9530

ST.MOTHER THERESA ENGINEERING COLLEGE

COMPUTER SCIENCE AND ENGINEERING

NM-ID: 7930244674B12BB982040D1318B703FE3

REG NO:9530231041074

DATE:16-09-2025

Completed the project named as

Phase-1

ROUTING WITH LOGIN PROTECTION

SUBMITTED BY,

M.MUTHUMARI

PH NO: 7845106149

Phase 1 Project Report

Topic: Routing with Login Protection

Objective

The objective of this project is to design and implement a secure routing mechanism for a web application with proper login protection to ensure that only authorized users can access restricted pages.

Aim 1

To implement client-side routing that allows navigation between multiple pages without reloading the entire application.

Aim 2

To integrate authentication mechanisms (such as JWT-based login) to protect routes and ensure access control.

Users & Stakeholders

• End Users: Individuals accessing the application. • Developers: Responsible for implementation. • Project Managers: Oversee the development and deployment process. • Administrators: Manage user roles and permissions.

User Stories

• As a user, I want to log in so that I can access my dashboard. • As an admin, I want to restrict access to certain routes based on user roles. • As a developer, I want a clear routing structure to make the app scalable.

MVP Features

• Login and Logout functionality • Route protection (authenticated & public routes) • Role-based access control • Error handling for unauthorized access

Wireframe / API Endpoint List

• /login → User authentication endpoint • /dashboard → Protected route accessible after login • /logout → Logout endpoint to clear user session

Acceptance Criteria

• Users must log in to access protected pages. • Unauthorized users must be redirected to login page. • System must display meaningful error messages for failed login attempts. • Application must maintain session state until user logs out.

Flowchart

The flow starts with user login. If login is successful, user is routed to the dashboard. If login fails, an error message is shown. When accessing a protected route, the system checks authentication status. If authenticated, access is granted; otherwise, user is redirected to login.

Conclusion

The Phase 1 report successfully defines the problem, objectives, and solution approach for implementing routing with login protection. The next phase will involve designing the UI, selecting the tech stack, and developing the backend logic for authentication.