Lifestyle Authentication System

Overview

This project implements a secure authentication system using Next.js (Frontend),

Spring Boot (Backend), MySQL (Database), and JWT for security.

Architecture

Frontend (Next.js) communicates with Backend (Spring Boot REST APIs) using HTTP JSON requests.

Backend interacts with MySQL using JPA/Hibernate.

Backend Explanation

The backend is built with Spring Boot and follows layered architecture:

Controller, Service, Repository, Entity, DTO, and Security layers.

User Entity

The User entity represents the users table in MySQL. It stores user details,

encrypted password, role, and creation timestamp.

Authentication Flow

Registration: User submits details, password is encrypted, role assigned, and saved.

Login: Credentials validated and JWT token is generated and returned.

JWT Security

JWT tokens are used for stateless authentication. Tokens are validated on each request.

Frontend Explanation

Frontend is built using Next.js App Router. Pages handle UI and call backend APIs using fetch.

Frontend Flow

User interacts with forms → API calls → Backend → Response displayed to user.

Database

MySQL stores users with unique email and mobile, encrypted password, role, and timestamps.

Future Enhancements

Admin roles, email verification, forgot password, refresh tokens, OAuth login.

Summary

This system provides a secure, scalable authentication solution suitable for production use.