Authentication and Role Control

Milestone-1: Infosys Internship Assessment

Intern Name:Anusha D R

Week1

Modern systems require secure access control to ensure that users can access only authorized resources.

In the absence of authentication and role control:

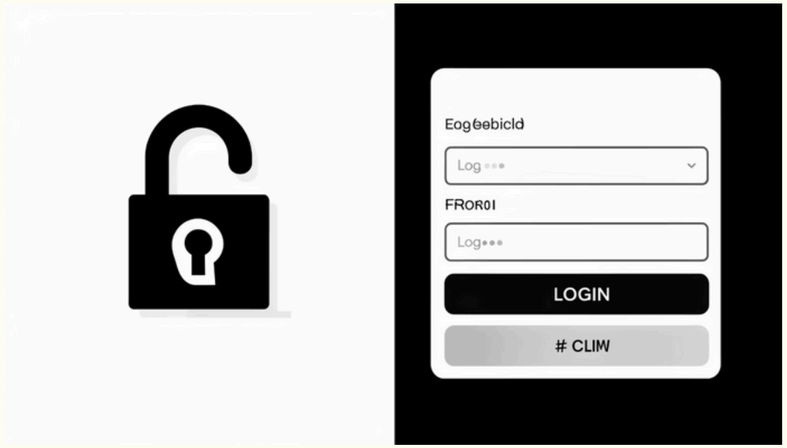
- Unauthorized users may access sensitive pages
- Admin-only features may be misused
- System security and data integrity are compromised

In traditional systems without role control:

- All users are treated the same
- No separation between Admin and Employee
- Any user can access admin-only pages
- High risk of security breaches

1. Login-based Authentication
2. Role-based Access Control
3. Admin & Employee Separation
4. Secure Redirection

Modules



1

Authentication Module

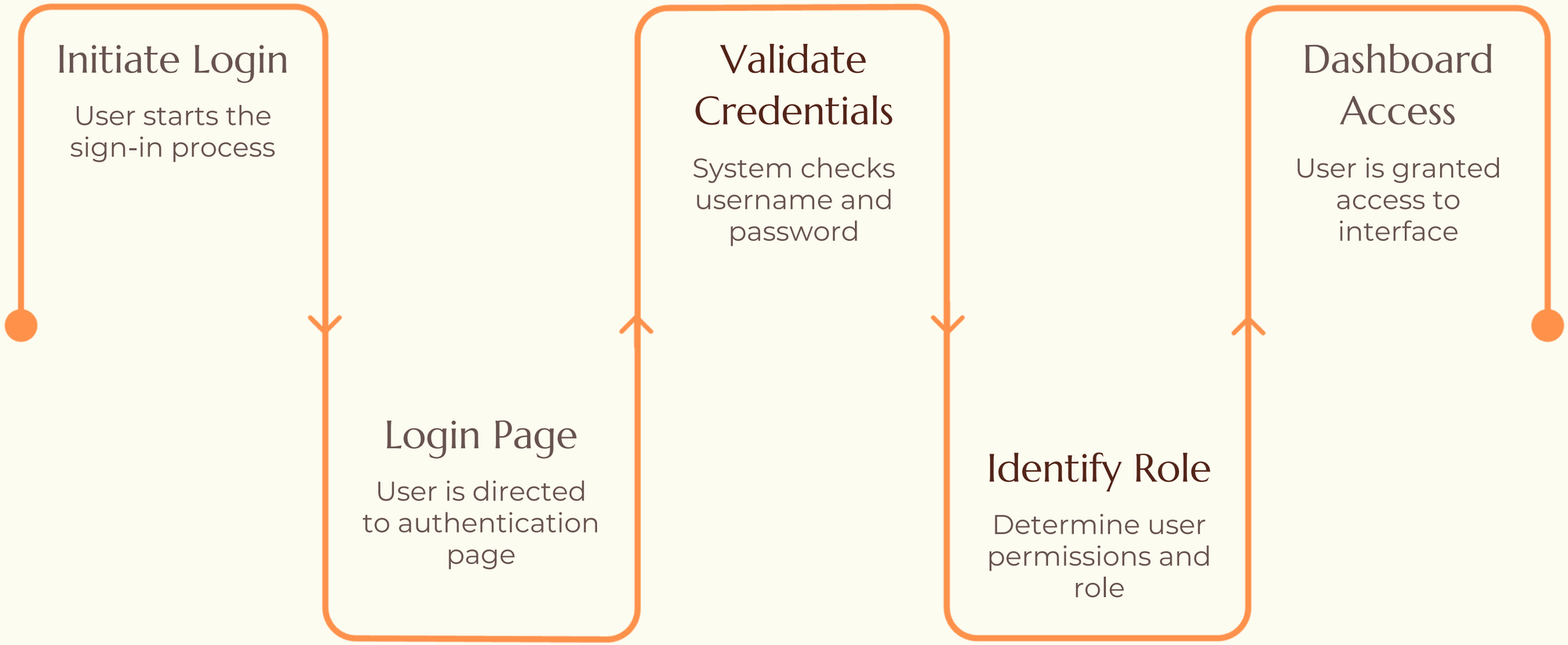
This module is responsible for validating user-provided login credentials against stored data, ensuring only legitimate users can proceed.

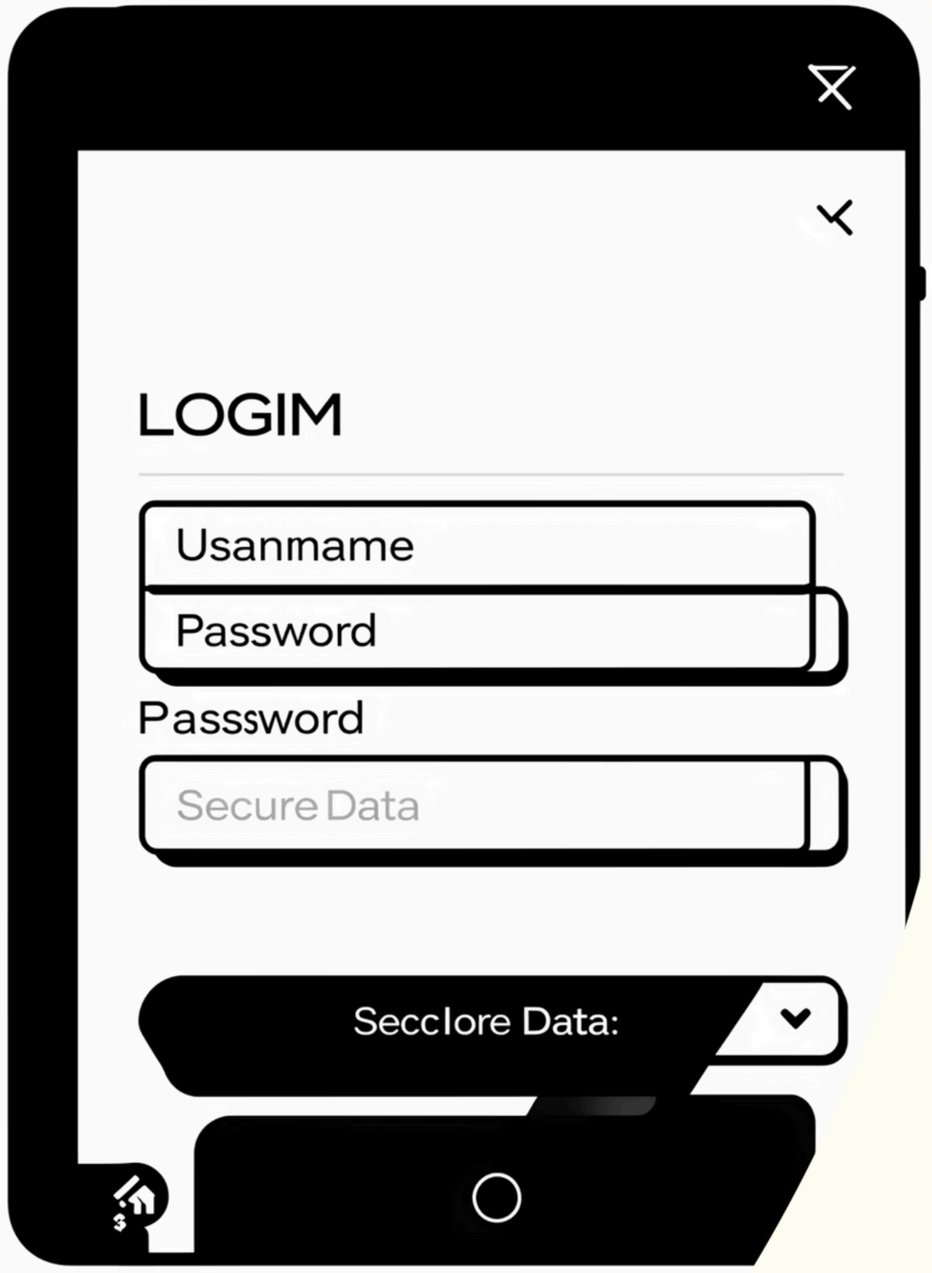
2

Role Control Module

Once authenticated, this module dynamically controls which pages and resources a user can access based on their assigned role (e.g., Admin or Employee).

System Flow: From Login to Dashboard





Module 1: The Login Gateway

01

Accepts Credentials

The login module provides a user-friendly interface for entering a username and password.

02

Validates Credentials

It then processes these inputs, verifying their accuracy against predefined user data using JavaScript logic.

03

Redirects by Role

Upon successful validation, the user is automatically directed to their designated page based on their identified role.

Key Components:

login.html

The primary entry point for user authentication, structured with HTML for form elements.

admin.html

The restricted dashboard accessible only to authenticated administrators.

employee.html

The dedicated interface for regular employees, with features relevant to their role.

JavaScript Validation Logic

Client-side scripting responsible for handling credential checks and dynamic redirection.

Pseudocode

```
START
Read username and password

IF username = admin AND password valid
    Redirect to Admin Dashboard
ELSE IF username = employee AND password valid
    Redirect to Employee Dashboard
ELSE
    Show error message
END IF

END
```

PSEUDOCODE – AUTHCONTROLLER

```
FUNCTION signup(request)
    userDetails = request data
    result = AuthService.registerUser(userDetails)
    RETURN result
END FUNCTION

FUNCTION signin(request)
    token = AuthService.authenticate(username, password)
    RETURN token
END FUNCTION
```

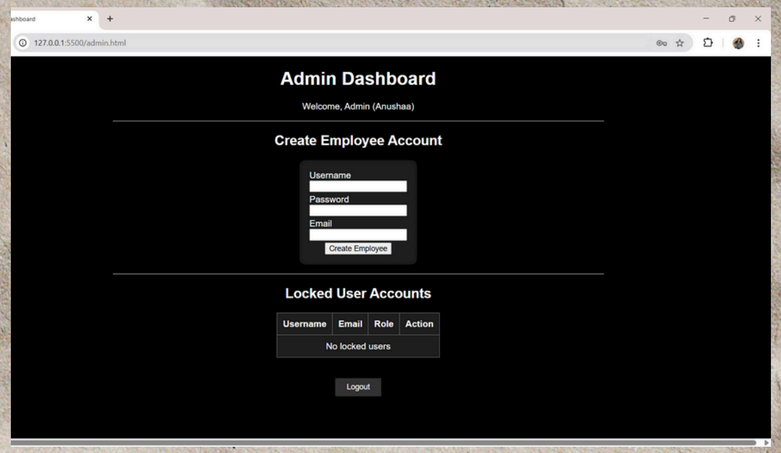
PSEUDOCODE – AUTHSERVICE

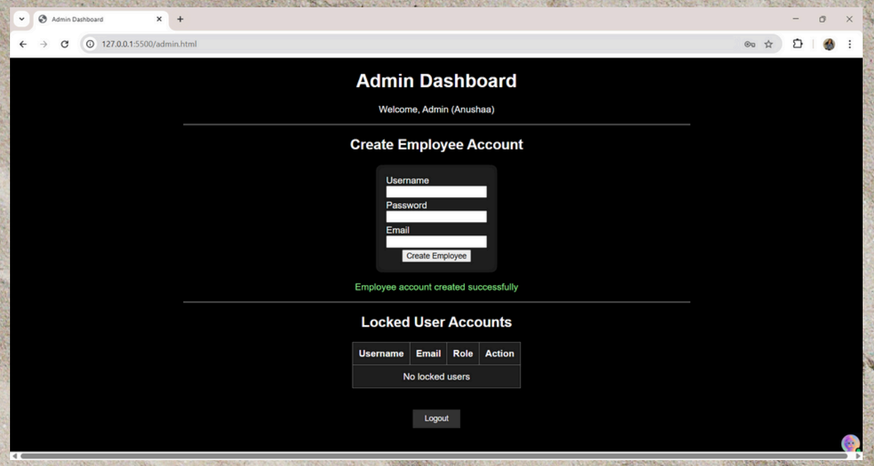
```
FUNCTION registerUser(userDetails)
    IF username exists THEN
        RETURN "User already exists"
    END IF
    encrypt password
    save user
    RETURN "Signup successful"
END FUNCTION

FUNCTION authenticate(username, password)
    validate user
    generate JWT token
    RETURN token
END FUNCTION
```

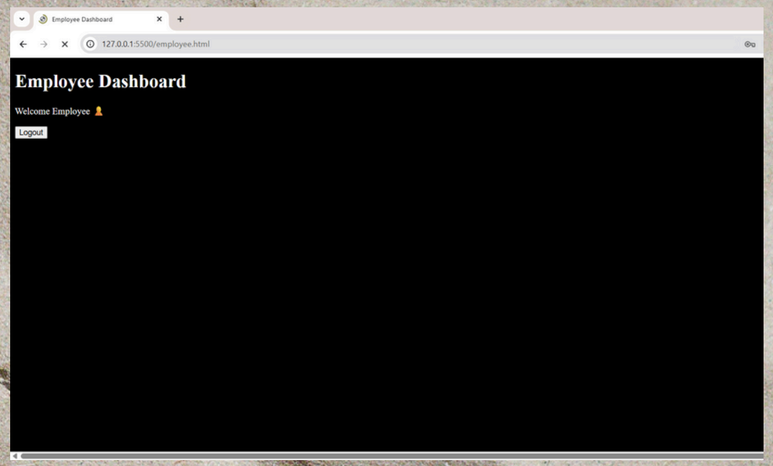
Pseudocode – JWTUtility

```
FUNCTION generateToken(user)
    add username & role to payload
    sign token with secret key
    RETURN JWT
END FUNCTION

FUNCTION validateToken(token)
    verify signature
    check expiry
END FUNCTION
```


Inventra Login
127.0.0.1:5500/index.html
Inventra Login
Username *
Password *
Login
Sign Up
Forgot Password

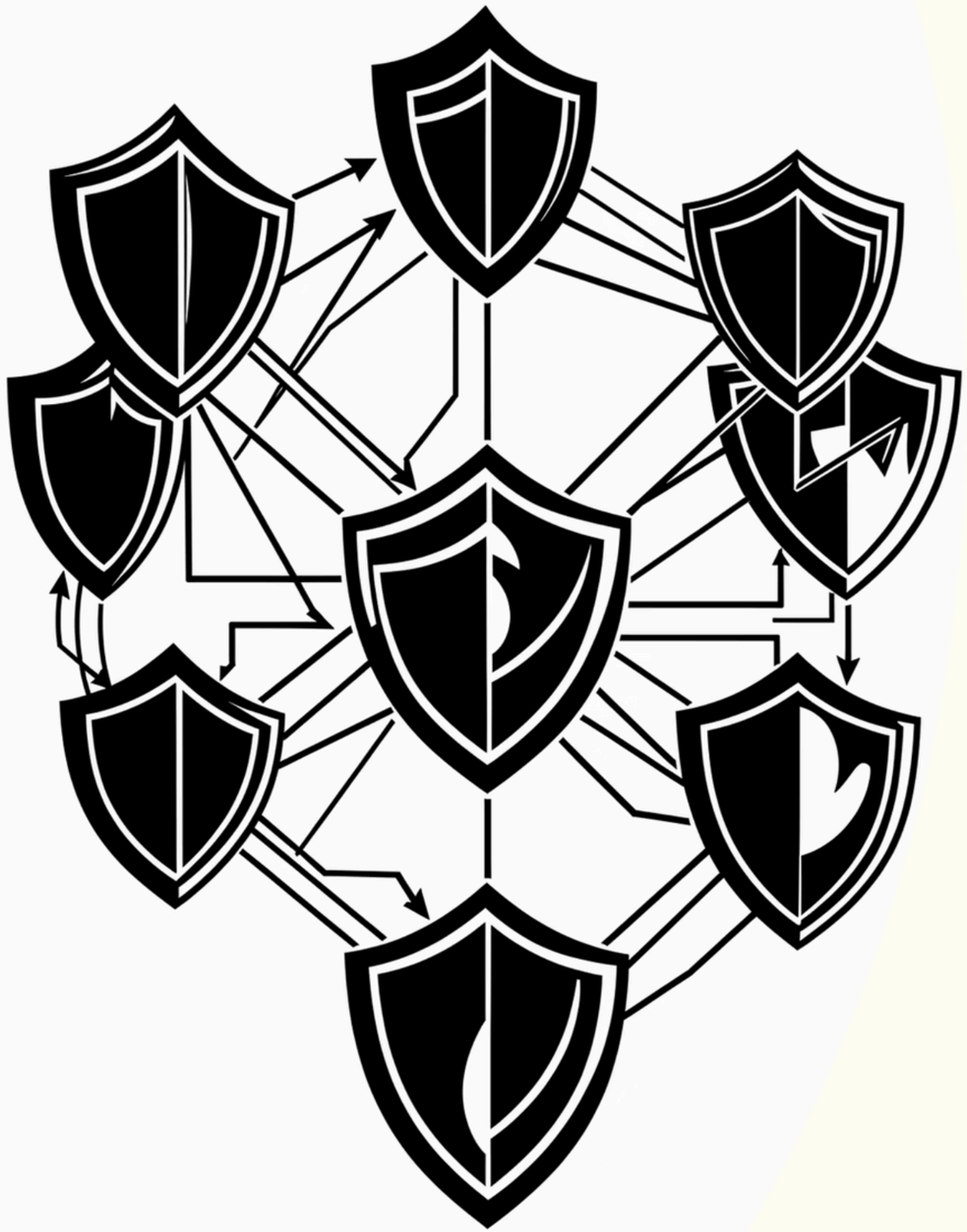

127.0.0.1:5500/admin.html
Admin Dashboard
Welcome, Admin (Anushaa)
Create Employee Account
Username
Password
Email
Create Employee
Locked User Accounts
Username
Email
Role
Action
No locked users
Logout


Admin Dashboard
127.0.0.1:5500/admin.html
Admin Dashboard
Welcome, Admin (Anushaa)
Create Employee Account
Username
Password
Email
Create Employee
Employee account created successfully
Locked User Accounts
Username
Email
Role
Action
No locked users
Logout


Employee Dashboard
127.0.0.1:5500/employee.html
Employee Dashboard
Welcome Employee
Logout

REFERENCES

- SPRING BOOT DOCUMENTATION
- SPRING SECURITY OFFICIAL DOCS
- JWT.IO
- INFOSYS TRAINING MATERIALS



Conclusion:

- **Enhanced Security:** Login-based authentication significantly improves system security.
- **Restricted Access:** Role control effectively limits user access to designated areas.
- **Scalable Foundation:** The modular design allows for easy future expansion and integration of backend services.

Improved Security

Restricted Access

Scalable System

THANK YOU