9530

St. MOTHER THERESA ENGINEERING COLLEGE

COMPUTER SCIENCE ENGINEERING

NM-ID: 5caa608a93ff57485dc4d0b381bdf4f6

REG NO: 953023104105

DATE:15-09-2025

Completed the project named as Phase 1

FRONT END TECHNOLOGY

Login Authentication System

SUBMITTED BY:

K. SAM GIFTSON

9600282616

Login Authentication System

Problem Understanding & Requirements

1. Problem statement

In today's digital environment, data security is a top priority. Applications that lack proper authentication are prone to risks such as unauthorized access, data theft, and identity fraud. A secure login authentication system is essential to ensure that only verified users can access sensitive resources.

Objective

- To design and implement a Login Authentication System that provides:
- User identity verification through secure login.
- Data protection using encryption and secure protocols.
- Role-based access control for different stakeholders.
- Scalability to integrate with other systems (e.g., APIs, web apps, mobile apps).

2. Users and Stakeholders

- **End Users**
  - Individuals who will create accounts and log in to access the system.
  - Expect simple, secure, and quick authentication.

- **Administrators**
    - Manage user accounts (approve, suspend, reset passwords).
    - Monitor login attempts and security logs.

- **Developers**
    - Build and maintain the authentication system.
    - Integrate APIs with frontend and third-party services.

- **Business Stakeholders**
    - Ensure the system complies with security standards (e.g., GDPR).
    - Want cost-effective and scalable authentication.

3. MVP Features

- User Registration & Login (username/email + password).
- Password Security (hashing, salting, encryption).
- Session Management (JWT or secure cookies).
- Forgot Password / Reset Password workflow.
- Basic Role Management (User, Admin).
- Login Attempt Monitoring (lockout after multiple failed attempts).

4. Wireframes / API Endpoint List

Wireframes (Textual Representation)

Login Screen

- Fields: Email, Password

- Button: Login, Forgot Password

Registration Screen

- Fields: Name, Email, Password, Confirm Password
- Button: Sign Up

Admin Dashboard

- View all users

* Reset password, Lock/unlock accounts

5. Acceptance Criteria

User Registration

- User can register with email and password.
- Passwords are stored using strong hashing (e.g., bcrypt/argon2).
- Email must be unique.

Login

- Valid credentials generate a secure JWT token/session.
- Invalid credentials show error messages without revealing details.
- After 5 failed login attempts, account is temporarily locked.

Password Reset

- User can request a password reset via email.
- Reset link/token is valid only once and expires after set time (e.g., 15 minutes).

Session Management

- JWT tokens expire after a defined time (e.g., 1 hour).
- Refresh tokens are supported for re-authentication.

Admin Controls

- Admin can view all registered users.
- Admin can lock/unlock accounts.

Security

- All communication over HTTPS.
- Input validation prevents SQL injection, XSS, CSRF.
- Logs are maintained for audit and monitoring.