ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 2
www.ijisea.org

User Authentication System

CH. Lakshmi Narayana[1],Sk. Ayesha Yasmeen[2],Sk. Jasmine[3],K. Sasi Kumar[4],R.Dhanush[5]
Assistant Professor[1],UG Student[2,3,4,5]
Computer Science and Engineering
Amrita Sai Institute of Science & Technology
Paritala, Andhra Pradesh , India

ABSTRACT

A User Authentication System is a crucial component in securing digital platforms, ensuring that only authorized individuals gain access to resources and sensitive information. It verifies the identity of users and grants access based on predefined permissions. The core functions of such a system include user registration, login, password management, and role- based access control (RBAC). Modern authentication systems also incorporate advanced features like multi-factor authentication (MFA), OAuth for third-party login, and password less options, enhancing both user experience and security.

Key words: User Authentication, Access Control, Role-Based Access Control (RBAC)

Abbreviations: Role Based Access Control

I.INTRODUCTION

This project is focused on developing a comprehensive user authentication system designed to enhance security and user experience. The system incorporates essential features such as email verification and password reset functionality, utilizing a secure 6-digit OTP sent directly to the user's registered email address. The project is structured into two core components: backend and frontend development. The backend involves setting up a robust server to handle all authentication-related requests. Using the MERN stack—comprising MongoDB, Express, React, and Node.js—the backend will include APIs to manage user registration, login, email verification, and password reset operations. For authentication, JWT (JsonWebToken) will be implemented, ensuring secure communication between the client and the server by providing token-based authentication. The database will be designed to securely store user credentials and manage OTP-related information efficiently.

II.RELATED WORK

The primary objective of this project is to develop a secure and user-friendly authentication system with modern features, ensuring robust protection of user data and seamless usability. The specific objectives include:

1. Backend Development: Design and implement a backend server using the MERN stack (MongoDB, Express, React, and Node.js).

    - Create APIs to handle user authentication processes, including registration, login, email verification, and password reset.
    - Implement JWT(JsonWebToken) for secure token-based user authentication.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 2
www.ijisea.org

2. Email Verification and OTP System: Generate and send secure 6-digit OTPs to user email addresses for verification and password reset purposes.

    - Verify OTPs and ensure their secure storage and expiration to prevent misuse.

3. Frontend Development: Build a responsive and user-friendly client application using React and Tailwind CSS.

    - Develop interactive forms for user registration, login, and password reset with OTP input functionality.
    - Integrate the frontend with backend APIs for seamless operation and communication.
    -

Features of Modern Authentication Systems Modern authentication systems incorporate advanced features to enhance security and usability

- Email Verification: Validates user identity by confirming their email address through OTPs.
- Password Reset Mechanism: Allows users to reset their passwords securely via email or SMS.
- Session Management: Uses tokens (e.g., JWT) to maintain user sessions without compromising security.
- Scalability: Designed to support a growing user base without performance issues.

III.METHODOLOGY

1. MongoDB

- **Type:** NoSQL Database
- **Role:**
    - Stores user-related data such as emails, passwords, OTPs, and JWT tokens
    - Offers high scalability and performance for dynamic data
    - Provides flexibility with a schema-less document structure

2. Express.js

- **Type:** Web Application Framework for Node.js
- **Role:**
    - Handles API routes for user authentication (e.g., login, registration, password reset)
    - Connects to MongoDB to fetch and store user data
    - Provides middleware for authentication and security

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 2
www.ijisea.org

3. React.js

- **Type:** JavaScript Library for Building User Interfaces
- **Role:**
    - Develops interactive UI components such as login, registration, and password reset forms
    - Ensures a responsive and seamless user experience

IV.RESULTS

The main Test code running

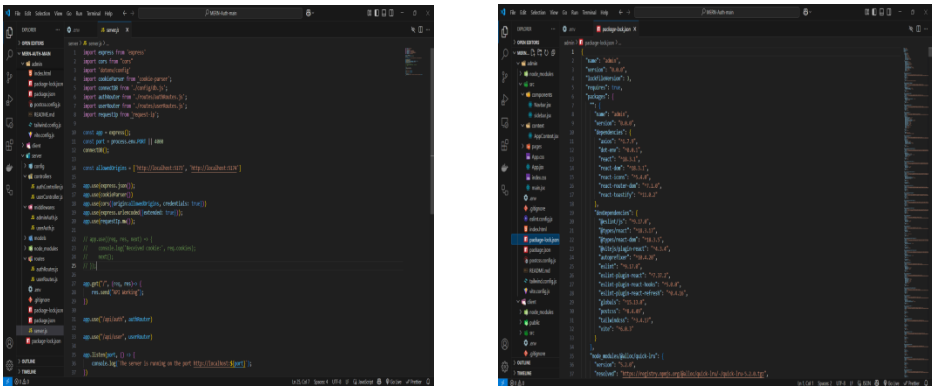

Figure 1 : Shows the main test

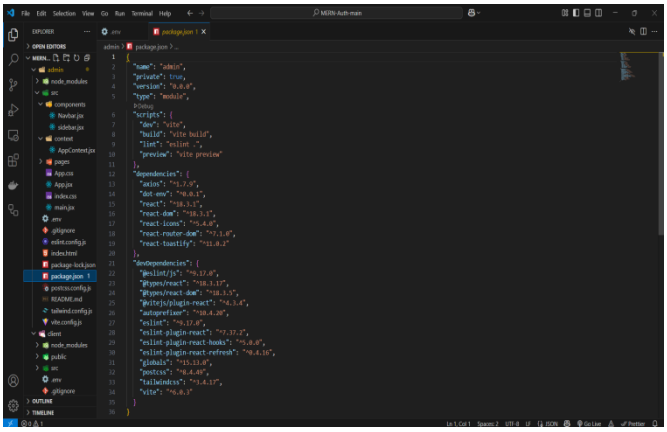

Figure 2 : Shows the Libraries& Dependencies

Output Test Results

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 2
www.ijisea.org

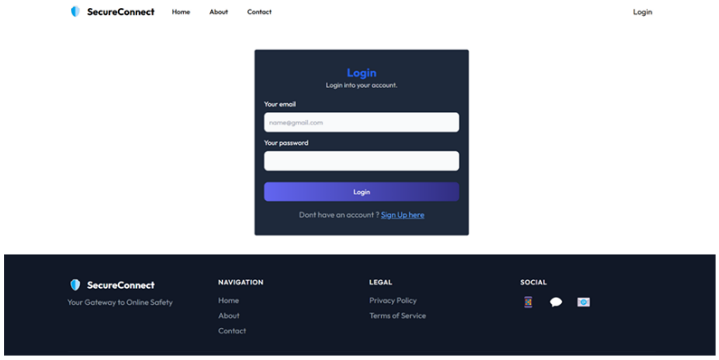

Figure 3 : Shows Login page

Figure 4 : Menu Page

V.CONCLUSIONS

The User Authentication System successfully implements a secure and efficient method for user verification and password management. By integrating modern technologies like the MERN stack and employing features such as JWT-based authentication and OTP verification, the system ensures robust security and a seamless user experience. The combination of backend API development and frontend UI design has resulted in a fully functional application that meets contemporary authentication needs. This project demonstrates the importance of secure practices in user authentication, laying a strong foundation for further enhancements and scalability in real-world applications.

ACKNOWLEDGEMENT(S):

We wish to express our sincere and profound gratitude to our guide Mr.CH. LAKSHMINARAYANA, for his significant suggestions, encouragement, everlasting patience, and keen interest in discussions that have benefited us to an extent that cannot be spanned by words.

We express our profound gratitude to Dr. P. CHIRANJEEVI M.Tech, Ph.D., Professor and Head of the Department for his indispensable encouragement and salient guidelines and suggestions throughout the work.

We thank Dr. M. SASIDHAR, Principal of Amrita Sai Institute of Science and Technology, for providing an excellent academic environment in the college.

We are very pleased to convey our gratitude to the teaching and non-teaching staff who directly or indirectly supported the completion of this project.

Our acknowledgments conclude with expressing our gratefulness to our parents for their great support. Project Associates

REFERENCES:

[1] N.K. Ratha, J.H. Connell, and R.M. Bolle, “Enhancing Security and Privacy in Biometrics-Based Authentication Systems,” *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[2] *Security Analysis and Implementation of JUIT-IBA System using Kerberos Protocol*, Proceedings of the 7th IEEE International Conference on Computer and Information Science, Oregon, USA, pp. 575–580, 2008.

[3] R.E. Newman, P. Harsh, and P. Jayaraman, “Security Analysis of and Proposal for Image-Based Authentication,” 2005.

[4] S. Chiasson, R. Biddle, and P.C. van Oorschot, “A Second Look at the Usability of Click-Based Graphical Passwords,” *ACM Symposium on Usable Privacy and Security (SOUPS)*, 2007.

[5] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, “A New Graphical Password Scheme Resistant to Shoulder-Surfing.”

[6] Z. Zheng, X. Liu, L. Yin, and Z. Liu, “A Hybrid Password Authentication Scheme Based on Shape and Text,” *Journal of Computers*, vol. 5, no. 5, pp. –, May 2010.