Technical Project Overview

User Authentication System — Polished Version

Executive Summary

This document provides a refined overview of the User Authentication System built with Node.js, Express, MongoDB, and JWT. The system delivers secure user registration, login, and protected route access using industry best practices for authentication, token management, and API design.

Core Objectives

• Implement secure signup and login workflows. • Protect API endpoints using JWT-based authorization. • Ensure password security through hashing. • Provide clear API documentation via Swagger. • Support scalable backend architecture.

Architecture Overview

The backend follows a modular structure separating configuration, controllers, models, routes, and middleware. MongoDB serves as the primary data store with Mongoose managing schemas and database interactions. JWT handles stateless authentication while middleware enforces access control.

Security Features

• Password hashing using bcrypt. • Token expiration and validation. • Protected routes with authorization middleware. • Error handling for invalid credentials and unauthorized access.

Conclusion

The User Authentication System demonstrates a production-ready approach to implementing secure authentication in modern web applications. Its modular design, strong security practices, and clear documentation make it suitable as a foundation for scalable services.