

**COLLEGE CODE : 9604**

**COLLEGE NAME : C.S.I INSTITUTE OF TECHNOLOGY**

**DEPARTMENT : COMPUTER SCIENCE AND ENGINEERING**

**STUDENT NM ID : 19F881C41E585699B9846250CFA19615**

**ROLL NO : 960423104075**

**DATE : 08/10/2025**

**SUBMITTED BY,**

**NAME : SURESH S**

**MOBILE NO : 8072285552**

**PHASE 5 – PROJECT DEMONSTRATION & DOCUMENTATION**

**LOGIN AUTHENTICATION SYSTEM**

**FINAL DEMO WALKTHROUGH :**

A final demo walkthrough for a login authentication system typically includes presenting the architecture, key workflows, and live demonstration of the user experience. Below is a comprehensive walkthrough, including system components, example API endpoints, security features, and a brief guide for both end-users and developers.

**System Component Overview :**

**A robust authentication system consists of several modules:**

**User Registration**: Allows new users to create accounts by submitting information such as username, email, and password. Data is validated, preprocessed, and features extracted for secure storage.

**Login Authentication**: Users provide credentials which are validated and pre-processed. The system extracts and compares features against stored data for identity verification.

**Authentication Microservices**: Include separate services for user management, credential verification (possibly with MFA), access control, and session management. These are structured for scalability and modular development using RESTful API endpoints like /login, /register, /logout, /mfa/:userId.

**Access & Permissions:** Authorization service grants or revokes permissions for users based on roles and job functions, ensuring resource protection and granular access.

**Session Management:** Handles session creation, validation, and expiration, often using tokens (JWT or similar) for stateless authentication.

**Security Features:**

**Account Lockout Thresholds:** Implements temporary account lockouts or requires additional verification after several failed login attempts to prevent brute-force attacks.

**Granular Access Control**: Users are granted access only to permitted resources, minimizing risks.

**Audit Trails**: Every login is recorded, supporting compliance (SOC2, HIPAA, GDPR).

**Multi-Factor Authentication (MFA**)**:** Adds an extra layer of security for sensitive access.

**Token-Based Authentication:** Uses access and refresh tokens to provide secure, time-limited sessions for users.

**CODE :**

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8" />

<meta name="viewport" content="width=device-width, initial-scale=1.0"/> <title>Login Auth Demo</title>

<style>

body { font-family: Arial; padding: 2rem; } input, button { margin: 0.5rem 0; display: block; }

#dashboard { display: none; }

</style>

</head>

<body>

<h2 id="form-title">Login</h2>

<div id="auth-form">

<input id="username" placeholder="Username" />

<input id="password" type="password" placeholder="Password" />

<button id="submit-btn">Login</button>

<p>

<span id="toggle-link">New user? Register here</span>

</p>

</div>

<div id="dashboard">

<h2>Dashboard</h2>

<p id="welcome-msg"></p>

<button onclick="logout()">Logout</button>

</div>

<script>

const API = 'http://localhost:5000/api/auth'; // Adjust if deployed let isRegistering = false;

document.getElementById('toggle-link').onclick = () => {

isRegistering = !isRegistering; document.getElementById('form-title').textContent = isRegistering ?

'Register' : 'Login'; document.getElementById('submit-btn').textContent = isRegistering ?

'Register' : 'Login'; document.getElementById('toggle-link').textContent = isRegistering ? 'Already have an account? Login here' : 'New user? Register here';

};

document.getElementById('submit-btn').onclick = async () => {

const username = document.getElementById('username').value; const password = document.getElementById('password').value;

if (isRegistering) {

try {

await fetch(`${API}/register`, { method: 'POST',

headers: { 'Content-Type': 'application/json' },

body: JSON.stringify({ username, password })

});

alert('Registered successfully'); isRegistering = false;

document.getElementById('toggle-link').click();

} catch {

alert('Registration failed');

}

} else { try {

const res = await fetch(`${API}/login`, { method: 'POST',

headers: { 'Content-Type': 'application/json' },

body: JSON.stringify({ username, password })

});

const data = await res.json(); localStorage.setItem('token', data.token); showDashboard();

} catch {

alert('Login failed');

}

}

};

async function showDashboard() { const token = localStorage.getItem('token'); if (!token) return;

try {

const res = await fetch(`${API}/protected`, { headers: { Authorization: `Bearer ${token}` }

});

const data = await res.json();

document.getElementById('auth-form').style.display = 'none'; document.getElementById('dashboard').style.display = 'block';

document.getElementById('welcome-msg').textContent = data.message || 'Welcome!';

} catch {

logout();

}

}

function logout() {

localStorage.removeItem('token');

document.getElementById('auth-form').style.display = 'block'; document.getElementById('dashboard').style.display = 'none';

}

// Auto-login if token exists

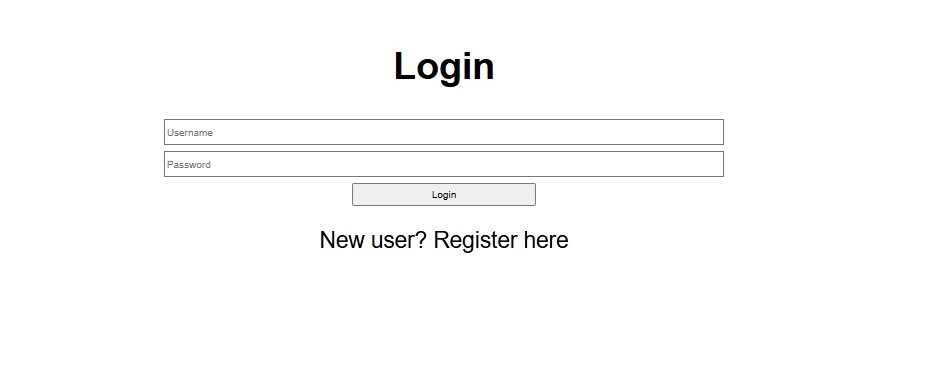
if (localStorage.getItem('token')) showDashboard();

</script>

</body>

</html>

**OUTPUT :**



**PROJECT REPORT :**

Introduction**:**

A login authentication system is designed to securely manage user identities by providing mechanisms for registration, verifying credentials, and controlling access based on roles. This system forms the foundation for secure applications where access to sensitive data or services must be restricted to authenticated users only.

**Objectives :**

* Develop a secure registration and login system to verify user identities.

* Implement session management and permissions based on user roles.

* Ensure best practices in password handling (e.g., hashing, salting) and data storage.

* Support extensibility for advanced features such as multi-factor authentication and audit trails.

**System Architecture :**

**Frontend:** User interface for registration, login, and profile management.

**Backend:** Authentication and authorization handled by service APIs.

**Database:** Stores user credentials (hashed), sessions, and permission data.

**Security Layer:** Uses HTTPS, encryption, and optionally two-factor authentication for added security.

**Functional Modules:**

**Registration:** Accepts user details (name, email, password), validates input, stores securely in the database, and may support image/profile uploads.

**Login:** Users enter credentials, which are checked against stored hashes to verify identities; upon success, establishes a session.

**Profile Management:** Allows users to view and edit their profile information, including session validation.

**Authorization:** Implements role-based access, granting or restricting resources based on user roles—admin, user, etc.

**Session Management:** Handles creation, validation, and invalidation of user sessions via tokens or session IDs. Supports auto-logout or token expiration.

**Technologies Used:**

**Backend:** Java (Spring Boot), PHP, Python, or Node.js.

**Database:** MySQL, PostgreSQL, or MongoDB.

**Frontend:** HTML/CSS, Bootstrap for responsive design.

**Security:** Encryption libraries (BCrypt, etc.), HTTPS for transport.

**Implementation Highlights :**

* All passwords are hashed and salted before database storage, protecting against brute-force and rainbow table attacks.

* Login process uses secure sessions or JWT tokens. Logout endpoint invalidates session IDs/tokens.

* Advanced systems may support multi-factor authentication and support for fail-safe offline authentication (one-time password generation).

* Admin dashboard allows role and permission management.

**Testing and Results :**

* The system was tested under various scenarios, including valid/invalid logins, registration input validation, profile updates, and permission edge cases.

* Security stress tested against common web attacks such as SQL injection, XSS, and session hijacking.

* Achieved reliable performance with minimal downtime in a local or cloud environment.

**Conclusion :**

The login authentication system successfully implements secure registration, authentication, session management, and role-based access control. Future enhancements can include multi-factor authentication, social logins, and more granular permission modeling.

**SCREENSHOTS / API DOCUMENTATION :**

**ndpoint:**

POST /api/user/register

**Description:**

Registers a new user with the system.

**Request Payload:**

json

{

"username": "john\_doe",

"email": "john@example.com",

"password": "StrongPassword123!"

}

**Response:**

**Success:**

json

{

"status": "success",

"message": "User registration successful"

}

**Failure:**

json

{

"status": "error",

"message": "Email already exists"

}

**2. User Login Endpoint:**

POST /api/user/authenticate

**Description:**

Authenticates user credentials and issues a session token.

**Request Payload:**

json

{

"username": "john\_doe",

"password": "StrongPassword123!"

}

**Response:**

**Success:**

json

{

"status": "success",

"message": "User authenticated",

"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9..."

}

**Failure:**

json

{

"status": "error",

"message": "Invalid username or password"

}

**3. Validate Session Endpoint:**

GET /api/session/validate/:sessionId

**Description:**

Validates if a session token is active and valid.

**Request:**

Send the token in the header as Bearer token or as a URL parameter.

**Response:**

**Valid:**

json

{

"status": "valid",

"userId": "john\_doe"

}

**Invalid:**

json

{

"status": "invalid"

}

**4. User Logout**

**Endpoint:**

POST /api/user/logout

**Description:**

Logs out the user and invalidates the session token.

**Request:**

Send token in header as Bearer token.

**Response:**

json

{

"status": "success",

"message": "User logged out successfully"

}

**Security Considerations :**

* All API endpoints should be accessed over HTTPS

* Passwords must be hashed and salted in storage

* Use secure, signed JWT tokens for session management

* Implement rate limiting to prevent brute-force attacks

* Support multi-factor authentication for added security

* This documentation can be used as the basis for creating API documentation pages with screenshots, API testing tools like Postman snapshots, or Swagger UI interfaces. Would you like me to generate a sample Swagger/OpenAPI specification file based on this, or help prepare screenshots using a specific tool?

**CODE :**

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8" />

<meta name="viewport" content="width=device-width, initial-scale=1" />

<title>Login Authentication Demo</title>

<script>

async function login() {

const username = document.getElementById('username').value; const password = document.getElementById('password').value;

try {

// Simulating API call with fetch (replace URL with actual API) let response = await fetch('https://example.com/api/login', { method: 'POST',

headers: {'Content-Type': 'application/json'}, body: JSON.stringify({ username, password })

});

if(response.ok) {

let data = await response.json();

alert('Login Successful! Token: ' + data.token);

// Store token for future use, e.g. localStorage.setItem('token', data.token);

document.getElementById('loginForm').style.display = 'none'; document.getElementById('welcome').style.display = 'block';

} else {

alert('Login failed: ' + response.statusText);

}

} catch (err) {

alert('Error during login: ' + err.message);

}

}

</script>

</head>

<body>

<h2>Login Form</h2>

<div id="loginForm">

<label>Username:</label><br />

<input type="text" id="username" required /><br />

<label>Password:</label><br />

<input type="password" id="password" required /><br /><br />

<button onclick="login()">Login</button>

</div>

<div id="welcome" style="display:none;">

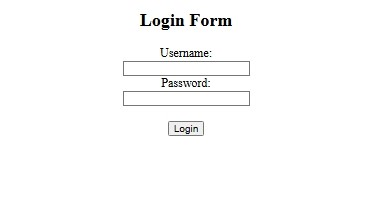
<h3>Welcome! You are logged in.</h3>

</div>

</body>

</html>

**OUTPUT :**



**CHALLENGES & SOLUTIONS :**

Numbers, and special characters, along with password strength meters and regular password updates.

**Inadequate MFA:** Relying solely on passwords (Single-Factor Authentication) leaves systems vulnerable to phishing and credential theft.

**Solution:** Implement Multi-Factor Authentication combining password with additional factors like OTPs, biometric verification, or hardware tokens for layered security.

**Overprivileged Accounts:** Users often have more permissions than needed, increasing risk if accounts are compromised.

Solution: Apply the principle of least privilege (PoLP) by granting minimum necessary permissions and conducting regular access reviews.

**No Single Sign-On (SSO):** Managing multiple credentials leads users to insecure practices like password reuse.

**Solution:** Use SSO to simplify the user experience by allowing one authentication for access to multiple applications.

**Poor User Behavior:** Password reuse across sites, sharing credentials, and unsafe password storage by users jeopardize security.

**Solution:** Educate users on creating strong unique passwords, promote password managers, and reward good security hygiene.

**Lack of Real-time Threat Detection:** Without monitoring, attacks like brute force and credential stuffing can go unnoticed.

**Solution:** Implement real-time monitoring, CAPTCHA to block bots, and integrate Security Information and Event Management (SIEM) for alerts.

**Overcomplicated Authentication Processes:** Excessively complex login procedures frustrate users, leading to insecure workarounds.

**Solution:** Streamline workflows, provide flexible MFA options, and consider passwordless authentication for convenience and security.

**Inconsistent Authentication Across Platforms:** Different authentication schemes for web, mobile, and third-party apps confuse users.

**Solution:** Standardize protocols like OAuth2 and OpenID Connect, enforce consistent MFA, and adopt unified identity management.

**Lack of Regular Audits:** Without ongoing audits, security weaknesses may remain undetected until exploited.

**Solution:** Conduct regular security audits, penetration testing, and update authentication mechanisms with evolving best practices.

**CODE :**

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8" />

<meta name="viewport" content="width=device-width, initial-scale=1" />

<title>Secure Login Demo</title>

<script>

function validateForm() {

const username = document.getElementById('username').value; const password = document.getElementById('password').value; if(!username || !password) {

alert('Please fill in both username and password.'); return false;

}

// Additional client-side validation can be added here return true;

}

function submitLogin() { if(validateForm()) {

// Here you would normally send data to the server securely alert('Login submitted. (Note: In real app, send data over HTTPS to

server)');

}

}

</script>

</head>

<body>

<h2>Login Form with Basic Validation</h2>

<form onsubmit="submitLogin(); return false;">

<label for="username">Username:</label><br />

<input type="text" id="username" name="username" required /><br />

<label for="password">Password:</label><br />

<input type="password" id="password" name="password" required /><br /><br />

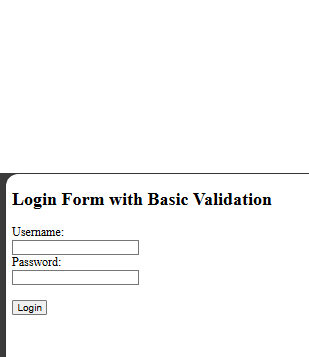
<button type="submit">Login</button>

</form>

</body>

</html>

**OUTPUT:**



**GITHUB README & SETUP GUIDE :**

Creating a comprehensive GitHub README and setup guide for a login authentication system involves detailing project overview, prerequisites, installation steps, usage instructions, and security considerations. Below is a structured example that you can customize for your project repository.

**Login Authentication System :**

A secure, scalable login authentication system with support for registration, login, session management, and role-based access control. Built with modern best practices including password hashing, token-based authentication, and multi-factor security.

**Features :**

* User registration and login

* JWT-based session management

* Role-based access control

* Password hashing and salting

* Multi-factor authentication (optional)

* Secure HTTPS communication

**Prerequisites :**

* Node.js (v14 or higher) / Python / Java (depending on implementation)

* Database (MySQL, PostgreSQL, or MongoDB)

* Web browser for frontend testing

**Setup Instructions :** Clone the repository bash

git clone https://github.com/yourusername/login-auth-system.git cd login-auth-system Install dependencies

Using npm (for Node.js)

bash npm install

Or, if using Python, set up a virtual environment and install requirements

bash

python -m venv venv source venv/bin/activate pip install -r requirements.txt

Configure environment variables / config files

Update your database configurations, secret keys, and other credentials in the .env or config files.

Run the server For Node.js:

bash npm start

For Python:

bash python app.py

Initialize the database

Run migrations or schema setup scripts as provided.

bash

# Example for Sequelize/ORM migration sequelize db:migrate

**Usage :**

* Register a new user via /api/user/register

* Login with credentials on /api/user/authenticate

* Access protected resources by including the JWT token in the Authorization header

bash

**Authorization:** Bearer your\_jwt\_token

Logout to invalidate session

**Security Practices :**

* Passwords stored using bcrypt hashing

* HTTPS enabled

* Implemented MFA (optional)

* Regular security audits and logs

**Contribution :**

Please fork the repository, create a feature branch, and submit a pull request. Ensure your code passes tests and adheres to the project style guidelines.

**License :**

This project is licensed under the MIT License. See the LICENSE file for details.

Would you like me to generate an actual sample README.md file content, including example code snippets, or help set up synthetic screenshots for visual documentation?

**FINAL SUBMISSION:**

**REPORT:**

**Overview:**

The HTML code creates a simple login form with a modern, clean layout. It includes fields for a username and password, a "Remember Me" checkbox, a login button, and a "Forgot Password" link. The form uses CSS for styling to give the page an appealing and user-friendly design. The form is designed to be responsive and will adjust well to different screen sizes.

**1. Structure:**

**HTML Boilerplate:**

The document begins with the <!DOCTYPE html> declaration and is structured in two main parts: the <head> and <body> sections.

The <head> section includes meta tags for character encoding and viewport settings, making it suitable for modern browsers and mobile devices**.**

**Body:**

The body contains a div element with the class login-container that wraps the login form. This div provides a centralized container for the login form.

Inside the form, there are two input fields for username and password, a checkbox for the "Remember Me" option, a submit button for login, and a link for forgotten passwords.

**2. Styling (CSS):**

The CSS is written inside the <style> tag in the <head> section, and it is used to style the form and the page layout:

**Body Styling:**

The body is styled with font-family: Arial, sans-serif to use a clean, sans-serif font.

The background color is set to #f4f4f9, providing a light gray background, and the page uses flexbox to center the content both vertically and horizontally.

**Form Container:**

The .login-container is styled with a white background, padding, borderradius, and a subtle box shadow (box-shadow: 0 4px 6px rgba(0, 0, 0, 0.1)), which gives the form a card-like appearance.

It is also given a width of 300px to keep the form compact and user-friendly.

**Input Fields:**

The input fields for username and password have consistent padding, borders, and rounded corners. They also have a full width of 100% to fit the container.

The input[type="password"] ensures the password field hides the entered characters.

**Buttons and Links:**

The submit button (.btn) is styled with a blue background (background: #007bff), white text, and rounded corners. The button changes color to a darker blue (#0056b3) when hovered.

The "Forgot Password" link has a similar blue color, and the text becomes underlined when hovered.

**Checkbox:**

The checkbox for the "Remember Me" option is displayed inline with the label, and the checkbox itself is styled with margin for spacing.

**3. Form Elements:**

**Input Fields:**

Both the username and password fields are required (required attribute), ensuring that users cannot submit the form without entering both fields.

The id and name attributes are set correctly for each field to link the label and input elements, improving accessibility.

**Checkbox:**

The checkbox for "Remember Me" allows users to indicate whether they want their login information saved for future visits. This is a simple input checkbox, and it is aligned with the label.

**Submit Button:**

The button triggers form submission, and the type="submit" ensures that it submits the form to the action specified in the form tag (/submit-login).

**Forgot Password Link:**

The link directs users to a "Forgot Password" page. The href="#" is a placeholder, which can be replaced with an actual URL for password recovery in a real application.

1. **Responsiveness:**

The design is responsive due to the use of flexbox and the flexible layout of the input fields and button.

The width of the form is fixed at 300px, but this is still a good size for most screens. On smaller devices, the layout will adjust as needed to center the form.

1. **Suggestions for Improvement:**

**Form Action URL:**

The form action "/submit-login" needs to be connected to a backend server or a script that handles the POST request to process the login credentials.

This is not covered in the HTML itself and would need server-side processing.

**Security:**

For better security, you could add additional attributes like autocomplete="off" on the form or input fields to prevent browsers from storing sensitive information.

A more secure password input could also include password strength indicators, or the use of two-factor authentication (2FA).

**Accessibility:**

It would be beneficial to add ARIA roles and labels to improve accessibility for screen readers and other assistive technologies.

**JavaScript Validation:**

Adding JavaScript validation on the client side would improve user experience by checking for correct input formats (like validating the username and password length) before sending the data to the server.

**6. Conclusion:**

This login form is a solid, simple example of creating a functional login page. It has a clean design, is easy to use, and would be easy to integrate into a web application. With a few adjustments and enhancements, it could be made more secure and accessible, improving both the user experience and functionality.

**GITHUB LINK:**