CEBU INSTITUTE OF TECHNOLOGY
UNIVERSITY

IT342-G1
SYSTEMS INTEGRATION AND ARCHITECTURE 1

FUNCTIONAL REQUIREMENTS SPECIFICATION (FRS)

Project Title: User Registration and Authentication System

Prepared By: Salonga, Andre D.

Date of Submission: February 15, 2026

Version: 1.3

Table of Contents

1. Introduction

1.1. Purpose

The purpose of this document is to define the functional and non-functional requirements of a User Registration and Authentication System. This document serves as a reference for documenting how users interact with the system through registration, login, accessing protected pages, and logout.

The intended audience of this document includes students, instructors, and developers who will use this specification as a basis for system design and implementation during the succeeding development phase.

1.2. Scope

The system provides basic user authentication functionalities, including account registration, login, access to a protected user profile or dashboard, and logout. It ensures that only authenticated users can access protected pages of the system.

This document focuses only on the functional behavior and system flow of the authentication process. Advanced features such as role management, password recovery, email verification, and account management are outside the scope of this system.

1.3. Definitions, Acronyms, and Abbreviations

Authorization

The process of determining whether an authenticated user is allowed to access protected pages or system resources.

JWT (JSON Web Token)

A secure token generated after successful authentication that is used to authorize access to protected system features.

API

Stands for Application Programming Interface; it enables communication between the frontend user interface and the backend system services.

User Interface (UI)

The part of the system where users interact with the application, such as registration and login forms.

Password Hashing

A security process that converts a user’s password into an unreadable format before storing it in the database.

Authentication

The process of verifying a user’s identity using valid credentials such as email and password.

Protected Page

A system page or resource that can only be accessed by authenticated users with a valid authentication token.

Authentication Token

A generated credential, such as a JWT, used to maintain user authentication and authorize access to protected system resources.

2. Overall Description

2.1. System Perspective

The system is a web-based authentication module designed to be part of a larger application. It follows a client–server architecture where the frontend (React UI) communicates with a backend service (Spring Boot API) through RESTful endpoints.

The authentication system acts as a foundational component that controls access to protected features within the application.

2.2. User Classes and Characteristics

1. **Guest User**
    - Has no account or is not logged in.
    - Can register a new account.
    - Can log in using valid credentials.
2. **Authenticated User**
    - Has a registered account.
    - Can log in and access protected pages such as the profile or dashboard.
    - Can log out of the system.

2.3. Operating Environment

1. **Hardware**

- Desktop or laptop computer

2. **Software**

   - Web browser (Google Chrome, Mozilla Firefox, Microsoft Edge)
   - Frontend: React
   - Backend: Spring Boot
   - Database: Relational Database Management System

3. **Tools**

   - draw.io (diagrams.net) for system diagrams
   - Microsoft Word or PDF reader for documentation

2.4. Assumptions and Dependencies

- Users have access to a stable internet connection.
- The backend API is available and operational.
- JWT is used for managing authentication tokens.
- Passwords are securely hashed before being stored.
- The system depends on external libraries and frameworks such as React and Spring Boot.

3. System Features and Functional Requirements

3.1. Feature 1: User Registration

Description: This feature allows a guest user to create a new account by providing the required registration details. The system securely stores user information and credentials.

Functional Requirements:

1. The system shall allow users to register using valid registration details.
2. The system shall encrypt or hash user passwords before storing them.
3. The system shall confirm successful registration to the user.

3.2. Feature 2: User Authentication and Session Management

Description: This feature enables registered users to log in, access protected pages, and log out of the system. Authentication is handled using secure tokens.

Functional Requirements:

1. The system shall authenticate users using valid email and password credentials.
2. The system shall generate and return an authentication token upon successful login.

3. The system shall restrict access to protected pages for unauthenticated users.

3.3. Feature 3: User Logout and Access Control

Description: This feature allows authenticated users to securely log out of the system and ensures that protected pages cannot be accessed once the user is logged out.

Functional Requirements:

1. The system shall allow authenticated users to log out of the application.
2. The system shall invalidate or remove the authentication token upon logout.
3. The system shall prevent unauthenticated users from accessing protected pages.

4. Non-Functional Requirements

Performance

The system shall respond to authentication requests within an acceptable time frame.

Security

User passwords shall be securely hashed, and authentication tokens shall be validated before granting access.

Usability

The system shall provide clear feedback for successful and failed actions.

Reliability

The system shall consistently handle login, registration, and logout requests without data loss.

Scalability

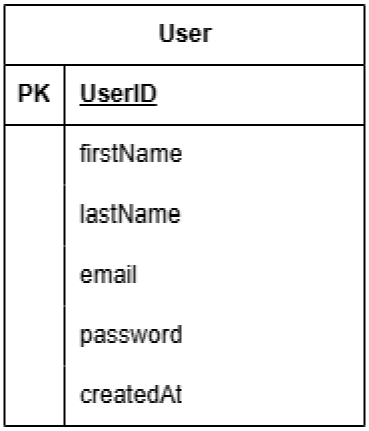
The system shall support multiple concurrent users without performance degradation.

Maintainability

The system shall be designed using a modular architecture to allow easier updates and maintenance.

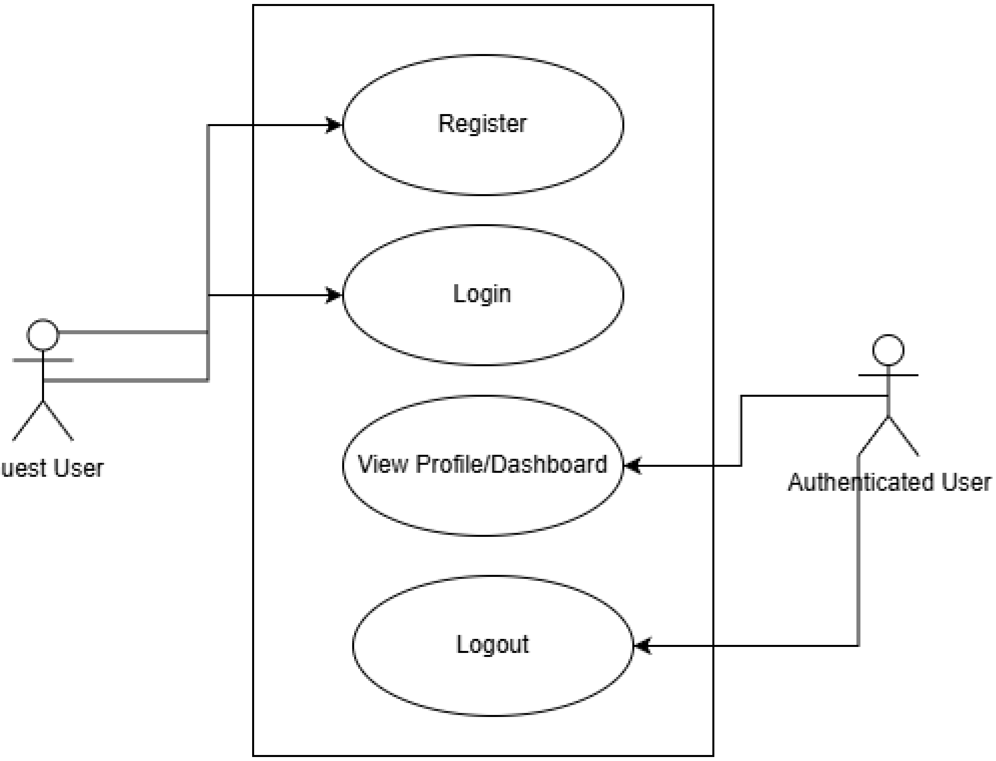
5. System Models (Diagrams)

5.1. ERD

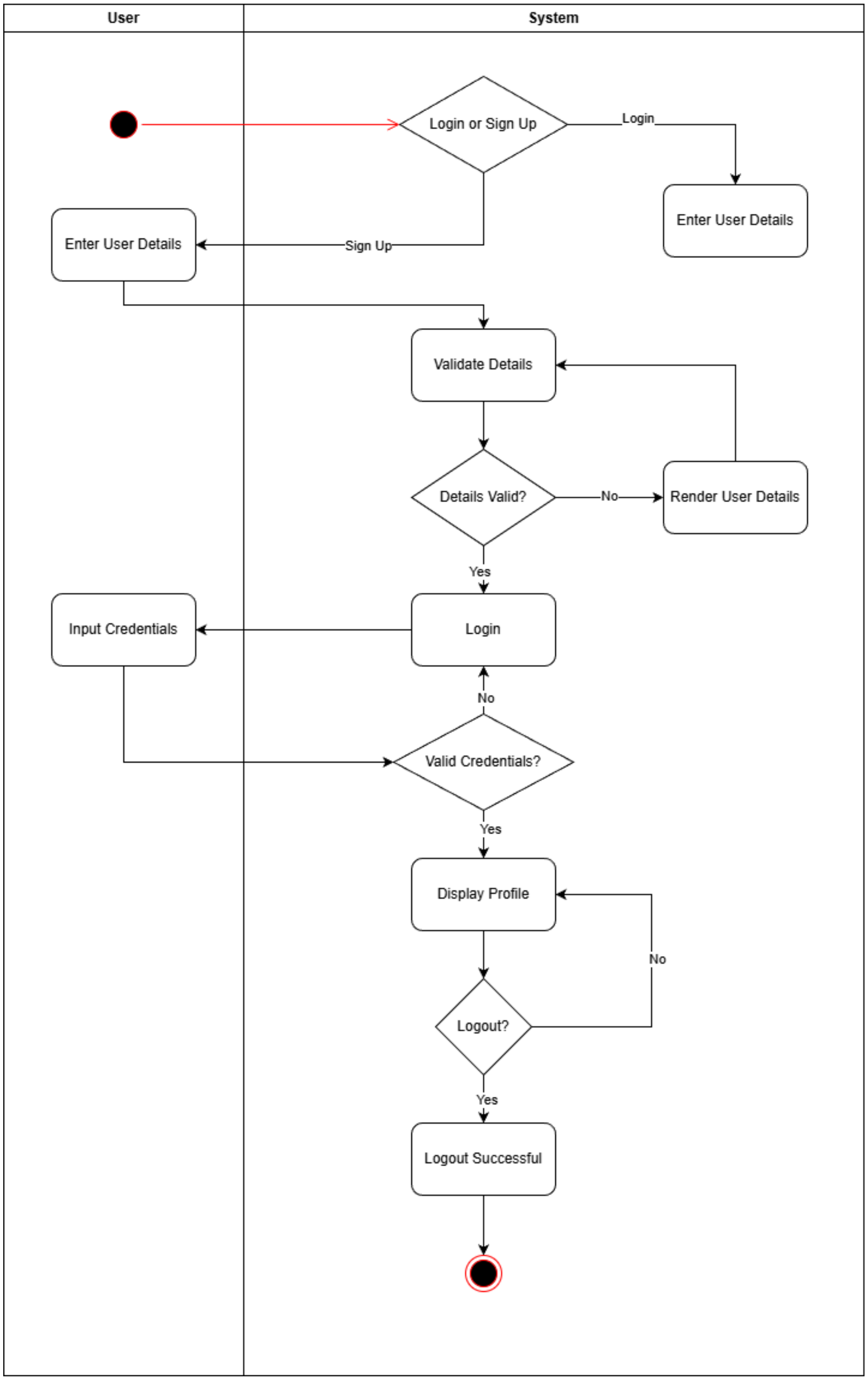


User	
PK	UserID
	firstName
	lastName
	email
	password
	createdAt

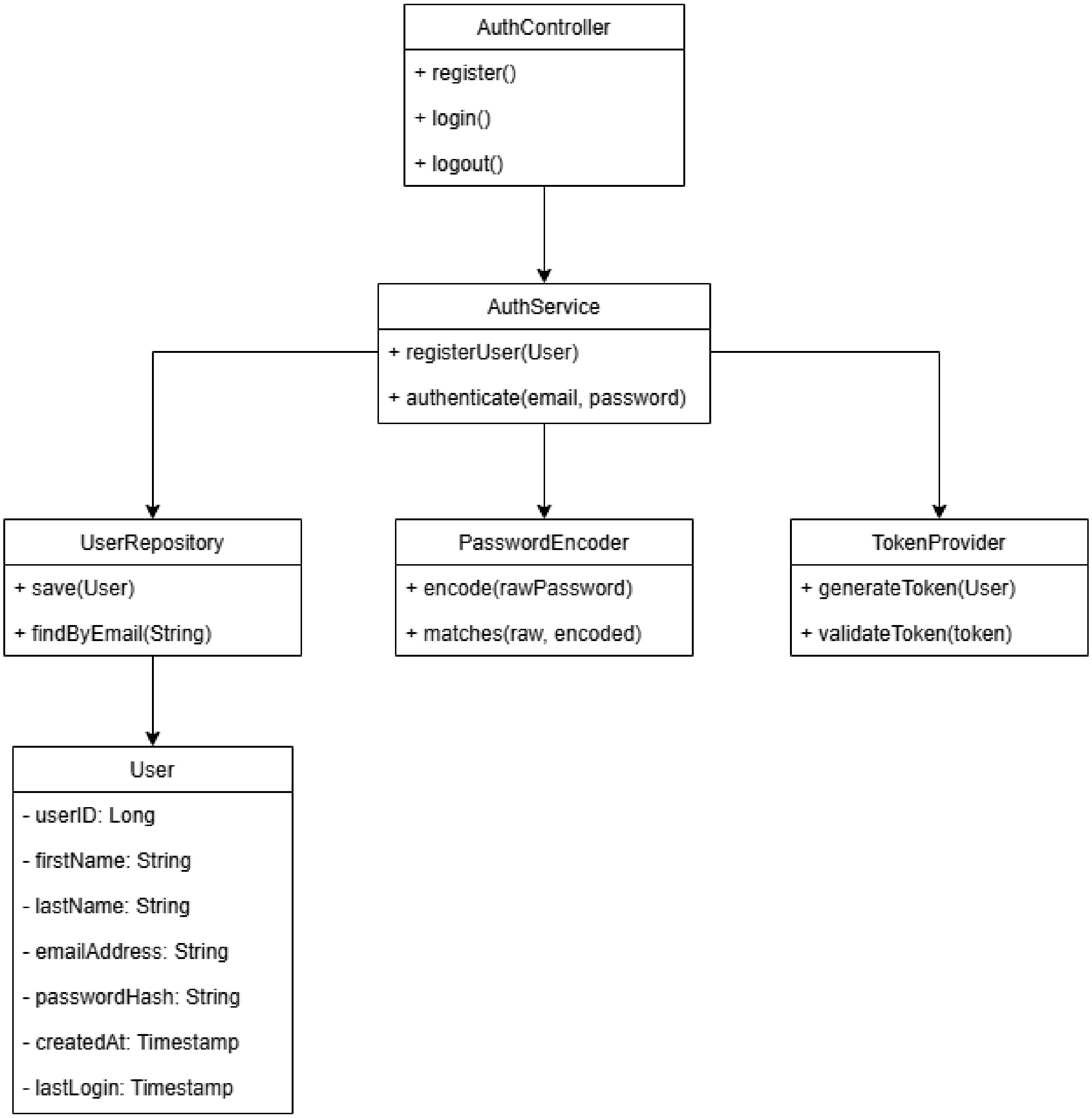
5.2. Use Case Diagram



5.3. Activity Diagram

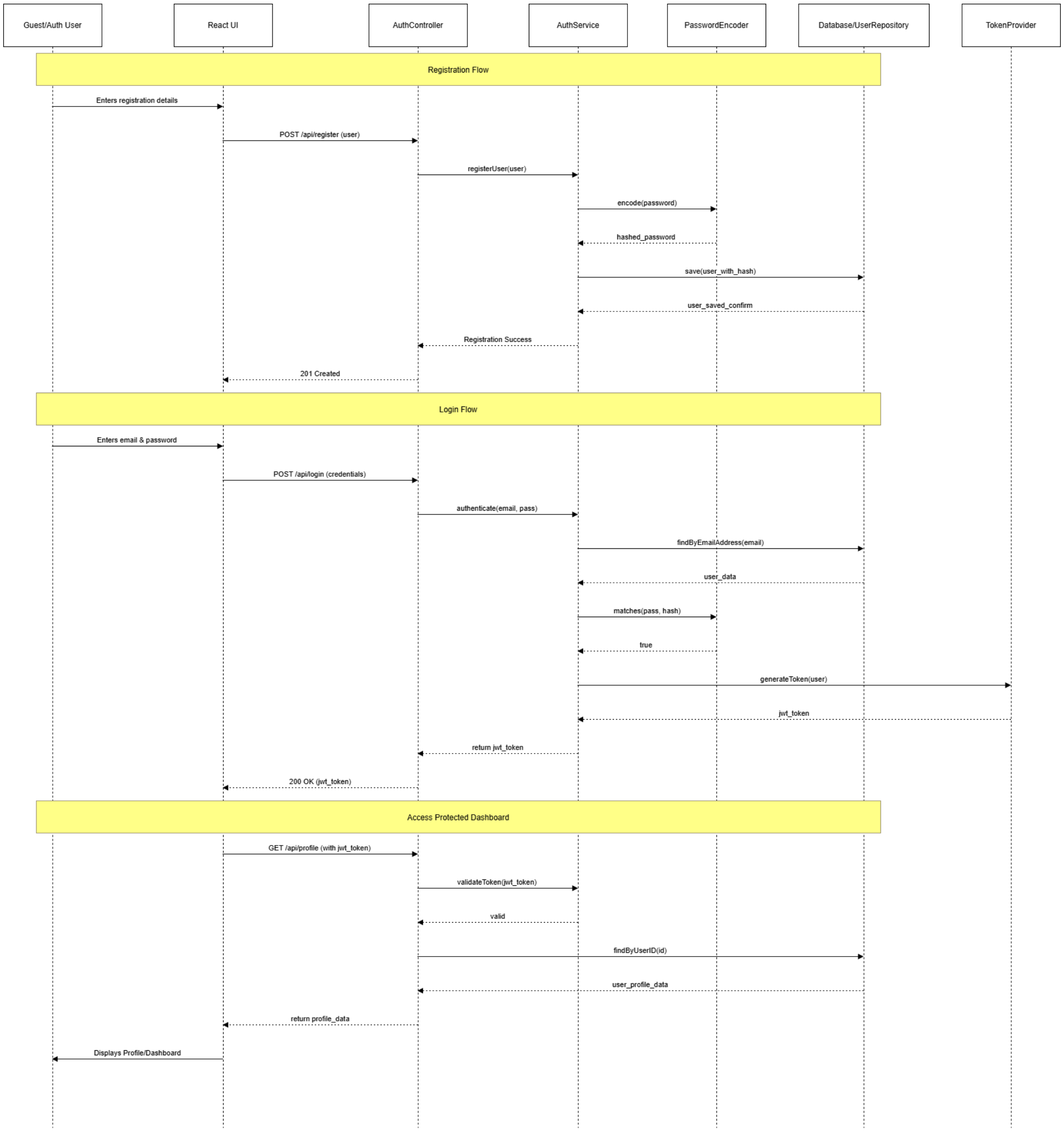


5.4. Class Diagram



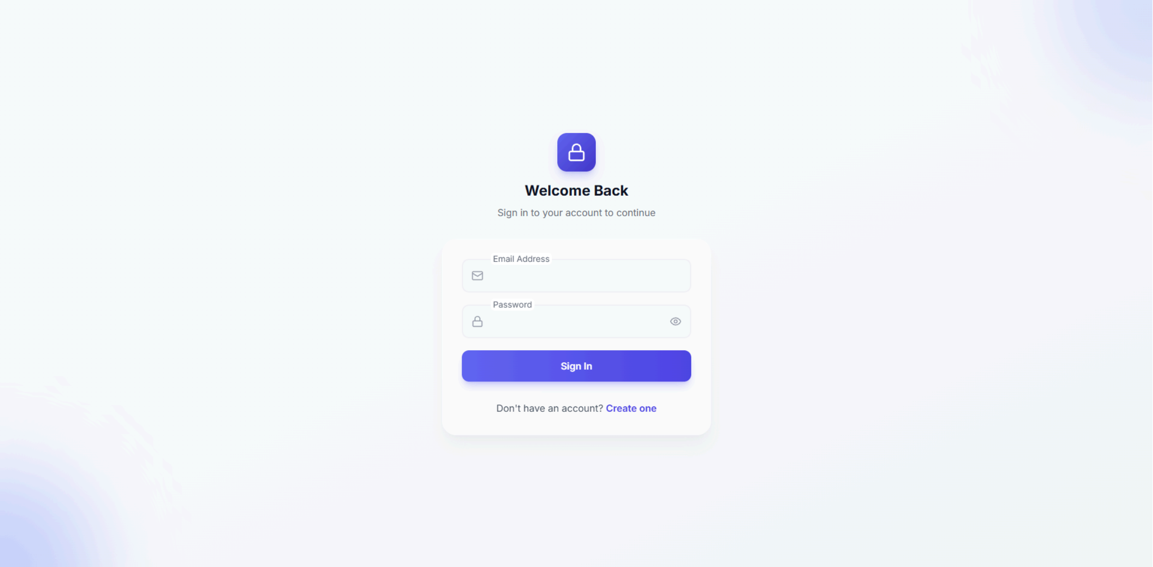
5.5. Sequence Diagram

For a clearer version, you may access the sequence diagram through the link below: *https://drive.google.com/file/d/1ViNng5BeHDfeSRlxyISQMe_HXqpE8nI7/view?usp=sharing*



6. Appendices

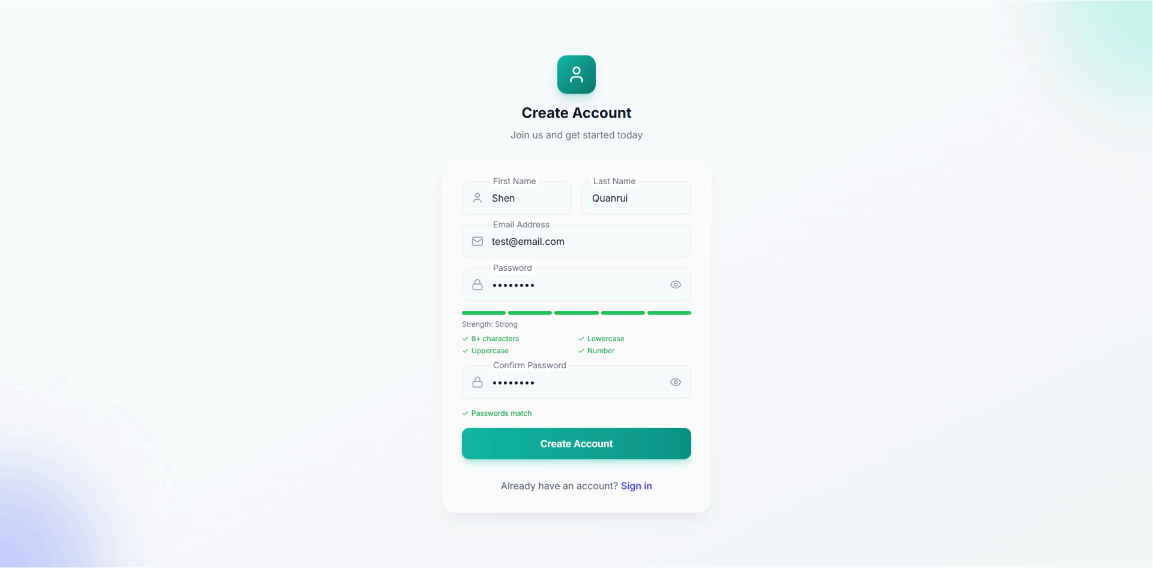
Appendix A: Web Screenshots



Welcome Back

Sign in to your account to continue

Don't have an account? Create one



Create Account

Join us and get started today

First Name: Shen

Last Name: Quanrui

Email Address: test@email.com

Password: ••••••••

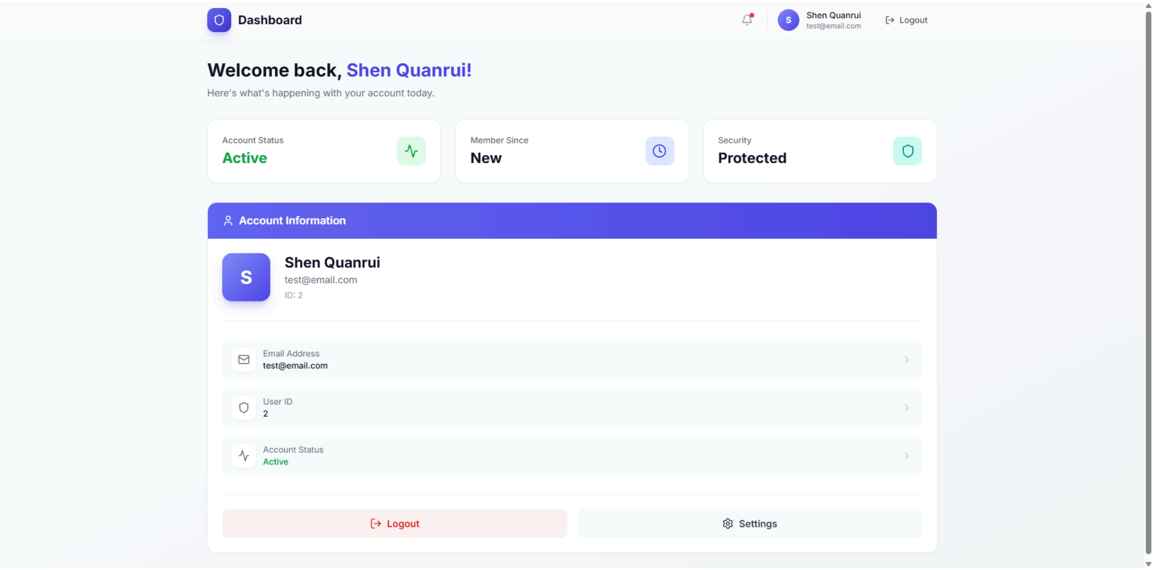
Strength: Strong

✓ 8+ characters
✓ Lowercase
✓ Uppercase
✓ Number

Confirm Password: ••••••••

✓ Passwords match

Already have an account? Sign in



Welcome back, Shen Quanrui!

Here's what's happening with your account today.

Account Status
Active

Member Since
New

Security
Protected

Account Information

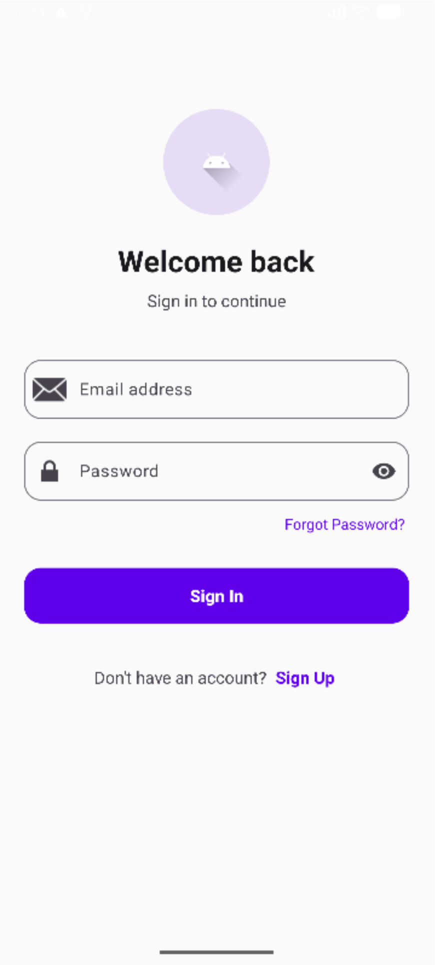
Shen Quanrui
test@email.com
ID: 2

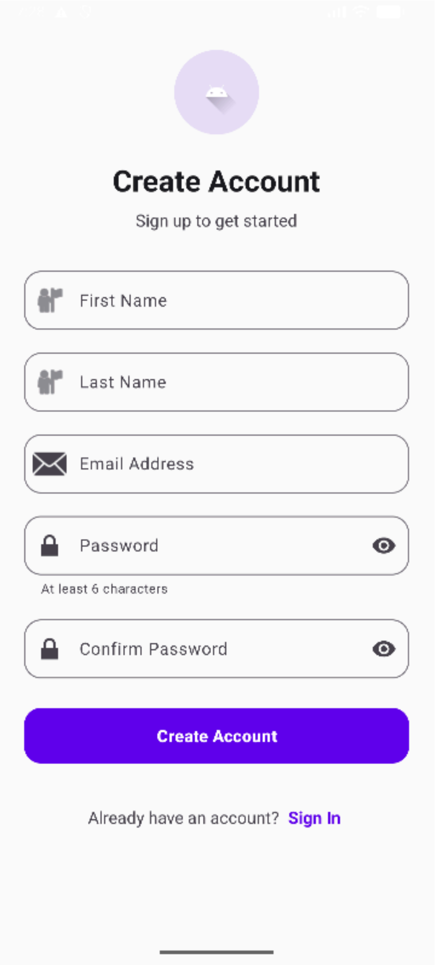
Email Address
test@email.com

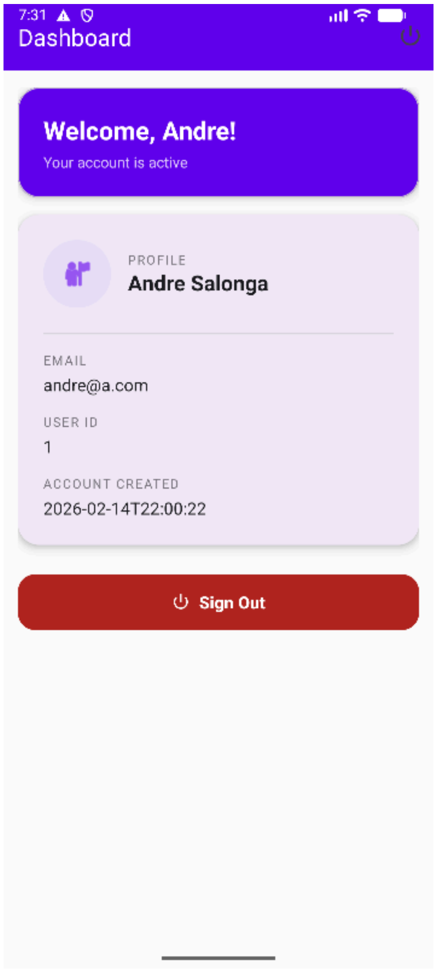
User ID
2

Account Status
Active

Appendix B. Mobile Screenshots







Dashboard

Welcome, Andre!

Your account is active

PROFILE
Andre Salonga

EMAIL
andre@a.com

USER ID
1

ACCOUNT CREATED
2026-02-14T22:00:22