



**CEBU INSTITUTE OF TECHNOLOGY**  
**UNIVERSITY**

# IT342-Section SYSTEMS INTEGRATION AND ARCHITECTURE 1

---

## **FUNCTIONAL REQUIREMENTS SPECIFICATION (FRS)**

---

Project Title: Mini App – User Registration & Authentication

Prepared By: Aytona, Rod Ivanne G.

Date of Submission: 2/5/2026

Version: 1.0

# Table of Contents

1.	Introduction .....	3
1.1.	Purpose.....	3
1.2.	Scope.....	3
1.3.	Definitions, Acronyms, and Abbreviations .....	3
2.	Overall Description .....	3
2.1.	System Perspective.....	3
2.2.	User Classes and Characteristics.....	3
2.3.	Operating Environment.....	3
2.4.	Assumptions and Dependencies .....	4
3.	System Features and Functional Requirements .....	4
3.1.	Feature 1:.....	4
3.2.	Feature 2:.....	4
4.	Non-Functional Requirements .....	5
5.	System Models (Diagrams) .....	6
5.1.	ERD.....	6
5.2.	Use Case Diagram.....	6
5.3.	Activity Diagram .....	7
5.4.	Class Diagram.....	8
5.5.	Sequence Diagram .....	9
6.	Appendices .....	9

## 1. Introduction

### 1.1. Purpose

The purpose of this system is to provide a secure and user-friendly authentication mechanism for users. The system will allow users to register, log in, access their profile/dashboard, and log out.

### 1.2. Scope

The system will:

- Enable users to register an account.
- Enable users to sign in with their credentials.
- Prevent unauthenticated users from accessing restricted pages.
- Allow users to log out securely.
- Allow authenticated users to view their dashboard/profile

### 1.3. Definitions, Acronyms, and Abbreviations

User	A person who registers and logs in to the system.
Registration	The process of creating a new user account
Login	The process of verifying a registered user's credentials.
Logout	Terminating a user's session.
Dashboard	Protected page visible only to authenticated users.

## 2. Overall Description

### 2.1. System Perspective

The Authentication System operates as a standalone module responsible for validating users, maintaining session states, and controlling access to protected resources.

### 2.2. User Classes and Characteristics

Guest User	Can register and attempt to login. Cannot access protected pages.
Authenticated User	Can access protected pages, view profile/dashboard, and log out.

### 2.3. Operating Environment

- Web browser or mobile device for user access.
- Backend server handling authentication logic.
- Database to store user credentials securely.

#### **2.4. Assumptions and Dependencies**

- Users will provide valid and accurate credentials.
- Password will be encrypted and securely stored.
- Database server is available and operational.
- Frontend and backend are properly connected.

### **3. System Features and Functional Requirements**

Describe each major feature of the system and its functional requirements.

#### **3.1. Feature 1: User Registration**

Description: This feature allows a guest user to create a new account. The user provides basic information, and the system saves it securely.

Functional Requirements:

- The system allows a guest user to register an account.
- The system lets the user enter an email and password.
- The system checks if the email is already registered.
- The system encrypts the password before saving it.
- The system stores the user's information in the database.
- The system shows a message to let the user know if registration is successful or failed.

#### **3.2. Feature 2: User Login**

Description: This feature allows a registered user to log in using valid credentials. The system verifies the credentials, manages user sessions, and controls access to protected pages.

Functional Requirements:

- The system allows a registered user to log in using email and password.
- The system verifies the entered credentials against stored user data.
- The system denies access if the credentials are invalid.
- The system creates a session or authentication token upon successful login.
- The system allows authenticated users to access protected pages such as the dashboard.
- The system prevents unauthenticated users from accessing protected resources.

#### **3.3. Feature 3: User Logout**

Description: This feature allows an authenticated user to securely log out, ending their session and preventing further access to protected pages.

#### Functional Requirements:

- The system allows authenticated users to log out from the system.
- The system invalidates the user's session or authentication token upon logout.
- The system redirects the user to the login page after logging out.
- The system prevents access to protected pages after logout.

### 4. Non-Functional Requirements

#### Security:

- The system encrypts user passwords.
- The system allows only logged-in users to access protected pages.

#### Performance:

- The system responds to user actions quickly.

#### Usability:

- The system displays clear error messages to the user.
- The system is easy for the user to use and understand.

#### Reliability:

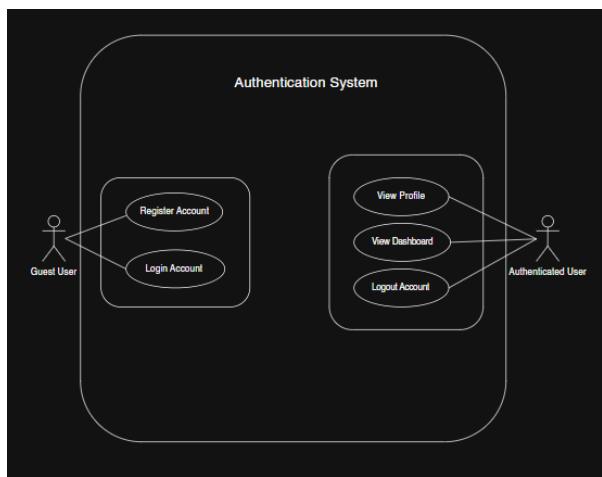
- The system handles login and logout properly.
- The system remains stable during normal use.

## 5. System Models (Diagrams)

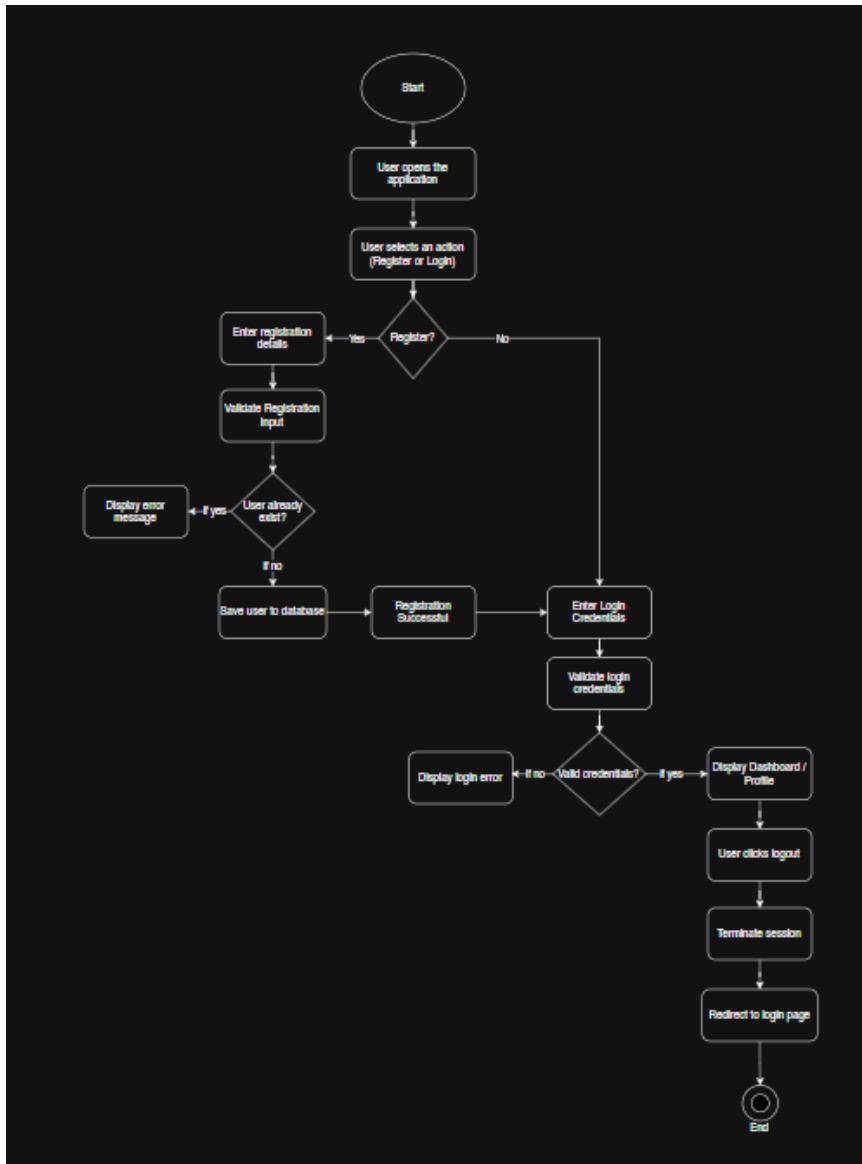
### 5.1. ERD

Users	
PK	userId (int)
	username (varchar)
	email (varchar)
	password (varchar)

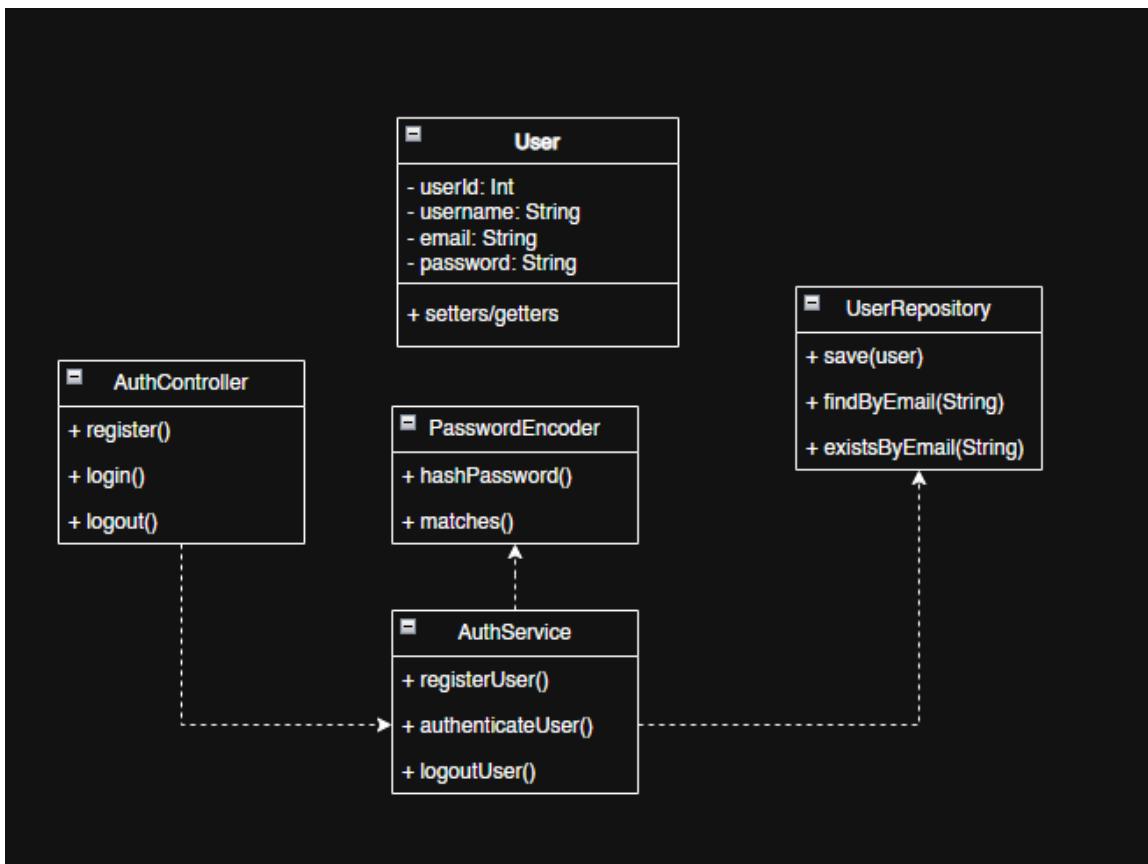
5.2. Use Case Diagram



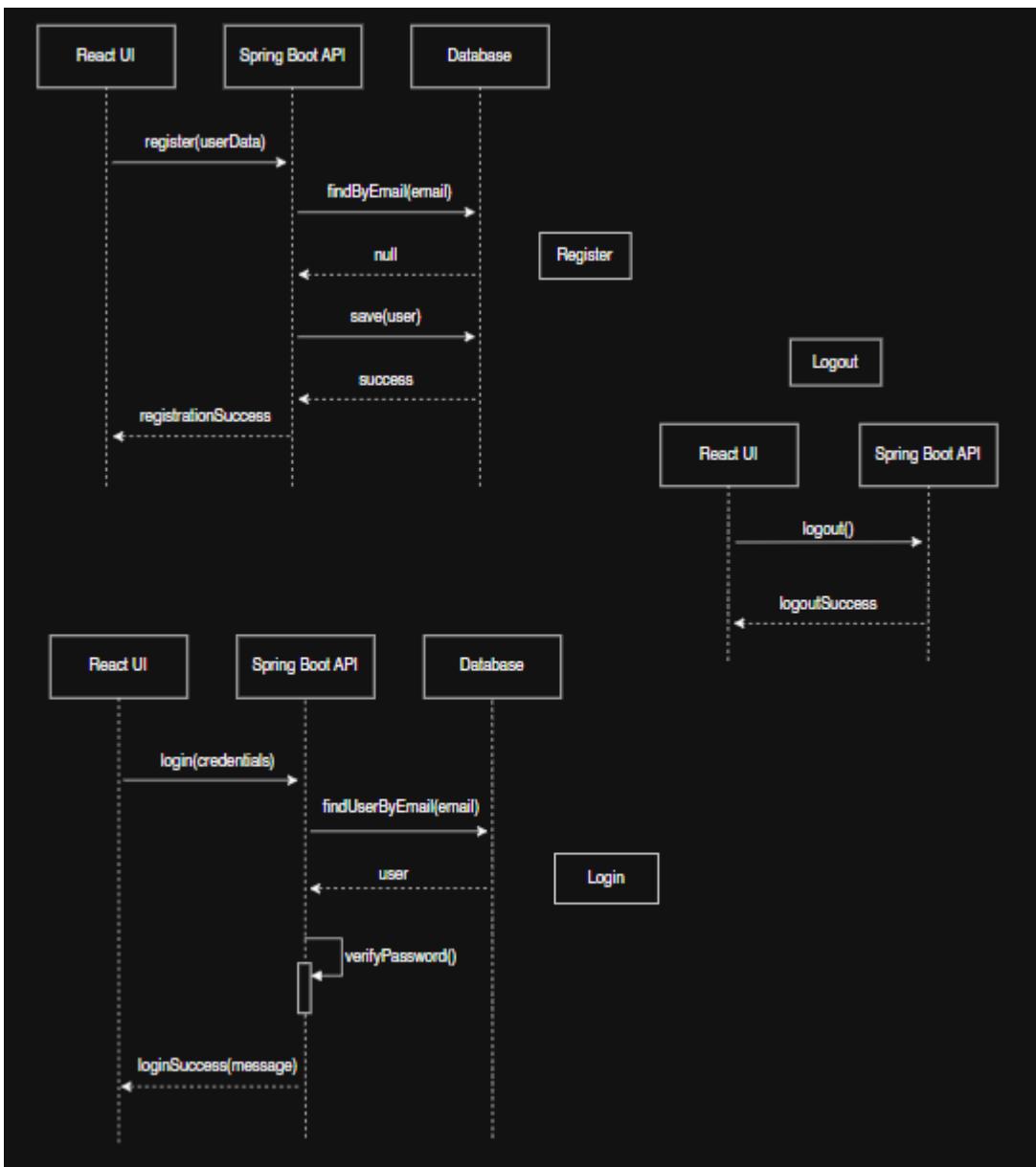
### 5.3. Activity Diagram



#### 5.4. Class Diagram



## 5.5. Sequence Diagram



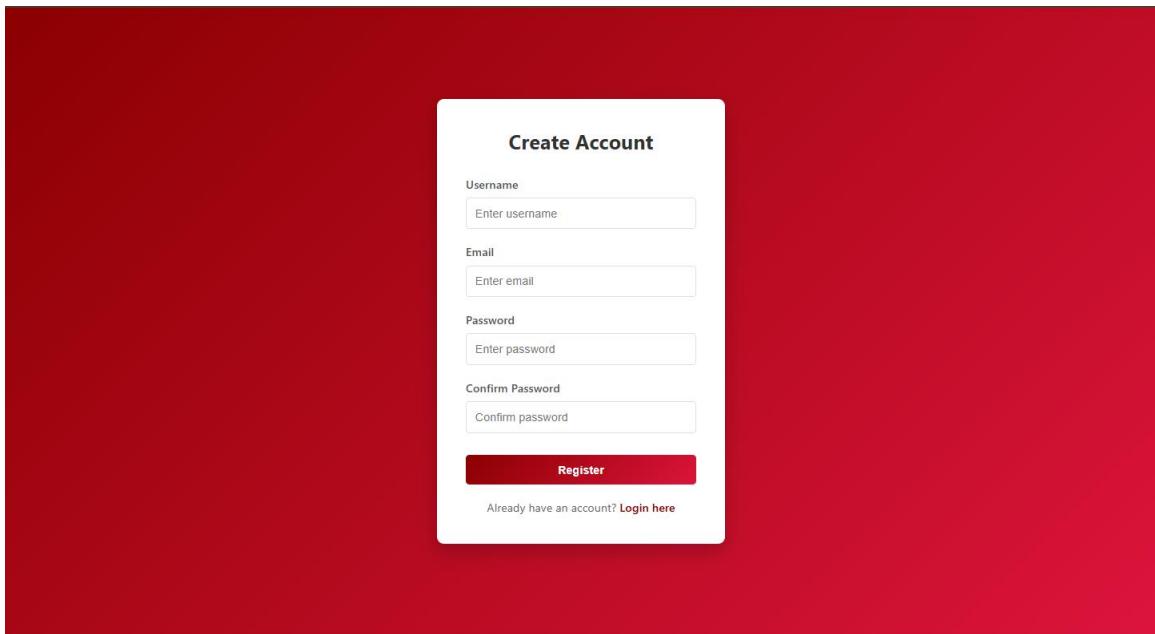
## 6. Appendices

### Testing and Validation

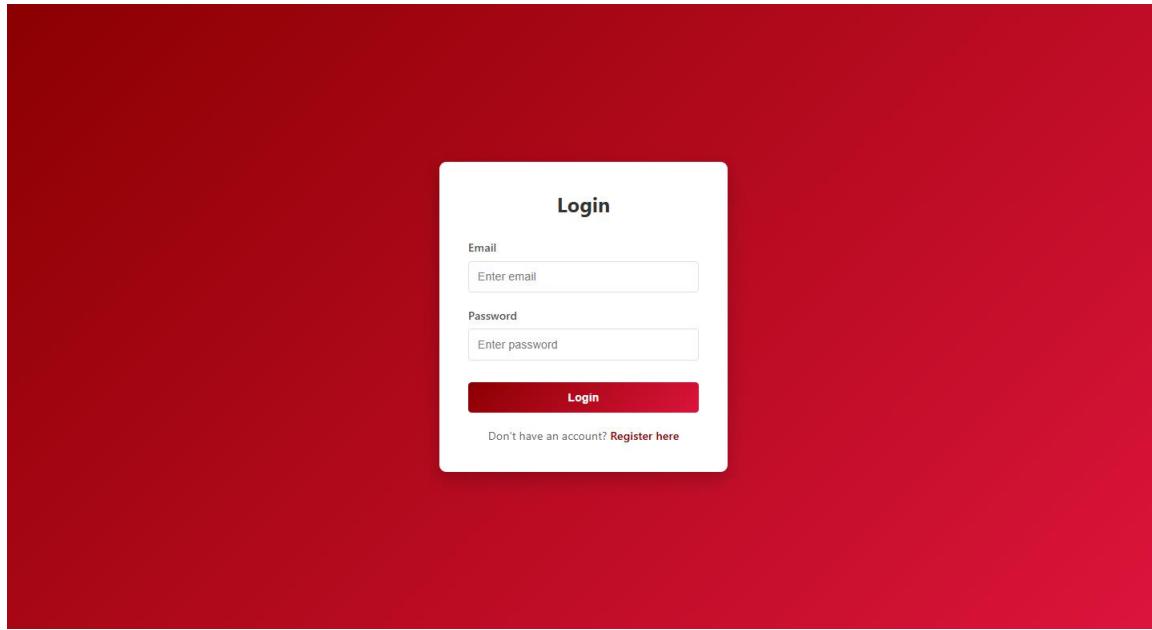
- Checked that users can register, log in, and log out successfully.
- Verified that invalid emails or passwords show error messages.

## 8. Web Screenshots

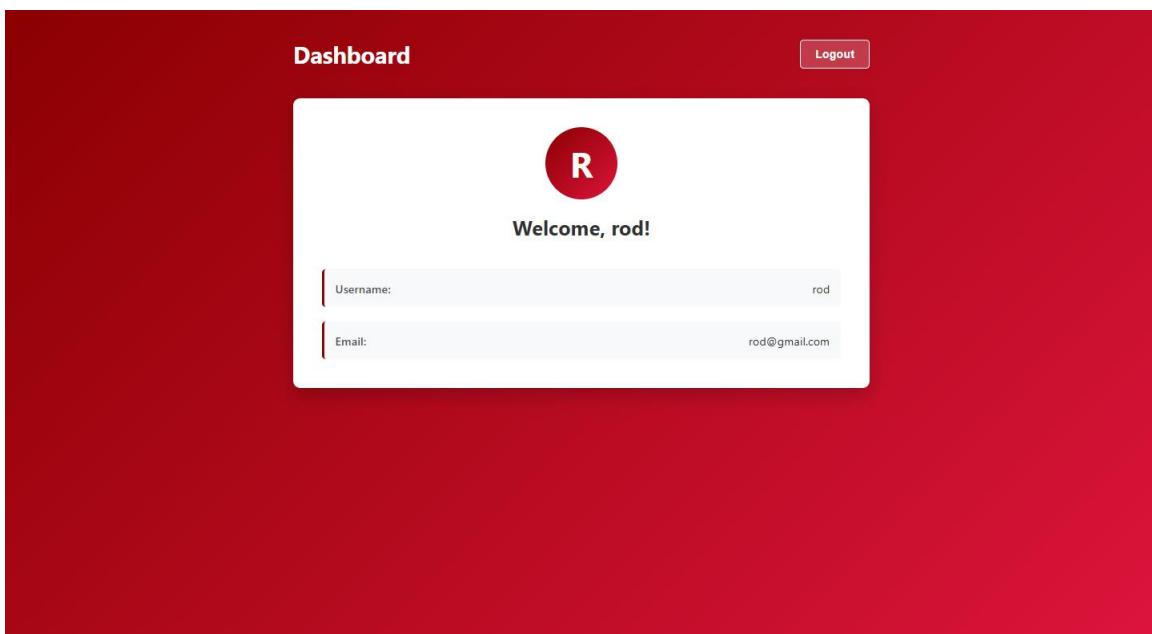
### User Registration



### User Login



## Display Profile/Dashboard



Logout

