IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15173

Multi-Factor Authentication System

Ganesh[1], Rajeshwari N[2]

Department of MCA, BIT, K.R. Road, V.V. Pura, Bangalore, India[1,2]

Abstract: This paper presents a web-based Multi-Factor Authentication System designed to improve security and prevent unauthorized access to web applications. The system verifies user identity using multiple authentication layers such as password-based login, email-based One-Time Password (OTP) verification, and face recognition. By combining these security mechanisms, the system reduces the risks associated with traditional single-factor authentication methods.

The proposed system integrates secure authentication logic with a modern web application to provide real-time verification at each stage of the login process.In addition to authentication, the platform includes features such as user registration, login activity tracking, session management, and administrative monitoring, making it suitable for real-world security applications. This approach demonstrates how multi-factor authentication techniques can deliver a reliable,scalable, and user-friendly solution for strengthening web application security.

Keywords: Multi-Factor Authentication, Web Security, One-Time Password, Face Recognition,Session Management, Secure Web Application.

I. INTRODUCTION

With the rapid growth of web-based applications and online services, ensuring secure user authentication has become a critical requirement. Many applications still rely on traditional username and password–based authentication methods, which are highly vulnerable to security threats such as password theft, brute-force attacks, phishing, and unauthorized access. As cyber threats continue to increase, there is a strong need for more robust and intelligent authentication mechanisms that can protect user data and system resources effectively. This project introduces a web-based Multi-Factor Authentication System designed to enhance login security by incorporating multiple verification layers. Instead of depending solely on passwords, the proposed system combines password verification, email-based One-Time Password (OTP) validation, and face recognition to strengthen user identity verification. By integrating these authentication factors into a single platform, the system reduces security risks while maintaining usability and ease of access. The solution focuses on real-time verification, user awareness, and secure session handling, making it suitable for modern web applications.

1.1 Project Description

This project implements a Multi-Factor Authentication System that verifies users through a step-by-step authentication process. Initially, users authenticate using their registered email and password. Upon successful verification, an email-based OTP is generated and sent to the user for second-level authentication. Finally, face recognition is used as an additional biometric verification step before granting access to protected resources. The system is developed as a web application using modern technologies. The frontend provides a user-friendly interface for registration, login, OTP verification, and face authentication, while the backend handles authentication logic, session management, and database operations. User activity and session details are securely stored, allowing both users and administrators to monitor authentication events. Overall, the project delivers a secure, scalable, and practical solution for protecting web applications from unauthorized access.

1.2 Motivation

The motivation for this project arises from the increasing number of security breaches caused by weak authentication mechanisms. Many users reuse passwords across multiple platforms, making single-factor authentication unreliable. There is a strong need for a security solution that can provide higher protection without significantly increasing user complexity. By implementing multiple authentication factors, the proposed system ensures that even if one verification method is compromised, unauthorized access can still be prevented. The use of email OTP and face recognition adds an extra layer of trust and identity assurance. Providing this functionality through a web-based platform makes the system accessible and practical for real-world use. The project aims to promote secure authentication practices and contribute to safer digital environments.

DOI: 10.17148/IJARCCE.2026.15173

II. RELATED WORK

Paper [1] studies traditional authentication systems that rely on username and password–based login mechanisms. These systems are simple to implement and widely used; however, they are highly vulnerable to security threats such as password guessing, brute-force attacks, and credential theft, making them unsuitable for secure web applications.

Paper [2] focuses on two-factor authentication methods that combine passwords with One-Time Password (OTP) verification. While OTP-based systems improve security compared to single-factor authentication, the study highlights issues such as delayed OTP delivery and the lack of additional verification layers to handle advanced attack scenarios.

Paper [3] explores token-based and session-based authentication techniques for securing web applications. These methods enhance access control by managing user sessions effectively, but they often fail to verify user identity beyond the initial login, leaving systems exposed if session data is compromised.

Paper [4] investigates the use of biometric authentication methods such as fingerprint and facial recognition for user verification. The study demonstrates improved security and identity assurance; however, it points out challenges related to hardware dependency, environmental conditions, and system integration complexity.

Paper [5] reviews recent advancements in multi-factor authentication systems and emphasizes the importance of combining multiple authentication techniques within a single platform. The survey concludes that integrating password verification, OTP validation, and biometric authentication in a web-based system can significantly enhance security, usability, and real-world applicabilit

III. METHODOLOGY

A. System Environment

The system environment is designed to evaluate the Multi-Factor Authentication System under realistic and practical usage conditions. The application operates in a web-based environment where users act as individual clients accessing the system through standard web browsers. Users interact with the system by registering, logging in, verifying their identity through multiple authentication steps, and accessing protected resources in a secure manner.

The backend environment consists of a server-based application that manages user authentication, credential validation, OTP generation, face recognition processing, and session management. After a user enters login credentials, the backend verifies the information and initiates email-based OTP verification followed by face recognition for identity confirmation. All authentication processes are handled securely within the server without exposing sensitive user data to external systems.

A database is used to store user registration details, authentication status, session information, and activity logs in a structured format. This enables secure data storage and allows administrators to monitor login activities and system usage. The system environment simulates a real-world security scenario where multiple users can access the application simultaneously while maintaining data privacy, reliability, and access control. The setup ensures smooth performance, secure authentication handling, and scalability for future enhancements such as additional biometric methods or deployment on cloud platforms.

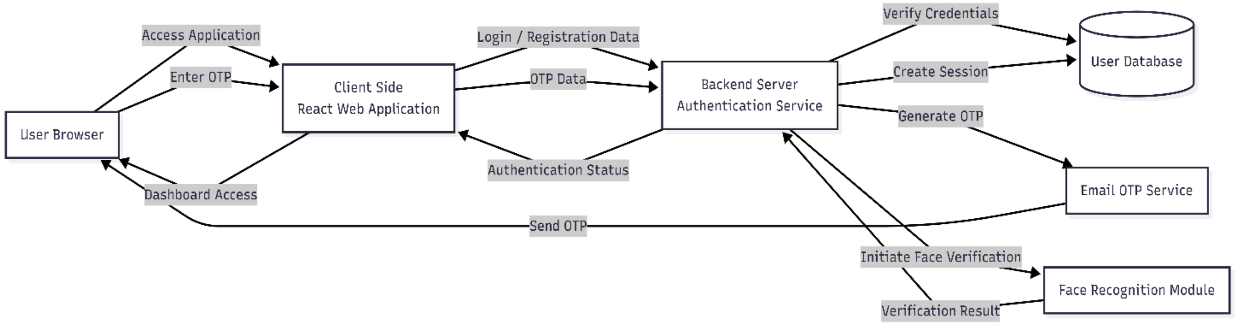


Fig.1.Flowchart of methodology

DOI: 10.17148/IJARCCE.2026.15173

B. Authentication Architecture

- Client-Side Processing:
  In the Multi-Factor Authentication System, user details such as email address and password are collected through a secure web-based interface. The client-side application performs basic validation to ensure that all required fields are filled correctly and follow the expected format before sending the data to the backend server. This initial validation helps reduce invalid requests and improves user experience.

- Authentication Execution:
  The backend authentication module verifies the validated credentials against stored user records in the database. After successful password verification, the system generates a One-Time Password (OTP) and sends it to the user's registered email address. Upon successful OTP validation, a face recognition module is triggered to confirm the user's identity before granting access to the system.

C. Adaptive Security Mechanism

The authentication mechanism is designed to be adaptive and extensible. As security requirements evolve, additional authentication factors or improved biometric verification techniques can be integrated into the system. This adaptive design ensures that the system remains effective against emerging security threats while maintaining consistent authentication accuracy and system reliability.

D. Implementation Flow

1. The user accesses the Multi-Factor Authentication System through a web application.
2. The user registers or logs in using a valid email address and password.
3. The system validates the entered credentials on the backend.
4. An email-based One-Time Password (OTP) is generated and sent to the user.
5. The user enters the received OTP for verification.
6. After successful OTP verification, face recognition is initiated.
7. The system verifies the facial data with stored records.
8. A secure session is created for the authenticated user.
9. The user is redirected to the dashboard with access to protected resources.

E. Hardware and Software Requirements

- Hardware:
  A standard computer system with a minimum of 4 GB RAM is sufficient to run the application. No specialized hardware is required for end users, as the authentication process is lightweight and optimized for web deployment. A basic webcam is required only for face recognition.

- Software:
  The system uses modern and open-source technologies including Python for backend development, Node.js and Express.js for authentication services, React.js for frontend development, SQLite for database management, and HTML, CSS, and JavaScript for user interface design.

IV. SIMULATION AND EVALUATION FRAMEWORK

This section describes the system design, execution flow, and evaluation strategy adopted for the Multi-Factor Authentication System. The framework focuses on validating the effectiveness of the authentication mechanisms and the overall performance of the web application under realistic usage scenarios. The system is implemented using modern web technologies with a secure backend architecture that supports password verification, email-based OTP validation, and face recognition for real-time authentication.

A. System Architecture and Workflow

The overall architecture is designed to provide secure and reliable user authentication while maintaining usability and scalability. The key components of the system are described below:

DOI: 10.17148/IJARCCE.2026.15173

- **User Interaction Layer:** Users interact with the system through a web-based interface where they can register, log in, verify OTPs, and complete face recognition. All interactions are designed to be simple and intuitive for users with varying technical backgrounds.

- **Application Processing Layer**: The backend processes user requests by validating credentials, generating and verifying OTPs, managing face recognition workflows, and handling secure session creation. This layer also manages user activity logs and authentication status storage.

- **Authentication and Security Module:** This module combines password verification, OTP validation, and biometric face recognition to ensure multi-layer security. Each authentication step is verified before allowing access to protected resources.

B. Simulation Setup

The simulation environment is designed to represent real-world usage of the authentication system by multiple users with different access scenarios.

- **User Authentication Simulation:** Multiple test cases are created to simulate valid and invalid login attempts, OTP verification failures, face recognition success and failure scenarios, and session expiration conditions.

- **Scenario Testing**: Various scenarios such as repeated login attempts, incorrect OTP entry, unauthorized access attempts, and logout operations are tested to ensure system robustness and reliability.

C. Authentication and Evaluation Process

During simulation, user login requests are processed through the authentication pipeline. Credentials are verified first, followed by OTP validation and face recognition. Upon successful authentication, a secure session is created and stored in the database. Authentication results and session details are logged and displayed appropriately to users and administrators. This process is repeated across multiple test cases to evaluate consistency, correctness, and response time.

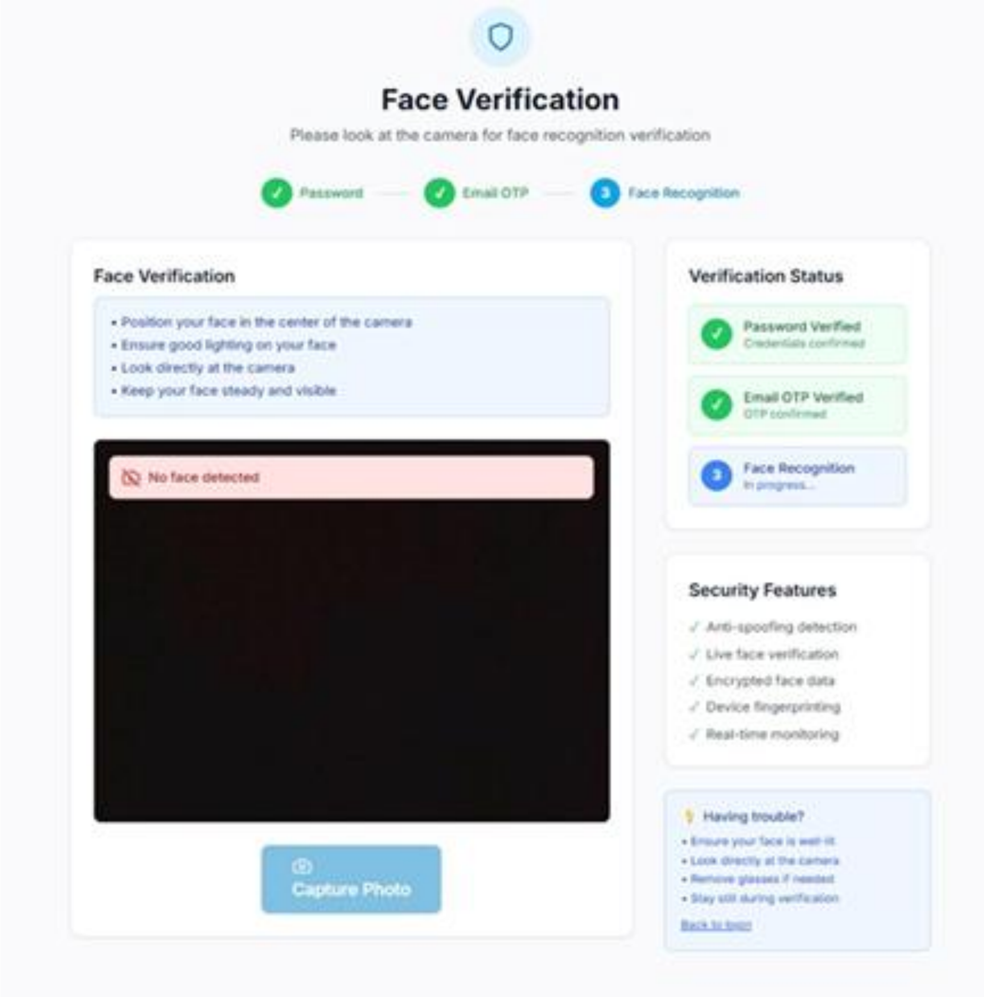
D. Results and Observations

- **Authentication Accuracy:** The system consistently allowed access only to valid users who successfully completed all authentication steps, effectively preventing unauthorized access.

- **System Reliability:** The interaction between the frontend, backend services, authentication modules, and database was smooth, with minimal response delay and stable performance during simulations.

- **Usability and Practicality:** The evaluation confirmed that the system is easy to use, even for non-technical users, while providing strong security. The authentication flow proved suitable for real-world web application deployment.

DOI: 10.17148/IJARCCE.2026.15173



Face Verification

Please look at the camera for face recognition verification

✓ Password — ✓ Email OTP — 3 Face Recognition

Face Verification

- Position your face in the center of the camera
- Ensure good lighting on your face
- Look directly at the camera
- Keep your face steady and visible

No face detected

Verification Status

✓ Password Verified
Credentials confirmed

✓ Email OTP Verified
OTP confirmed

3 Face Recognition
In progress...

Security Features

✓ Anti-spoofing detection
✓ Live face verification
✓ Encrypted face data
✓ Device fingerprinting
✓ Real-time monitoring

Having trouble?

- Ensure your face is well-lit
- Look directly at the camera
- Remove glasses if needed
- Stay still during verification

Fig. 2. Face Verification Page

Model Performance and Adaptability Analysis

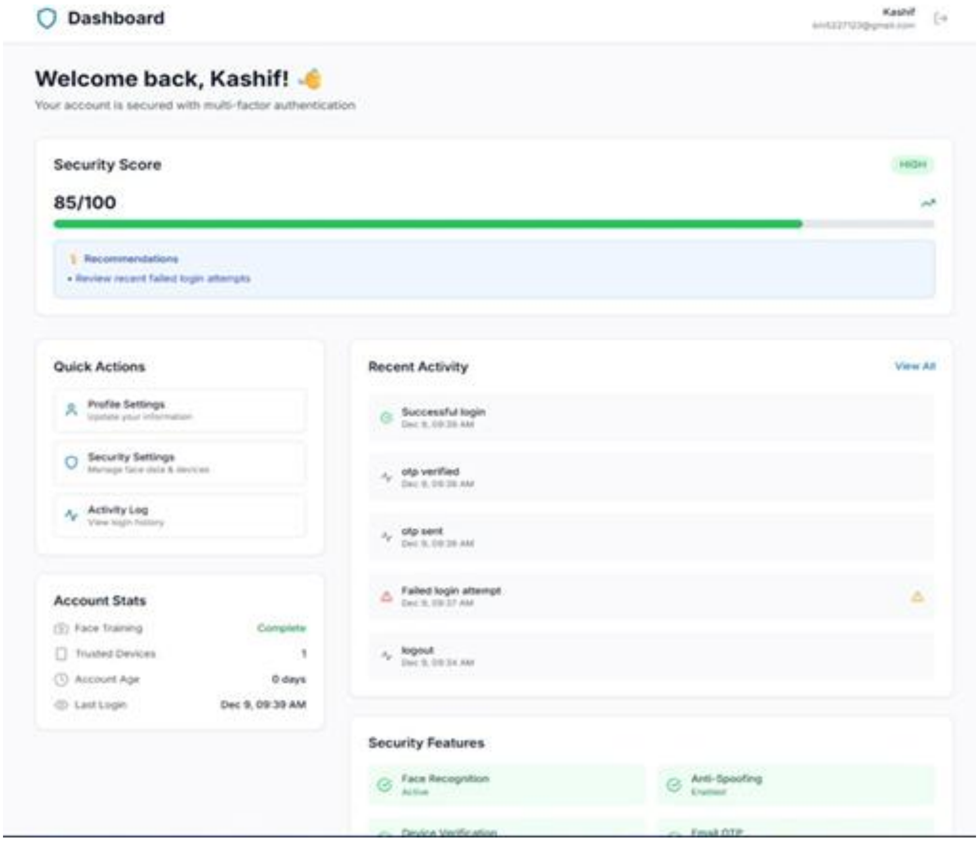
- Authentication Stability and Consistency: The multi-factor authentication system demonstrated stable and consistent performance during testing and simulation. Across repeated login attempts and verification cycles, the system reliably authenticated valid users while blocking unauthorized access, indicating dependable operation of all authentication layers.

- Security Effectiveness Improvement: The authentication accuracy improved through the combination of password verification, email-based OTP validation, and face recognition. This layered approach significantly reduced the chances of unauthorized access compared to single-factor authentication methods, confirming the effectiveness of the selected security mechanisms.

- Handling of Diverse User Scenarios: The system effectively handled different user behaviors, including valid logins, incorrect password attempts, invalid OTP entries, and face recognition failures. It adapted well to varied authentication scenarios while maintaining correct access control and system stability.

- Result Transparency and Validation: Authentication outcomes were clearly communicated to users through success or failure messages at each stage. Session status and login feedback enhanced user awareness and trust, ensuring that authentication decisions were understandable and verifiable rather than hidden system processes.

DOI: 10.17148/IJARCCE.2026.15173



Dashboard

Kashif
[illegible]

Welcome back, Kashif! 👋

Your account is secured with multi-factor authentication

Security Score HIGH

85/100

Recommendations
- Review recent failed login attempts

Quick Actions

Profile Settings
Update your information

Security Settings
Manage face data & devices

Activity Log
View login history

Account Stats

Face Training	Complete
Trusted Devices	1
Account Age	0 days
Last Login	Dec 9, 09:39 AM

Recent Activity View All

Successful login
Dec 9, 09:39 AM

otp verified
Dec 9, 09:38 AM

otp sent
Dec 9, 09:38 AM

Failed login attempt
Dec 9, 09:37 AM

logout
Dec 9, 09:34 AM

Security Features

Face Recognition
Active

Anti-Spoofing
Enabled

Device Verification

Email OTP

Fig. 3. Dashboard Page

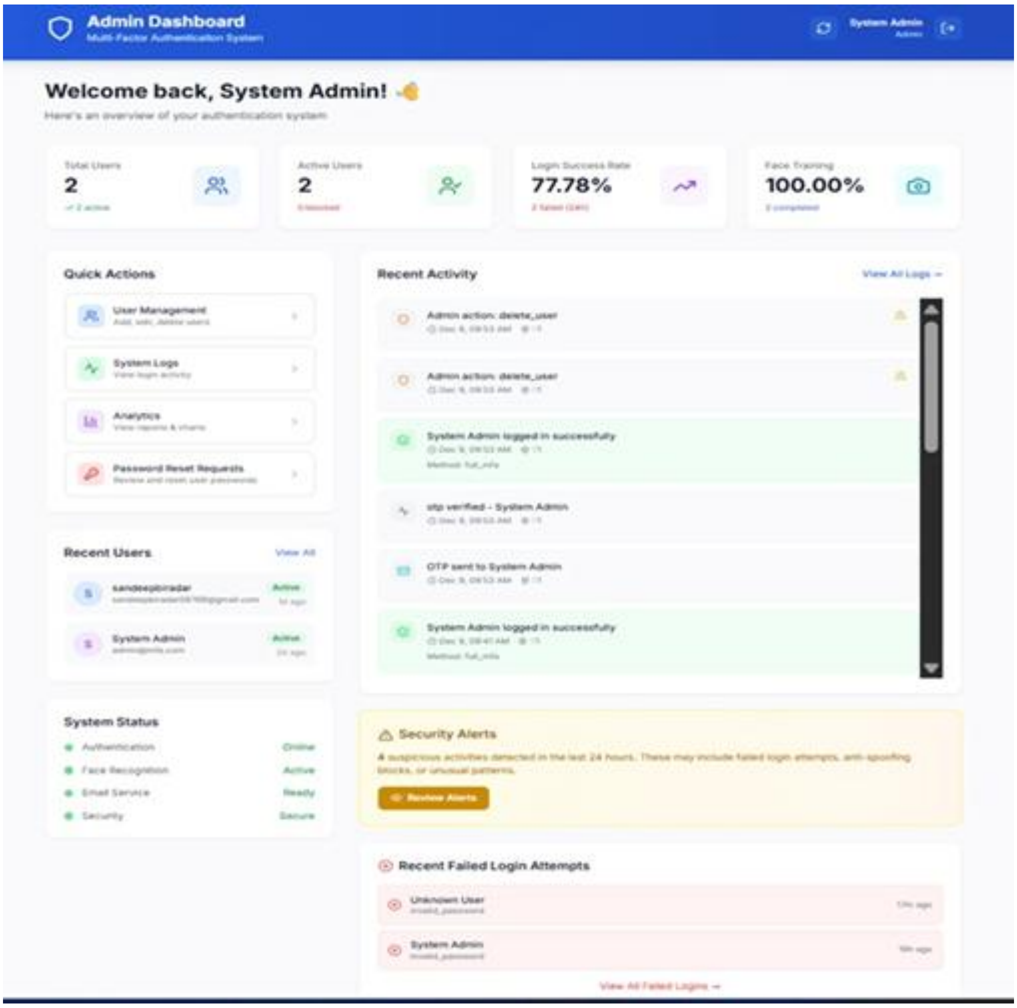
Impact on System Efficiency:

- **Low Computational Overhead**: The Multi-Factor Authentication System operates efficiently with minimal computational load. Since authentication processes such as password verification, OTP validation, and face recognition are optimized, user verification is completed quickly without slowing down the system, even during multiple concurrent login attempts.

- **Efficient Authentication Processing:** Only essential authentication data such as credentials, OTP values, and facial features are processed during verification. This lightweight handling reduces unnecessary computation and ensures fast response times across different devices and browsers.

- **Secure and Controlled Data Flow:** User authentication data is transmitted securely within the system and stored only when required for session management and activity logging. This controlled data flow enhances system reliability while maintaining user privacy and data protection.

- **Scalable Web-Based Architecture:** The modular backend design allows the authentication system to scale easily as the number of users increases. The architecture supports higher user traffic without significant impact on authentication accuracy, response time, or system stability.authentication accuracy, response time, or system stability.



Admin action: delete_user

Admin action: delete_user

System Admin logged in successfully

otp verified - System Admin

OTP sent to System Admin

System Admin logged in successfully

4 suspicious activities detected in the last 24 hours. These may include failed login attempts, anti-spoofing blocks, or unusual patterns.

Fig. 4. Admin Dashboard Page

V. RESULTS AND DISCUSSION

The experimental evaluation of the Multi-Factor Authentication System demonstrates the effectiveness of using layered authentication techniques to enhance web application security. The system performed reliably during testing by allowing access only to users who successfully completed all authentication stages, including password verification, email-based OTP validation, and face recognition. This confirms that multi-factor authentication provides stronger protection compared to traditional single-factor login systems.

By integrating the authentication logic within a modern web-based application, the system delivers real-time verification with minimal response delay. Each authentication step provides clear feedback to the user, improving transparency and user understanding of the login process. The storage of authentication logs and session details further enhances reliability by enabling monitoring and review of login activities.

The evaluation also shows that the system operates efficiently with low computational overhead, as only essential authentication data is processed during verification. Secure handling of user credentials, OTPs, and biometric data ensures privacy and prevents unauthorized data access. Overall, the results indicate that the Multi-Factor Authentication System is secure, scalable, and user-friendly, making it suitable for real-world deployment in web applications that require enhanced access control and data protection.

VI. CONCLUSION

This paper presented a web-based Multi-Factor Authentication System aimed at enhancing application security by verifying user identity through multiple authentication layers. By integrating password-based login, email-based One-

DOI: 10.17148/IJARCCE.2026.15173

Time Password (OTP) verification, and face recognition within a unified web platform, the system provides a robust and reliable solution to prevent unauthorized access and improve overall authentication security.

The experimental evaluation demonstrated consistent authentication accuracy, efficient system performance, and reliable handling of different user authentication scenarios without introducing significant computational overhead. The inclusion of clear authentication feedback, secure session management, activity logging, and administrative monitoring improves transparency and practical usability. Overall, the proposed system proves to be a secure, scalable, and user-friendly solution for strengthening web application security, supporting safer digital access and promoting the adoption of advanced authentication practices in real-world environments.

VI. FUTURE WORK

The future work of this project focuses on further strengthening the Multi-Factor Authentication System by incorporating additional security mechanisms and advanced authentication techniques. Future enhancements may include the integration of mobile-based authentication methods such as push notifications and SMS-based OTPs to provide alternative verification options and improve system flexibility.

The system can also be extended by integrating more advanced biometric authentication techniques such as fingerprint recognition or behavioral biometrics to increase security accuracy. Deploying the system on cloud infrastructure can improve scalability and support a larger number of concurrent users. Additionally, developing a dedicated mobile application will enhance accessibility and user convenience. These improvements aim to make the authentication system more robust, scalable, and suitable for high-security real-world applications.

REFERENCES

[1]. Das, A., and Mukhopadhyay, D., "Secure Authentication Mechanisms for Web Applications: A Survey," Journal of Information Security, vol. 12, no. 2, pp. 85–96, 2021. https://www.scirp.org/journal/paperinformation.aspx?paperid=109123

[2]. Alotaibi, S., et al., "Multi-Factor Authentication Techniques: A Review of Security and Usability," International Journal of Computer Networks & Communications, vol. 13, no. 4, pp. 1–15, 2021. https://aircconline.com/ijcnc/V13N4/13421ijcnc01.pdf

[3]. Bonneau, J., et al., "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," IEEE Symposium on Security and Privacy, pp. 553–567, 2012. https://ieeexplore.ieee.org/document/6234436

[4]. Ometov, A., et al., "Multi-Factor Authentication: A Survey," Cryptography, vol. 2, no. 1, pp. 1–22, 2018. https://www.mdpi.com/2410-387X/2/1/1

[5]. Jain, A. K., Ross, A., and Nandakumar, K., "Introduction to Biometrics," Springer, 2011. https://link.springer.com/book/10.1007/978-0-387-77326-1

[6]. Viola, P., and Jones, M., "Rapid Object Detection Using a Boosted Cascade of Simple Features," IEEE Conference on Computer Vision and Pattern Recognition, 2001. https://ieeexplore.ieee.org/document/990517

[7]. OWASP Foundation, "OWASP Authentication Cheat Sheet," 2023. https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[8]. OpenCV Team, "OpenCV Documentation," 2023. https://docs.opencv.org/

[9]. React Documentation, "React – A JavaScript Library for Building User Interfaces," Meta Platforms Inc., 2023. https://react.dev/

[10]. Node.js Foundation, "Node.js Documentation," 2023. https://nodejs.org/en/docs/