COLLEGE CODE:[8223]

COLLEGE NAME: [Vandayar Engineering college]

DEPARTMENT: [Computer Science And Engineering]

STUDENT NM-ID :3EB40010185B9B4BFD14530102F3457A

ROLL NO: 822323104013

DATE:[19.09.2025]

Completed the project named as

Phase-1

TECHNOLOGY PROJECT NAME: USER AUTHENTICATION SYSTEM

SUBMITTED BY, NAME:[KEERTHIKA.M]

MOBILE NO[70106 13062]

Problem Statement

1. Many systems face unauthorized access problems without proper authentication.

2. Users’ personal and confidential data is at risk of being stolen.

3. Weak or simple passwords lead to security breaches.

4. Lack of secure authentication causes identity theft.

5. Many applications do not use encryption for storing passwords.

6. Without a proper system, it is hard to manage user sessions safely.

7. Increasing cyber-attacks create the need for a strong user authentication system.

Users and Stakeholders

Users

1. End users who log in to access services.

2. Administrators who manage user accounts.

3. Developers maintaining the system.

4. IT support team helping users.

Stakeholders

1. Organization that owns the system.

2. Clients/customers depending on security.

3. Government/regulators ensuring compliance.

4. Security team preventing cyber threats.

MVP Features

1. User Registration – New users can sign up with username, email, and password.

2. Unique Username Check – System ensures no duplicate usernames.

3. User Login – Secure login with username and password.

4. Password Encryption – All passwords stored in encrypted format (e.g., SHA-256/bcrypt).

5. Forgot Password – Option to reset password via email/OTP.

6. Change Password – Logged-in users can change password anytime.

7. User Profile Management – Users can update personal details.

8. Logout Option – Secure logout to end active sessions.

9. Admin Panel – Admin can view, add, or remove users.

10. Role Management – Different roles like user, admin, developer.

11. Basic Session Management – Tracks login sessions for each user.

12. Invalid Login Attempts Control – Account lock after multiple failed logins.

13. Activity Logs – System records user login/logout history.

14. Responsive UI – Simple and user-friendly interface for web/mobile.

Wireframe / API Endpoints

1. Registration Page

Input fields: Username, Email, Password, Confirm Password

Button: Sign Up

API: POST /api/register – Create new user account

2. Login Page

Input fields: Username, Password

Button: Login

Link: Forgot Password

API: POST /api/login – Authenticate user

3. Forgot Password Page

Input field: Email or Username

Button: Send OTP / Reset Link

Input field: New Password, Confirm Password

API: POST /api/forgot-password – Send reset link/OTP

4. User Dashboard

Welcome message (e.g., "Hello, User!")

Menu: Profile, Settings, Activity Log

Button: Logout

API: POST /api/logout – End user session

5. Profile Management Page

Fields: Name, Email, Phone Number

Option: Change Password

Button: Save Changes

API: GET /api/us…

6. Admin Panel

Table: List of all users with details

Buttons: Add User, Delete User, Edit User

Option: Assign Roles (Admin/User)

API Endpoints

1. User Registration

Endpoint: POST /api/register

Function: Creates a new user account.

2. User Login

Endpoint: POST /api/login

Function: Authenticates user with username and password.

3. User Logout

Endpoint: POST /api/logout

Function: Ends user session safely.

4. Forgot Password

Endpoint: POST /api/forgot-password

Function: Sends OTP or reset link to user.

5. Change Password

Endpoint: PUT /api/change-password

Function: Allows logged-in user to update password

Acceptance Criteria

1. User Registration

1. Users can register with a valid username, email, and password.

2. System checks for unique usernames and emails.

3. Email verification is required to activate the account.

4. Registration errors are displayed clearly to the user.

2. User Login

1. Registered users can log in with correct credentials.

2. System restricts multiple failed login attempts.

3. Login activity is recorded for security monitoring.

4. Users are redirected to dashboard upon successful login.

3. Password Management

1. Users can reset password via OTP or email link.

2. Passwords are encrypted in the database.

3. Users can change password from profile settings.

4. Weak passwords are not allowed during reset or change.

4. Profile Management

1. Users can update personal details (name, email, phone).

2. Users can view account information.

3. Changes are saved securely in the database.

5. Admin Management

1. Admin can view a list of all registered users.

2. Admin can add or delete user accounts.

3. Admin can assign roles (Admin/User).

6. Session & Security

1. System tracks active sessions.

2. Sessions expire after inactivity.

3. Secure logout prevents unauthorized access.

7. Compliance & Audit

1. System maintains activity logs for auditing.

2. Security measures comply with standards.

3. Regulatory compliance is ensured for sensitive data.