COLLEGE CODE : 9623

COLLEGE NAME : Amrita College of Engineering And Technology

DEPARTMENT : Computer Science and Engineering

STUDENT NM-ID : BD196A9C241DE258504454E368A99484

ROLL NO : 23CS058

DATE : 11-09-2025

Completed the project named as

Phase 1 Problem Understanding & Requirements

PROJECT NAME : LOGIN AUTHENTICATION SYSTEM

SUBMITTED BY,

NAME : MITHRAN GJ
MOBILE NO : 8825427625

Phase 1-problem understanding & Requirements

1 Problem Statement

In the current digital landscape, secure and seamless user authentication forms the cornerstone of trustworthy applications. The challenge lies in implementing an authentication system that not only ensures robust security but also provides a smooth user experience. Traditional username-password methods often suffer from vulnerabilities such as weak password practices, phishing, and cumbersome user flows, leading to poor adoption and increased security risks.

This project aims to develop a **Login Authentication System** leveraging *Google Authentication* integrated with a *Firebase* backend. The objective is to provide users a streamlined login experience via their Google accounts while maintaining secure and reliable data storage for user credentials and session management. Phase 1 focuses on establishing the foundational authentication flow, ensuring that users can securely sign in with Google and have their data managed appropriately within Firebase's real-time database.

Such a solution addresses user demands for convenience and security while providing stakeholders with a scalable and maintainable authentication infrastructure. This foundation sets the stage for future enhancements, such as multiprovider support, role-based access control, and analytics integration.

2 Users & Stakeholders

The users include:

- Regular end-users who register and log in.
- Administrators who manage user accounts and access control.

Stakeholders include the development team, security team, and business owners who rely on user security to maintain trust.

3 User Stories

The following user stories capture the core needs and behaviors envisaged for Phase 1 of the Login Authentication System.

- **As an end user**, I want to log in using my Google account so that I don't need to remember a new password.
- **As an end user**, I want my login session to be secure and protected from unauthorized access.
- **As an end user**, I want to receive clear feedback if my login fails, so I understand what went wrong.
- **As a product owner**, I want the authentication data stored securely in Firebase so that user management is centralized.
- **As a developer**, I want reusable API endpoints to facilitate login and session validation.
- **As a support agent**, I want accessible logs to troubleshoot authentication issues reported by users.

4 MVP Features

- User Registration & Email Verification
- Login with JWT or session-based authentication
- Secure password hashing using bcrypt
- Password reset with token expiration
- Role-based access control
- Audit logs for login attempts
- Input validation and sanitization

5 Wireframes / API Endpoint List

Wireframes: Login Page, Registration Page, Forgot Password Page, Reset Password Page, Dashboard.

API Endpoints:

- POST /register
- POST /login
- POST /logout
- POST /forgot-password
- POST /reset-password- GET /profile (protected route)

6 Acceptance Criteria

- Users can register, log in, log out successfully.
- System rejects weak passwords and invalid inputs.
- JWT tokens must expire after a defined time.
- Passwords are never stored in plain text.
- System is tested against brute force and injection attacks.

.