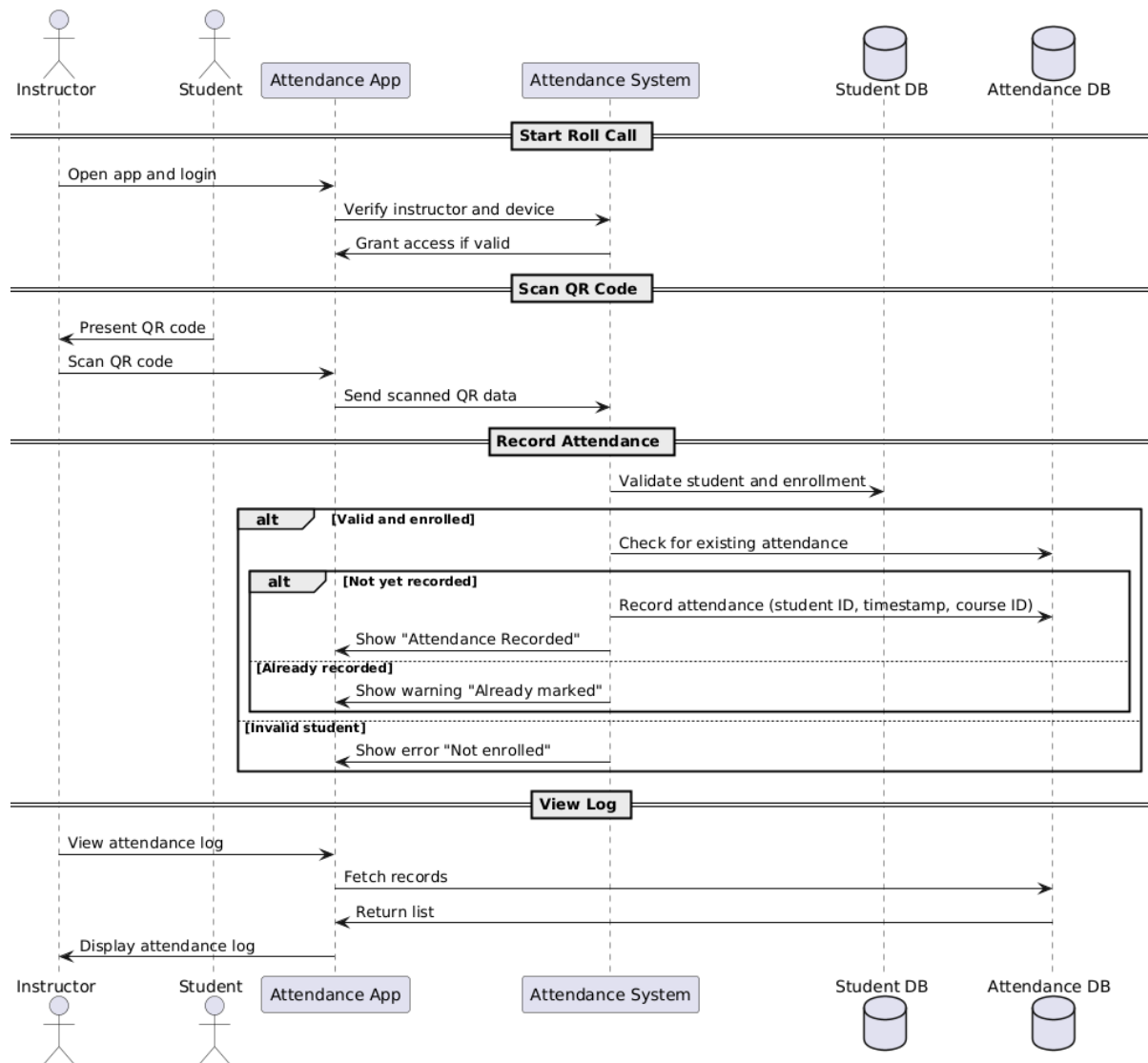- Instructor
- Student

Preconditions:

- The instructor must be logged in on a registered device.
- The class must already be scheduled in the system.
- Students must have valid QR codes and be enrolled in the course.
- Instructor opens the attendance system on a registered device.
- System verifies the device is registered to the instructor.
- The instructor selects the course and scheduled session.
- Each student presents their QR code.
- The instructor scans the QR code using the system interface.
- The system decodes the QR and matches it to a valid enrolled student.
- The system checks if the student's attendance for the session is already recorded.
- If not, the system records the attendance with:

    - Student ID
    - Course ID
    - Timestamp

- The system displays a confirmation (e.g., "Attendance Recorded").
- After all students are scanned, the instructor can view the attendance log.

Alternative Flow (Duplicate Scan):

- If a student's QR code is scanned more than once for the same session:
    - The system shows a warning and does **not** re-record the entry.

Alternative Flow (Unregistered Device):

- If the instructor is using an unregistered device:
    - The system denies access and prompts for device registration.

Sequence Diagram

Participants: Instructor, Student, Attendance App, Attendance System, Student DB, Attendance DB

Start Roll Call

- Instructor → Attendance App: Open app and login
- Attendance App → Attendance System: Verify instructor and device
- Attendance System → Attendance App: Grant access if valid

Scan QR Code

- Attendance App → Student: Present QR code
- Student → Attendance App: Scan QR code
- Attendance App → Attendance System: Send scanned QR data

Record Attendance

- Attendance System → Student DB: Validate student and enrollment

alt [Valid and enrolled]

- Attendance System → Attendance DB: Check for existing attendance

  alt [Not yet recorded]

- Attendance System → Attendance DB: Record attendance (student ID, timestamp, course ID)
- Attendance System → Attendance App: Show "Attendance Recorded"

  [Already recorded]

- Attendance System → Attendance App: Show warning "Already marked"

[Invalid student]

- Attendance System → Attendance App: Show error "Not enrolled"

View Log

- Instructor → Attendance App: View attendance log
- Attendance App → Attendance DB: Fetch records
- Attendance DB → Attendance App: Return list
- Attendance App → Instructor: Display attendance log

Use Case Scenario #4: Automated Attendance System

Scenario: Manage Verification and Authentication

Actors:

- Administrator
- Instructor
- Student

Preconditions:

- The user must have an existing account.
- The device must be internet-connected.
- The user must be using a registered device (if required).

Main Flow:

- User opens the system login page or app.
- User enters their credentials (e.g., username and password).
- The system verifies the credentials.
- If valid, the system sends a One-Time Password (OTP) to the user via email or SMS.
- User enters the OTP.
- The system verifies the OTP.
- If valid, the system checks if the current device is registered.
- If the device is registered, the system logs the user in and creates a session.
- The user is redirected to their dashboard.
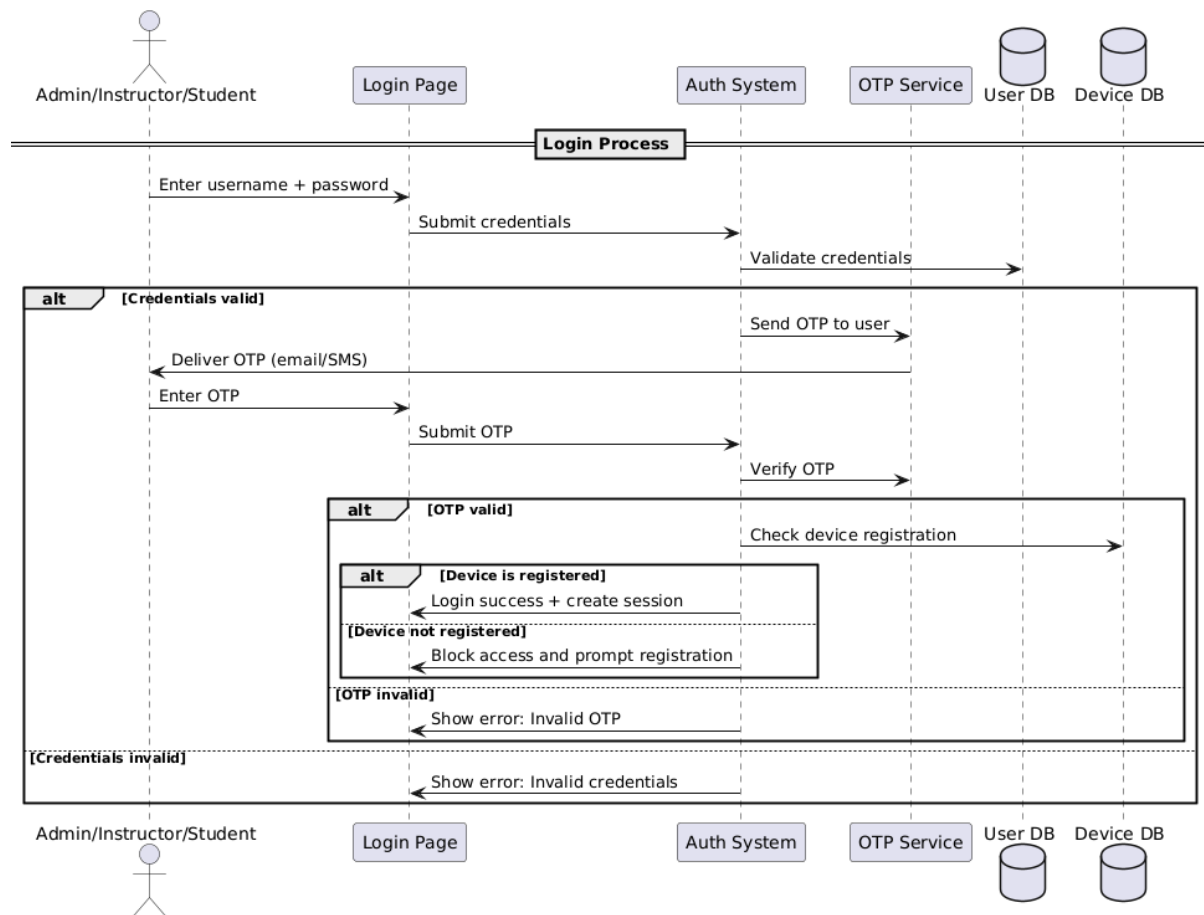
Alternative Flow 1: Incorrect OTP

- If the OTP is incorrect:
  - The system denies access and prompts for re-entry.
  - After several failed attempts, the account may be temporarily locked.

Alternative Flow 2: Unregistered Device

- If the device is not registered:
  - The system blocks access and prompts the user to register the device (if allowed).

Alternative Flow 3: Invalid Credentials

- If the username or password is incorrect:
  - The system shows an error message and denies access.

Admin/Instructor/Student   Login Page   Auth System   OTP Service   User DB   Device DB

Login Process

Enter username + password

Submit credentials

Validate credentials

alt   [Credentials valid]

Send OTP to user

Deliver OTP (email/SMS)

Enter OTP

Submit OTP

Verify OTP

alt   [OTP valid]

Check device registration

alt   [Device is registered]

Login success + create session

[Device not registered]

Block access and prompt registration

[OTP invalid]

Show error: Invalid OTP

[Credentials invalid]

Show error: Invalid credentials

Admin/Instructor/Student   Login Page   Auth System   OTP Service   User DB   Device DB

Use Case Scenario #5: Automated Attendance System

Scenario: Student Interface

Actor:

- Student

Preconditions:

- The student must be registered in the system.
- The student must log in via a valid device using credentials and OTP.
- The student must be enrolled in at least one course.

Main Flow:

- Student launches the system app or web portal.
- Student logs in using credentials and OTP verification.
- System verifies identity and allows access.
- Student navigates the dashboard and can perform the following actions:

    - View their current **enrolled courses**.
    - View their **attendance records** by course.
    - View the **class schedule**.
    - Update their **profile picture** (if permitted).

- Student can log out when finished.

Alternative Flow 1: Not Enrolled in Any Course

- If the student is not enrolled in any course:
    - The system displays an empty course list with a message.

Alternative Flow 2: Failed Login

- If credentials or OTP are invalid:
    - Access is denied, and the user is prompted to retry.