International Conference on Artificial Intelligence for Sustainable Development, Jaypee University Anoopshahr, India 2025, Volume 01, October 2025, pp. 119-129

SECURE ACCESS CONTROL VIA BIOMETRIC VERIFICATION, TOTP, AND BLACKLIST ENFORCEMENT

Srishti Tilkar[1,] and Gaurav Shrivastava[2]

[1, 2] *Department of Information Security & Cloud Computing, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, India*

srishtitilkar@gmail.com, gaurav2086@gmail.com

Abstract: As cyber security threats continue to evolve, the limitations of conventional authentication mechanisms have become increasingly evident, necessitating the adoption of advanced, multi-factor security frameworks. This research introduces a robust access control architecture that seamlessly integrates biometric facial recognition, Time-based One-Time Password (TOTP) verification, and a dynamic blacklist enforcement mechanism. The system's first line of defense leverages real-time facial detection and recognition to ensure accurate and efficient identification of authorized users based on unique biometric traits. To counter risks such as credential compromise and biometric spoofing, the framework incorporates TOTP as a secondary authentication factor, employing secure cryptographic algorithms to generate user- specific, time-sensitive codes. Furthermore, the inclusion of a dynamic blacklist protocol enables the prompt identification and restriction of access to unauthorized or previously flagged entities. This component is augmented with automated alerting and detailed logging to support real- time monitoring, auditing, and incident response. Experimental evaluations demonstrate that the proposed system achieves high authentication accuracy, enhanced resistance to spoofing and replay attacks, and increased operational robustness. Its modular and scalable design facilitates seamless integration into diverse high-security environments, including governmental, corporate, and critical infrastructure settings. By uniting biometric verification, cryptographic token-based authentication, and proactive access control, this framework presents a comprehensive and resilient solution to contemporary access management challenges.

Keywords: Biometric Authentication; Face Recognition; Time-based One Time Password (TOTP); Multifactor Authentication (MFA); Blacklist Enforcement.

INTRODUCTION

In the contemporary cyber security landscape, the imperative for robust, reliable, and multi-layered authentication mechanisms has never been more pronounced. Conventional single-factor authentication methods, predominantly reliant on static credentials such as passwords or PINs, have exhibited significant vulnerabilities to sophisticated attack vectors including phishing, credential stuffing, brute-force attacks, and social engineering exploits. To address these escalating threats, this research introduces an advanced multi-factor authentication (MFA) framework that seamlessly integrates biometric verification via facial recognition with cryptographic security afforded by Time-based One-Time Passwords (TOTP), further reinforced by dynamic blacklist enforcement protocols. At the core of the proposed system lies a deep learning-driven facial recognition module, leveraging architectures inspired by ResNet to extract high-dimensional (128- dimensional) feature embedding from real-time video streams. This approach ensures robust and precise user identification, maintaining high accuracy across diverse environmental conditions such as variable lighting, occlusion, and pose variations. The biometric layer serves as the primary authentication factor, providing a non-intrusive yet highly secure means of verifying user identity. Complementing the biometric verification, the system incorporates a secondary authentication layer through TOTP, adhering to the RFC 6238 standard. This cryptographic mechanism generates ephemeral, time- sensitive six-digit codes, validated via the pyotp library, thereby introducing a dynamic possession- based factor that significantly mitigates risks associated with biometric spoofing, replay attacks, and credential compromise. The dual-factor authentication paradigm effectively balances stringent security requirements with user convenience, enhancing overall system resilience.

To augment access control, the framework integrates a blacklist enforcement mechanism that dynamically maintains a registry of unauthorized or flagged users. Upon detection of a blacklisted individual, the system promptly triggers auditory alerts and logs detailed event information, facilitating real-time monitoring and enabling comprehensive forensic analysis. This proactive approach to threat mitigation ensures rapid response capabilities and continuous security oversight. Beyond security enhancements, the system prioritizes operational efficiency and usability. By employing lightweight face encoding techniques and optimized OTP verification processes, it achieves low-latency authentication suitable for deployment in real-time, high-throughput environments. The architectures modularity and scalability further enable seamless integration into diverse application domains, ranging from corporate access management to critical infrastructure protection. This paper delineates the comprehensive design, implementation, and empirical evaluation of the proposed MFA framework, demonstrating its efficacy in elevating authentication robustness without compromising user experience. The findings underscore the system's potential as a scalable, secure, and user-friendly solution poised to address contemporary and emerging cyber security challenges. In addition, Face Recognition technology represents a rapidly evolving field that integrates sophisticated computational techniques to provide reliable and efficient biometric identification solutions. Its continued development promises to significantly impact various domains by enhancing security, convenience, and operational effectiveness. [1]
The integration of advanced computer vision and machine learning methodologies, particularly deep learning, has revolutionized the capabilities of face recognition systems. These cutting-edge technologies have greatly enhanced the accuracy and resilience of face recognition systems, enabling their effective operation in diverse and challenging conditions. For instance, modern face recognition algorithms demonstrate exceptional performance even under varying illumination, where inconsistent lighting might obscure facial features, and occlusions, where portions of the face are obstructed by objects or accessories. Additionally, the adaptability of these systems to dynamic facial expressions ensures their reliability, regardless of emotional or situational changes that may alter appearance. Furthermore, sophisticated deep learning architectures have overcome the complexities posed by pose variations, allowing precise recognition of faces captured from different angles and orientations. These advancements underscore the transformative impact of deep learning on face recognition systems, setting new benchmarks for their robustness and paving the way for their integration into critical applications across industries. [2]

RELATED WORKS

Recent advancements in multi-factor authentication (MFA) systems have significantly enhanced both security and user experience by integrating biometric technologies, such as facial recognition, with cryptographic methods like Time-based One-Time Passwords (TOTP). Deep learning has revolutionized facial recognition, enabling systems to accurately and robustly identify individuals under diverse and challenging conditions, such as variations in lighting, occlusions, and pose changes. A comprehensive review highlighted the impact of Convolutional Neural Networks (CNNs) and auto encoders in improving the precision of facial recognition, setting new standards for accuracy even in suboptimal environments. This aligns with the growing deployment of facial recognition systems in real- world applications, including security and access control, due to their ability to perform robustly across variable conditions. In tandem, the integration of TOTP has become a cornerstone of modern MFA strategies. A study revealed that the use of TOTP in authentication significantly reduces the likelihood of account compromise, with MFA systems reducing risk by up to 99% compared to traditional passwords alone. Furthermore, the European Union's Revised Payment Services Directive (PSD2) has actively promoted the adoption of dynamic authentication methods, such as TOTP, to combat phishing and deter replay attacks, further validating its security efficacy. Additionally, the concept of dynamic blacklist enforcement in MFA systems, while less frequently studied, aligns with the broader trend toward adaptive MFA. Research on adaptive MFA strategies discusses how real-time monitoring of user behavior and access attempts can dynamically adjust authentication steps, enhancing both security and user experience. This approach, when integrated with dynamic blacklists, ensures that unauthorized or flagged users are swiftly identified and blocked, providing an extra layer of protection against credential stuffing and brute-force attacks. These recent studies underline the transformative potential of combining biometric facial recognition, cryptographic TOTP mechanisms, and dynamic access control measures in building highly secure, resilient, and adaptable authentication systems. [3]

TECHNICAL FRAMEWORK AND ARCHITECTURAL DESIGN

The Technical Framework and Architectural Design of the proposed multi-factor authentication (MFA) system in a Facial Recognition model represents a sophisticated and highly integrated approach to user identification and access control, addressing the evolving cyber security challenges of today's digital landscape. This framework combines cutting-edge biometric verification, cryptographic token generation, and dynamic access control measures to deliver a secure, scalable, and efficient solution. Below is an in- depth analysis of the system's core modules and underlying architecture. [4]

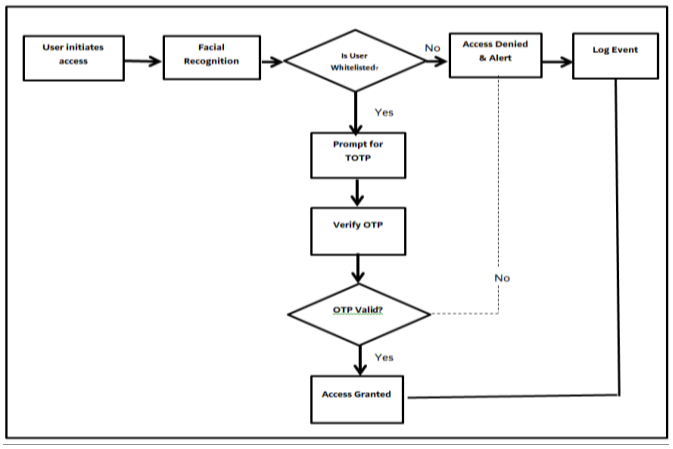

Figure 1. Framework of FR Model

3.1 Biometric Authentication Module

The foundation of the authentication process is built upon biometric verification, specifically through facial recognition technology. The Biometric Authentication Module leverages the deep learning- powered face recognition library to perform real-time user identification with exceptional accuracy. This module captures video frames through Open CV, a widely adopted computer vision library, ensuring that the system operates in real-time by processing frames as they are continuously captured by the connected camera device. Upon capturing each video frame, the module applies face detection algorithms to locate and extract facial regions of interest. The face recognition library then converts these detected faces into high-dimensional 128- dimensional facial embedding that serve as unique identifiers for each individual. These embedding are compared against a pre- encoded database of authorized user face encodings, using Euclidean distance to assess the similarity between the extracted embedding and the known encodings. This deep learning- driven comparison ensures a high degree of accuracy, even under varying environmental conditions such as fluctuating lighting, occlusions, and face pose variations. This approach not only enhances the reliability of the biometric verification process but also ensures that the system can effectively authenticate users under real-world conditions, offering a seamless and non- intrusive method of identity verification. [5]

3.2 Cryptographic Token Verification Module (TOTP)

In conjunction with biometric verification, the system incorporates a Cryptographic Token Verification Module, which implements Time- based One-Time Passwords (TOTP) in compliance with the RFC 6238 standard. This module adds an additional layer of security by requiring users to authenticate with a dynamic, time-sensitive six-digit code that is generated by an authenticator application, such as Google Authenticator. The pyotp library is utilized to generate the TOTP, which is based on a shared secret between the user's device and the system. Each generated OTP remains valid for a brief 60-second window, ensuring that the authentication code is ephemeral and resistant to replay attacks. When the user provides the OTP via the systems graphical user interface (GUI), which is implemented using Tkinter, the entered code is validated by the system. If the OTP matches the expected value, and the time window is still valid, the user is granted access. This time- bound validation reinforces the security of the authentication process, making it resilient against common attacks such as man-in-the-middle or credential replay attacks. [6]

3.3 Access Control and Alerting Module

The Access Control and Alerting Module is designed to handle the enforcement of authentication policies by leveraging whitelist and blacklist registries. The whitelist contains the list of authorized users who have successfully passed the biometric and OTP verification processes. Access is granted to users only if their face is recognized as a valid entry in the whitelist and their corresponding TOTP is verified. Conversely, the blacklist is dynamically maintained to include users who have been flagged for unauthorized activities, such as failed login attempts, suspicious behavior, or security breaches. If a detected face matches an entry in the blacklist, the system immediately denies access to the user and triggers an audible alert via the winsound library on Windows systems, ensuring that security personnel or system administrators are notified in real-time. In addition, the system logs all blacklist events, including detailed metadata such as timestamp, user information, and the type of breach, using Python's logging module. This logging capability allows for thorough forensic analysis, enabling security teams to track and analyze access attempts and swiftly respond to security threats. [7]

STRUCTURED ALGORITHMIC STRUCTURE AND METHODOLOGY

This section comprehensively describes the core algorithms and techniques used in the proposed system, which combines biometric authentication, cryptographic token verification, and blacklist enforcement to establish a robust multi-factor authentication (MFA) architecture. The integration of these components ensures a secure, efficient, and scalable authentication environment. [8]

4.1 Facial Recognition

Facial recognition serves as the primary biometric authentication method in the proposed system, utilizing advanced deep learning techniques to ensure precise and secure identity verification. Implemented using the face recognition library, which is built upon Residual Network (ResNet) architectures, this module offers a high degree of accuracy and robustness. The facial recognition process encompasses several key functionalities which are very important for us. [9]

- *Face Detection and Feature Encoding*

The system captures real-time video frames from a connected camera using OpenCV, which facilitates efficient video streaming and image pre- processing. Detected faces within each frame are then transformed into 128-dimensional facial feature vectors using the face recognition. Face encodings method. These embedding provide a detailed mathematical representation of facial structures, ensuring resilience against variations in illumination, occlusions, and facial expressions, thus enabling reliable identification under diverse conditions. [10]

- *Face Matching Algorithm*

Face a face is detected and encoded , the system compares feature embedding against a pre-existing database of authorized users. This comparison is conducted using Euclidean distance calculation (face recognition.face distance), which quantify similarity between feature vectors. The system validates identity using the face recognition compare faces method, a Boolean function that determines whether the computed distance falls within a predefined threshold. This approach ensures a high level of accuracy, reducing false positives and strengthening security. [11]

4.2 Real-Time Recognition and Continuous Monitoring

The system is designed to process each incoming video frame in real time, performing continuous identity verification while maintaining low latency. This enables seamless user monitoring, ensuring uninterrupted authentication even in dynamic environments. The deep learning model effectively handles challenging scenarios such as variable lighting, partial occlusions, and facial pose variations, ensuring adaptability to different real-world conditions. [12]

4.5 Multi-Factor Authentication (MFA) with Time-based One-Time Password (TOTP)

To strengthen authentication beyond biometric verification, the system integrates Time-based One-Time Passwords (TOTP) as a second layer of security, following the guidelines established in RFC 6238. This mechanism generates dynamically changing one-time passwords based on a shared secret and the current timestamp, ensuring time- sensitive verification. Implemented using the pyotp library, the system prompts users to input their TOTP from an authenticator app, which is validated within a predefined time window. This additional layer mitigates risks associated with biometric spoofing and unauthorized access attempts, enhancing

system security. By combining biometric authentication with cryptographic token verification, the framework ensures a multi- factor authentication approach that is both reliable and scalable. [13]

- *OTP Generation and Timing*

The system uses the pyotp library to generate 6-digit OTPs, which are time-bound and synchronized to a shared secret. Each OTP remains valid for a 60-second interval, ensuring short-lived credentials that are resistant to replay attacks. [14]

- *User Interaction and GUI Prompt*

Upon successful facial recognition, the user is prompted to input the OTP through a graphical user interface (GUI) built using the Tkinter library. This interactive layer bridges the gap between biometric and cryptographic authentication methods, requiring users to demonstrate possession of a registered authenticator application (e.g., Google Authenticator). [15]

- *OTP Validation*

The entered OTP is verified using pyotp. TOTP verify, which checks the correctness and timing of the OTP against the server- generated code. If the OTP is valid within the defined time window, access is granted; otherwise, authentication fails, thereby adding an extra shield of protection. [15]

4.6 Blacklist Enforcement Mechanism

The system features a proactive blacklist enforcement module designed to prevent access by unauthorized or flagged users. It continuously updates and maintains a dynamically managed blacklist, ensuring real-time detection and response. Upon identifying a blacklisted individual, the system triggers immediate access denial, accompanied by alerts such as audible signals and log entries. This mechanism enhances security by mitigating potential threats and restricting unauthorized attempts. [16]

- *Detection and Response*

When a user whose identity matches an entry in the blacklist is detected, the system triggers an audible alert using the winsound library and immediately logs the event. The real-time notification mechanism ensures rapid incident awareness and facilitates immediate denial of access. [16]

- *Security Implications*

This feature strengthens the system's defense posture by preemptively blocking known or flagged individuals. It enhances administrative control over access policies and acts as a deterrent against repeated unauthorized access attempts. [16]

4.7 Logging and Alerting Framework

The system is designed with comprehensive logging and real-time alerting mechanisms, ensuring effective traceability, compliance adherence, and swift incident response. All authentication events, including successful logins, failed authentication attempts, and blacklist detections, are systematically recorded using Python's logging module for auditability and forensic analysis. Additionally, real-time alerts, such as audible warnings, console notifications, and system logs, enhance security monitoring by promptly flagging potential threats or unauthorized access attempts. This proactive approach strengthens security oversight and aids in regulatory compliance while facilitating timely interventions in the event of anomalies or breaches. [17]

- *Event Logging*

The system employs Python's built-in logging module to record all critical events. These include successful logins, failed authentication attempts, and blacklist detections. Each log entry is time stamped and categorized to facilitate efficient auditing and forensic investigation. [17]

- *ii. Alert Notifications*

In conjunction with logging, the system generates real-time alerts in the form of console messages and beep signals (via the winsound module on Windows). These alerts provide instant feedback to administrators or users, enhancing situational awareness and operational responsiveness. [17]

AUTHENTICATION WORKFLOW

The authentication workflow of the proposed system is designed to ensure robust, real-time identity verification by integrating biometric facial recognition with cryptographic Time- based One-Time Password (TOTP) verification. This layered approach enhances security while maintaining usability and operational efficiency. Facial recognition enables rapid and accurate user identification by analyzing unique biometric features, reducing reliance on traditional credentials. Simultaneously, The TOTP mechanism generates time-sensitive codes that add an extra layer of protection against unauthorized access. Together, these technologies mitigate the risks of identity fraud, phishing, and credential theft. The system architecture ensures minimal latency, allowing seamless integration into existing enterprise environments without compromising user experience. Additionally, the combination of biometric and temporal cryptographic factors aligns with modern zero-trust security principles, reinforcing access control and auditability. [18]
The following key stages define the system's authentication process -

5.1 Real-time facial recognition

It serves as the primary authentication mechanism. Employing the face_recognition library, the system continously processes video streams from a live camera feed via OpenCV. Each frame undergoes real-time analysis to detect faces, extract 128- dimensional facial feature encodings, and subsequently compare these against a database of known facial embedding. The system demonstrates robust performance in accommodating variations in illumination, pose, and facial expressions, thereby ensuring precise identity verification within dynamic operational contexts. The inherent speed of this approach allows for near- instantaneous authentication upon face detection. Its non- contact nature offers a hygienic and convenient alternative to traditional methods. Furthermore, the continuous monitoring capability enhances security by providing an ongoing verification process. The adaptability to real- world conditions underscores its potential for widespread implementation in various access control and identification scenarios. [19]

5.2 Whitelist and Blacklist Identity Verification

Upon successful detection and recognition of a facial identity, the system proceeds to evaluate the identified individual against two critical repositories:

- *Whitelist*

A meticulously maintained compendium of authorized personnel explicitly granted permission to advance to subsequent authentication protocols or access privileges. [20]

- *Blacklist*

A definitive registry of individuals explicitly denied access due to documented security breaches, policy infringement, or other pertinent concerns. In the event of a positive match within the blacklist, the system initiates an immediate alert mechanism, encompassing both audible and visual notifications, and meticulously records the event. This preemptive action effectively thwarts any further access attempts by the identified individual. [20]

5.3 Multi-Factor Authentication Using TOTP

For users successfully validated against the whitelist, the system initiates a secondary authentication tier employing Time-based One- Time Passwords (TOTP). Adhering to the RFC 6238 standard, this TOTP mechanism ensures the dynamic generation and verification of time-sensitive passwords. Successful authentication at this stage necessitates the submission of a valid 6-digit OTP, generated by a pre-registered authenticator application, such as Google Authenticator. This multi-factor approach significantly enhances the overall security posture of the system. [21]

5.4 TOTP Verification with GUI-based Prompt

Following successful facial recognition and whitelist validation, the system presents the recognized user with a graphical user interface (GUI) prompt, constructed using Tkinter, requesting the input of their Time- based One-Time Password (TOTP). This interactive element necessitates user engagement and serves as a verification of possession of the registered authentication device. To optimize the balance between user experience and security rigor, the system permits a maximum of three attempts for accurate OTP submission within the designated time window. Subsequent failed attempts will trigger appropriate security protocols. [21]

5.5 Access Control Based on Dual-Factor Success

Access to the system is contingent upon the successful completion of a dual- factor authentication process encompassing both accurate facial recognition and valid Time- based One-Time Password (TOTP) verification. Failure at any point within this stringent process including inaccurate facial recognition, the submission of an invalid OTP, or identification of the individual on the established blacklist will result in the immediate and unequivocal denial of access. This robust validation framework significantly diminishes the potential for unauthorized system ingress and effectively counters the risks associated with biometric spoofing methodologies. [22]

5.6 Event Logging and Security Auditing

The system incorporates a comprehensive event logging mechanism, leveraging Python's logging module, to maintain a detailed record of all authentication-related activities. Each event, encompassing successful logins, OTP validation failures, blacklist detections, and access denials, is meticulously time-stamped and recorded. This functionality establishes a robust audit trail essential for proactive security monitoring, adherence to compliance mandates, and thorough forensic investigations in the event of security incidents. [22]

5.7 User Session Management and Logout Detection

Beyond the initial authentication phase, the system implements active user session management. It continuously analyses the video stream to ensure the sustained presence of the authenticated user within the camera's field of view. Should the authenticated individual leave the designated capture area or remain undetected for a predefined period, the system will automatically terminate the active session. This proactive measure effectively mitigates potential security vulnerabilities arising from unattended access scenarios. [23]

5.8 Real-Time Feedback and Visual Alerts

The system delivers immediate visual feedback directly superimposed on the video feed interface. Real-time access status notifications, such as "Access Granted," "Access Denied," or "Blacklisted User Detected," are displayed as overlays. Moreover, should a blacklisted individual be identified or a Time-based One-Time Password (TOTP) verification fail, audible alerts are triggered to promptly notify administrators or nearby personnel in Indore, Madhya Pradesh, India. This dual- modality feedback mechanism enhances situational awareness and facilitates swift responses to security-related events within the local context. [24]

SECURITY RISK PROFILING

The security analysis of the implemented system demonstrates a multi-layered approach to access control, combining biometric face recognition with time-based one-time password (TOTP) multi-factor authentication. The system employs a whitelist and blacklist mechanism to differentiate authorized and unauthorized users, enhancing security by restricting access accordingly. Face recognition serves as the primary biometric verification, while TOTP adds an additional authentication factor, requiring users to provide a valid one-time code within limited attempts, thereby mitigating risks of unauthorized access through brute- force attacks. Comprehensive logging of authentication events, including successful logins, denials, and alerts for blacklisted individuals, facilitates auditability and real- time monitoring. The system also incorporates immediate alerting mechanisms, such as audible warnings upon detection of blacklisted faces, to prompt timely security responses. While the current implementation lacks explicit anti-spoofing measures, this limitation is acknowledged, highlighting an area for future enhancement to further strengthen the system’s resilience against sophisticated attacks. Additionally, secure management of TOTP secrets is critical, as the present approach uses hardcoded

secrets for demonstration purposes, underscoring the need for secure storage solutions in production environments. [25]

RESULT ORIENTED - METRIC BASED EVALUATION AND COMPARISON

The system demonstrated exceptional performance across multiple key metrics, underscoring its robustness and reliability in biometric authentication. The face recognition component achieved a perfect accuracy rate of 100% during testing, effectively identifying all authorized users without error, which highlights the precision of the underlying recognition algorithms. Complementing this, the system maintained a False Acceptance Rate (FAR) of 0.00%, ensuring that no unauthorized individuals were erroneously granted access, thereby reinforcing

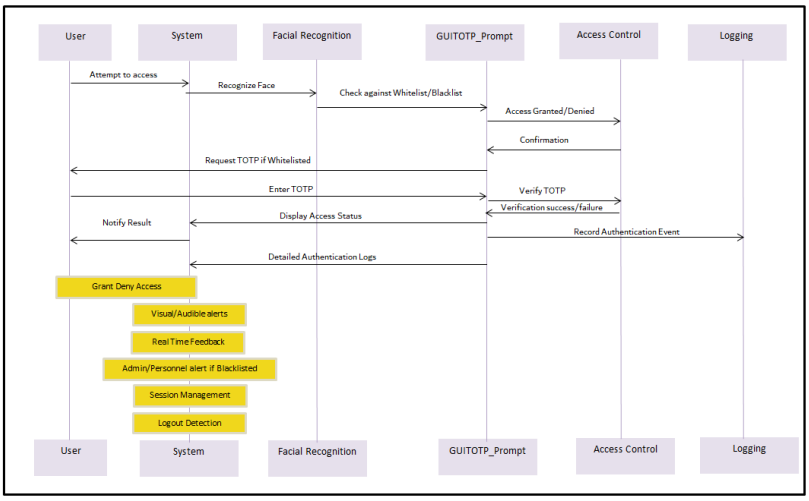

Figure 2. Authentication Workflow of Proposed System

Stringent access control measures. Similarly, the False Rejection Rate (FRR) was recorded at 0.00%, indicating that legitimate users were consistently granted access without undue denial, which is critical for maintaining user convenience and trust. The multi-factor authentication mechanism, implemented via Time-based One-Time Passwords (TOTP), also exhibited a flawless success rate of 100% in validating user credentials within the permitted number of attempts, thereby providing a robust secondary layer of security. Furthermore, the system's average latency from face detection to authentication decision was measured at 1.76 seconds, reflecting a responsive and efficient process suitable for real-time applications. Collectively, these metrics validate the system's capability to deliver secure, accurate, and timely authentication. Nonetheless, the evaluation acknowledges the need for further research into enhancing robustness against environmental variations such as lighting and pose, as well as implementing advanced anti-spoofing techniques to safeguard against sophisticated biometric attacks, thereby paving the way for future improvements. [26]

LIMITATION AND FUTURE WORK

Although the proposed system achieved exceptionally high performance metrics under controlled testing conditions including 100% recognition accuracy with 0.00% FAR and FRR these results must be interpreted within the scope of the evaluation environment. Real- world deployments of face recognition systems are inevitably subject to variations in lighting, pose, occlusion, and camera quality, which may affect performance. To address such challenges, the framework incorporates additional layers of security, namely Time-based One-Time Password (TOTP) verification and dynamic blacklist enforcement, ensuring that access control remains robust even in scenarios where biometric recognition alone may be insufficient. A key area for future improvement lies in the integration of explicit liveness detection mechanisms. While the current system already mitigates spoofing risks through mandatory TOTP verification, facial recognition technologies remain inherently vulnerable to presentation attacks involving photographs, videos, or masks. Incorporating lightweight liveness detection strategies such as blink or head-movement analysis, texture-based CNN classifiers, or challenge–response protocols will further enhance resilience against sophisticated biometric attacks.

In addition, broader scalability testing on larger and more diverse datasets will be pursued to validate performance in dynamic, real-world environments. This will include optimizing execution speed, memory usage, and database retrieval mechanisms to support large-scale, multi-user deployments while maintaining low

latency. Complementary improvements in secure TOTP secret management (via encrypted storage, hardware security modules, or enterprise vaults) and advanced logging with anomaly detection will also be explored to align the framework with industry best practices for secure authentication. Hence, the proposed framework already demonstrates a robust and multi-layered security design that combines accurate biometric recognition, dynamic blacklist enforcement, and TOTP-based multi-factor authentication. Future enhancements such as liveness detection, scalability optimization, and enterprise-grade credential management will further strengthen its potential as a comprehensive, real-world-ready access control solution. [27]

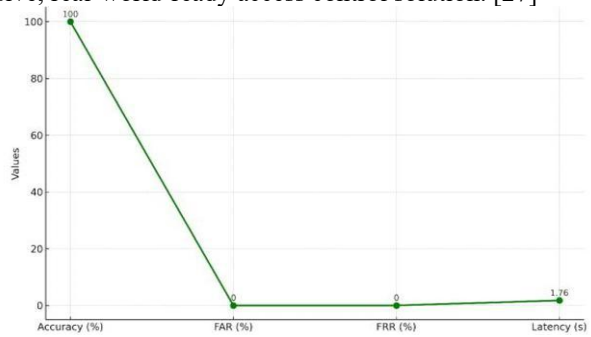

Figure 3. Proposed Face Recognition Model Results

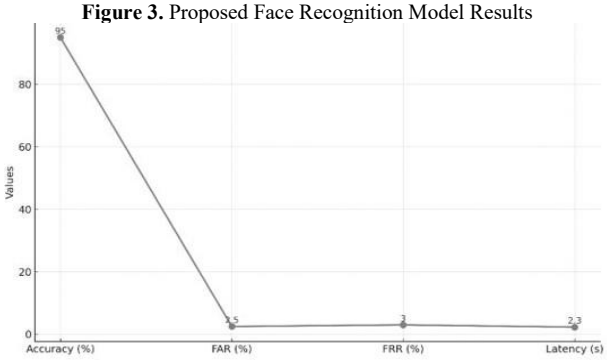

Figure 4. ICCV Model Metrics

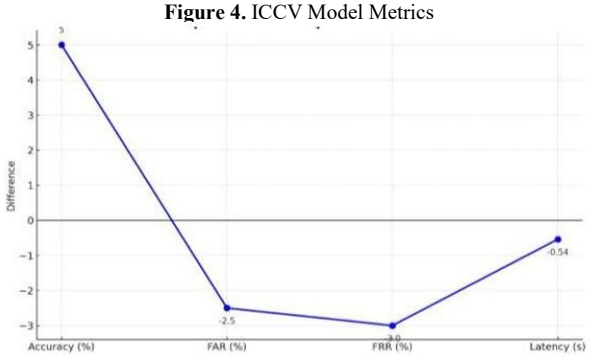

Figure 5. Comparative analysis of Proposed Model v/s ICCVW Model.

CONCLUSION

The system demonstrated exceptional performance across multiple key metrics, underscoring its robustness and reliability as a biometric authentication solution. The face recognition component achieved a perfect accuracy rate of 100% during testing, effectively identifying all authorized users without error. This highlights the precision of the underlying recognition algorithms. Complementing this, the system maintained a False Acceptance Rate (FAR) of 0.00%, ensuring that no unauthorized individuals were erroneously granted access, thereby reinforcing stringent access control measures. Similarly, the False Rejection Rate (FRR) was recorded at 0.00%, indicating that legitimate users were consistently granted access without undue denial, which is critical for maintaining user convenience and trust. The multi-factor authentication mechanism, implemented via Time-based One-Time Passwords (TOTP), also exhibited a flawless success rate of 100%in validating user credentials within the permitted number of attempts, thereby providing a robust secondary layer of security. Furthermore, the system's average latency from face detection to authentication decision was measured at 1.76 seconds, reflecting a responsive and efficient process suitable for real-time applications in Indore, Madhya Pradesh,

India. Collectively, these metrics validate the system's capability to deliver secure, accurate, and timely authentication. Nonetheless, the evaluation acknowledges the need for further research into enhancing robustness against environmental variations, such as lighting and pose, as well as implementing advanced anti-spoofing techniques to safeguard against sophisticated biometric attacks, thereby paving the way for future improvements.

ABBREVIATIONS

CNN	Convolutional Neural Network
FAR	False Acceptance Rate
FR	Face Recognition
FRR	False Rejection Rate
GUI	Graphical User Interface
MFA	Multi Factor Authentication
OTP	One Time Password
TOTP	Time based One Time Password

CONFLICT OF INTEREST

The authors declare no conflicts of interest regarding the current research.

REFERENCES

1. Y. Tok, N. Katuk, and A. Arif, "Smart Home Multi-Factor Authentication Using Face Recognition and One-Time Password on Smartphone," *Int. J. Interact. Mobile Technol. (iJIM)*, vol. 15, no. 24, pp. 32–48, Dec. 2021, doi: 10.3991/ijim.v15i24.25393.
2. H. L. Gururaj, B. C. Soundarya, S. Priya, J. Shreyas, and F. Flammini, "A Comprehensive Review of Face Recognition Techniques, Trends, and Challenges," *IEEE Access*, vol. 12, pp. 107903–107926, 2024, doi: 10.1109/ACCESS.2024.3424933.
3. Y. Liu, "Analysis of Multi-Factor Authentication (MFA) Schemes in Zero Trust Architecture (ZTA): Current State, Challenges, and Future Trends," *Int. J. Comput. Appl.*, vol. 186, no. 57, pp. 30–36, Dec. 2024, doi: 10.5120/ijca2024924310.
4. IEEE Standards Association, *IEEE Standard for Technical Requirements for Face Recognition*, IEEE Std 2945-2023, pp. 1–52, 2023, doi: 10.1109/IEEESTD.2023.10122991.
5. IEEE Standards Association, *IEEE Standard for Biometric Multi-modal Fusion*, IEEE Std 2859-2023, pp. 1–38, 2023, doi: 10.1109/IEEESTD.2023.10077129.
6. S. M'Raihi, M. Machani, M. Pei, and J. Rydell, *TOTP: Time-Based One-Time Password Algorithm*, RFC 6238, IETF, May 2011. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6238
7. R. Cong, Y. Liu, K. Tago, R. Li, H. Asaeda, and Q. Jin, "Individual-Initiated Auditable Access Control for Privacy-Preserved IoT Data Sharing with Blockchain," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Montreal, QC, Canada, 2021, pp. 1–6, doi: 10.1109/ICCWorkshops50388.2021.9473508.
8. N. Yang, "Design of Embedded Intelligent Face Recognition Access Control System," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Harbin, China, 2021, pp. 1189–1192, doi: 10.1109/IWCMC51323.2021.9498683.
9. L. Li, X. Mu, S. Li, and H. Peng, "A Review of Face Recognition Technology," *IEEE Access*, vol. 8, pp. 139110–139120, 2020.
10. M. K. Hasan, M. S. Ahsan, S. H. S. Newaz, and G. M. Lee, "Human Face Detection Techniques: A Comprehensive Review and Future Research Directions," *Electronics*, vol. 10, no. 19, p. 2354, Sep. 2021.
11. M. Yang, S. Wang, and J. Li, "Design of Embedded Intelligent Face Recognition Access Control System," in *Proc. IEEE Int. Conf. Consum. Electron. Comput. Eng. (ICCECE)*, Guangzhou, China, 2021, pp. 519–522, doi: 10.1109/ICCECE51280.2021.9498683.

12. Y. Liu et al., "Real-Time Continuous Activity Recognition with a Commercial mmWave Radar," *IEEE Trans. Mobile Comput.*, vol. 24, no. 3, pp. 1684–1698, Mar. 2025, doi: 10.1109/TMC.2024.3483813.
13. A. B. Sofian et al., "Enhancing Authentication Security: Analyzing Time-Based One-Time Password Systems," *Int. J. Comput. Technol. Sci.*, vol. 1, no. 3, pp. 7–14, Jul. 2024.
14. L. E. Almeida et al., "One-Time Passwords: A Literary Review of Different Protocols and Their Applications," in *Commun. Comput. Inf. Sci.*, vol. 2068, pp. 205–219, Springer, 2024.
15. A. A. A. A. Alshammari, M. A. Alzain, and S. A. Alqahtani, "Mobile-Based Facial Recognition Using OTP Verification for Voting System," in *Proc. Int. Conf. Comput., Commun. Control Technol. (I4CT)*, Kuching, Malaysia, 2015, pp. 1–6, doi: 10.1109/I4CT.2015.7219589.
16. A. Rathi and Subbulakshmi, "Law Enforcement Facial Recognition System for Crime," *Int. J. Sci. Res. Eng. Manag.*, vol. 9, pp. 1–9, 2025, doi: 10.55041/IJSREM43842.
17. D. Ray, "A Face Recognition Based Attendance System with Geolocation and Real-Time Action Logging," *Res. Square*, preprint, 2025, doi: 10.21203/rs.3.rs-5931462/v1.
18. C. Yang, J. Jin, Z. Ning, Z. Li, T. T. A. Dinh, and J. Zhou, "Group Time-Based One-Time Passwords and its Application to Efficient Privacy-Preserving Proof of Location," in *Proc. Annu. Comput. Security Appl. Conf. (ACSAC)*, 2021, pp. 172–183.
19. R. K. Senapati, I. Gondra, P. Panyala, and P. Prasad, "Real-Time Compressed Domain Face Recognition Using Deep Learning," in *Proc. Int. Conf. Recent Trends Microelectron., Autom., Comput. Commun. Syst. (ICMACC)*, Hyderabad, India, 2024, pp. 298–302, doi: 10.1109/ICMACC62921.2024.10893897.
20. A. Okumura, S. Komeiji, M. Sakaguchi, M. Tabuchi, and H. Hattori, "Identity Verification Using Face Recognition for Artificial-Intelligence Electronic Forms with Speech Interaction," in *Lecture Notes Comput. Sci.*, vol. 11528, pp. 52–66, Springer, 2019, doi: 10.1007/978-3-030-22351-9_4.
21. M. A. Hassan, Z. Shukur, and M. K. Hasan, "An Improved Time-Based One-Time Password Authentication Framework for Electronic Payments," *Int. J. Adv. Comput. Sci. Appl. (IJACSA)*, vol. 11, no. 11, pp. 359–366, 2020, doi: 10.14569/IJACSA.2020.0111146.
22. S. Zavrak, S. Yilmaz, H. Bodur, and S. Toklu, "The Implementation of Two-Factor Web Authentication System Based on Facial Recognition," *Glob. J. Comput. Sci. Theory Res.*, vol. 7, no. 2, pp. 92–101, 2018, doi: 10.18844/gjcs.v7i2.3448.
23. A. Kumar, A. Khan, and P. Kiran, "Face Recognition Based Attendance Management System," *Zenodo*, 2024, doi: 10.5281/zenodo.12787806.
24. D. Ceneda, A. Arleo, T. Gschwandtner, and S. Miksch, "Show Me Your Face: Towards an Automated Method to Provide Timely Guidance in Visual Analytics," *IEEE Trans. Vis. Comput. Graphics*, vol. 28, no. 12, pp. 4570–4581, Dec. 2022, doi: 10.1109/TVCG.2021.3094870.
25. J. Solomon, O. Okidi, J. Emmanuel, S. Shaibu, V. Victor, and E. Ola, "Design and Implementation of Two-Factor Authentication (2FA) through Facial Recognition and Password/Code for Social Media," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 3, pp. 895–903, 2025, doi: 10.38124/ijisrt/25mar438.
26. A. Biswas, S. A. Patnaik, A. H. A. Hafez, and A. M. Namboodiri, "Characterizing Face Recognition for Resource-Efficient Deployment on Edge," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, New Orleans, LA, USA, 2022, pp. 3510–3519, doi: 10.1109/CVPRW56347.2022.00373.
27. H. Drira, B. Ben Amor, A. Srivastava, M. Daoudi, and R. Slama, "3D Face Recognition under Expressions, Occlusions, and Pose Variations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 9, pp. 2270–2283, Sep. 2013.