IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, May 2025
Impact Factor: 7.67

User Authentication System in Angular

Ass. Prof. Shubhangi Kshirsagar and Kurandale Avinash
Department of Computer Engineering
D. Y. Patil College of Engineering and Innovation, Pune, MH, India

Abstract: *This paper presents a secure and scalable User Authentication System developed using Angular, a modern front-end framework. The system is designed to manage user sign-up, login, password encryption, session handling, and role-based access control. It provides a structured and modular approach to authentication for web applications. The solution improves both security and user experience while demonstrating the capabilities of Angular in handling secure access systems for modern web applications*

Keywords: Angular, Authentication, Login System, Web Security, Role-Based Access

I. INTRODUCTION

With the increasing number of web-based applications, ensuring secure access and authentication is crucial. Unauthorized access can result in data breaches, identity theft, and serious business risks. A robust authentication system prevents these risks by verifying user identity before granting access. This project implements a User Authentication System using Angular to handle login, registration, encrypted password storage, and role-based access for users and administrators. The frontend is built with Angular, while integration with backend APIs enables dynamic and secure data management.

II. LITERATURE REVIEW

YEAR	AUTHOR(S)	DESCRIPTION
2025	Juliana George	Discusses RBAC implementation using Spring Security and AngularJS, focusing on real-world security needs and access restrictions.
2025	Kornienko et al.	Focuses on the security of authentication workflows and session handling in Angular SPAs.
2022	Marinko Spasojević	Explains how Angular route guards and backend identity frameworks can enable role-based access control.
2023	Pavel Salauyou	Demonstrates the implementation of roles and permission services in modern Angular applications.
2023	Stream2085	Offers a practical guide to securing Angular applications using RBAC design principles.

III. PROPOSED SYSTEM

The User Authentication System includes the following core features:

User Registration and Login

A secure UI for users to create accounts and log in using a combination of email and password.

Password Hashing:

All passwords are encrypted before storage using hashing algorithms to enhance data security

Session Handling:

Sessions are tracked in browser memory and cleared on logout or timeout.

Role-Based Access Control (RBAC)

Users are assigned roles (e.g. User) that restrict or allow access to various modules.

DOI: 10.48175/568

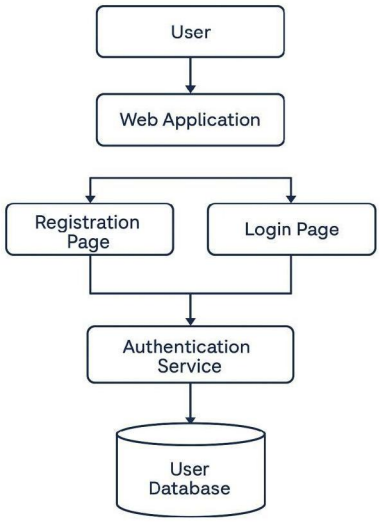
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, May 2025
Impact Factor: 7.67

Angular Routing and Guards:
Access to different application routes is protected by guards that check user authentication status.

Integration with Organic Certification Support:
Offering resources for organic certification and connecting farmers with support organizations.

User-Friendly Interface
Built using Angular Material, the frontend is responsive and accessible on multiple devices.

IV. WORKING



Proposed ahitecture System

V. EXPERIMENTAL RESULT

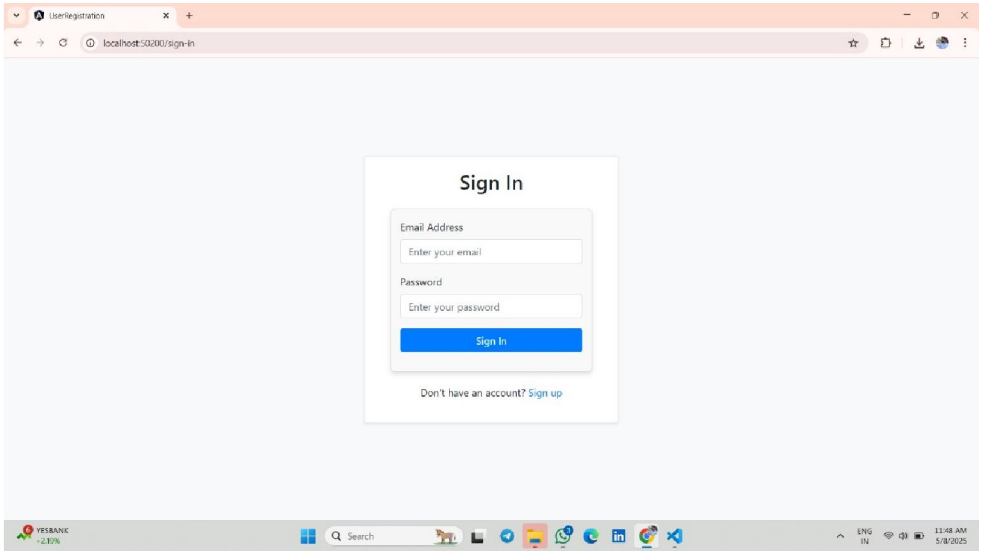


Fig. 1. Login Page

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, May 2025
Impact Factor: 7.67

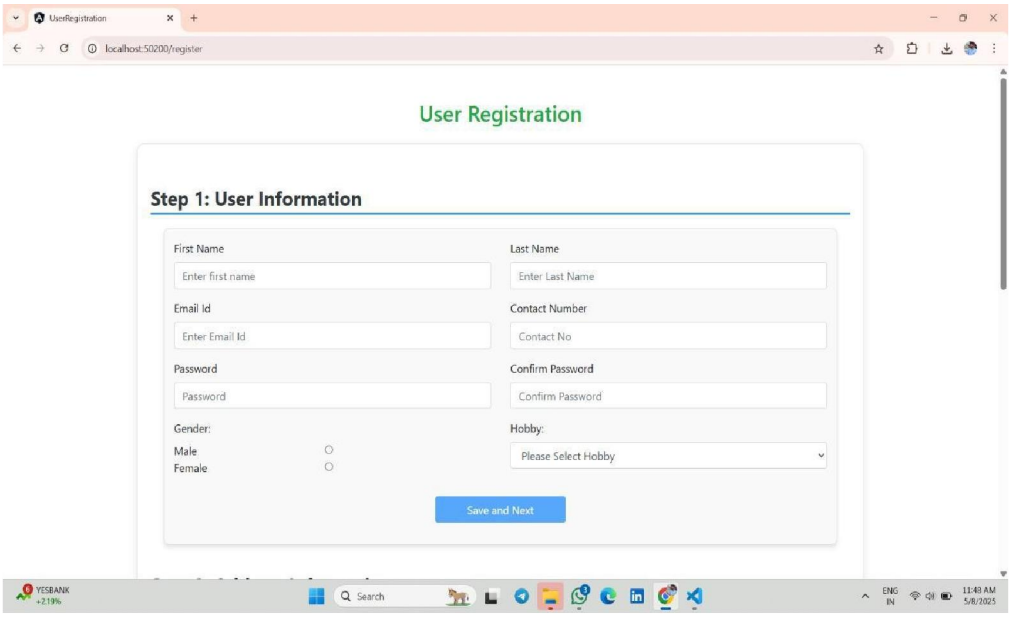


Fig. 2. Sign Up Page

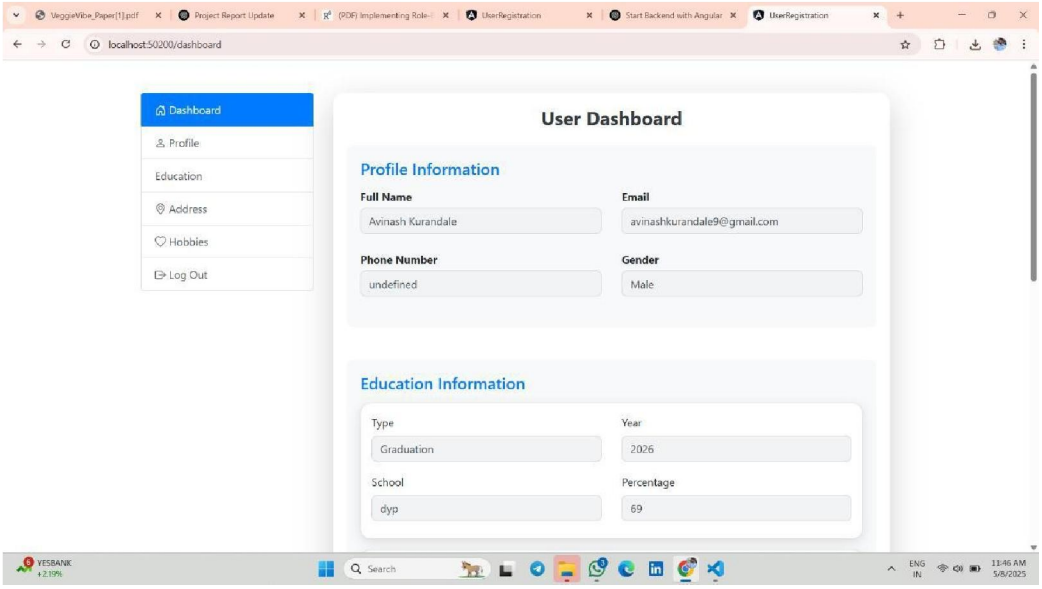


Fig. 3. Homepage of Portal

VI. CONCLUSION

The Angular-based User Authentication System provides a reliable way to manage secure user access. Its role- based mechanism helps enforce proper authorization policies in a scalable and maintainable way. It can be easily integrated with various backend services and further extended to include features like password recovery and multi-factor authentication..

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, May 2025
Impact Factor: 7.67

VII. ACKNOWLEDGMENT

I would like to express my heartfelt gratitude to Ass.Prof. Shubhangi Kshirsagar for her invaluable guidance throughout this project. I also thank the faculty of the Department of Computer Engineering, D. Y. Patil College of Engineering and Innovation, for their continuous encouragement. Special thanks to my family and peers for their motivation and support.

REFERENCES

[1]. George, J. (2025). Implementing Role-Based Access Control (RBAC) in Java and AngularJS Web Applications. ResearchGate.
[2]. Kornienko et al. (2025). Implementing Authentication and Session Management in an AngularJS Single-Page Application. EJAET Journal.
[3]. Spasojević, M. (2022). Angular Role-Based Authorization with ASP.NET Core Identity. CodeMaze.
[4]. Salauyou , P. (2023). Role-Based Access Control in Angular 16 Applications. Medium.
[5]. Stream2085. (2023). Role-Based Access Control (RBAC) in Angular Applications. Medium.
[6]. Danielecki, M. (2019). Security First Approach in Development of Single-Page Application Using Angular. University of Twente.
[7]. Arias, D. (2022). The Complete Guide to Angular User Authentication with Auth0. Auth0 Blog.
[8]. Zanetti, E. (2024). Enhancing Cybersecurity in Angular Applications: Best Practices. Medium.
[9]. Permit.io Team. (2024). How to Implement Role-Based Access Control (RBAC) in Angular. Permit.io Blog.
[10]. Descope Team. (2024). Add Authentication and RBAC to an Angular App. Descope Blog.
[11]. Ethelbert, O., Moghaddam, F.F., Wieder, P., & Yahyapour, R. (2017). A JSON Token-Based Authentication and Access Management Schema for Cloud SaaS Applications. arXiv preprint arXiv:1710.08281.
[12]. Rahman, M.U. (2020). Scalable Role-based Access Control Using The EOS Blockchain. arXiv preprint arXiv:2007.02163.
[13]. Zhang, G., Zhang, M., & Fan, X. (2020). Improvements Based on JWT and RBAC for Spring Security Framework. In Security and Privacy in Digital Economy (pp. 113-123). Springer, Singapore.
[14]. Crampton, J., & Sellwood, J. (2014). Path Conditions and Principal Matching: A New Approach to Access Control. arXiv preprint arXiv:1406.4988.
[15]. Ben Ghorbel-Talbi, M., Cuppens, F., Cuppens-Boulahia, N., & Bouhoula, A. (2010). Managing Delegation in Access Control Models. arXiv preprint arXiv:1012.2720.
[16]. Soni, K., & Kumar, S. (2018). Comparison of Various Role Based Access Control Scheme. International Journal of Engineering Research & Technology (IJERT), 7(5).
[17]. Rostami, G. (2024). Role-based Access Control (RBAC) Authorization in Kubernetes. Journal of ICT Standardization, 11(3), 32.