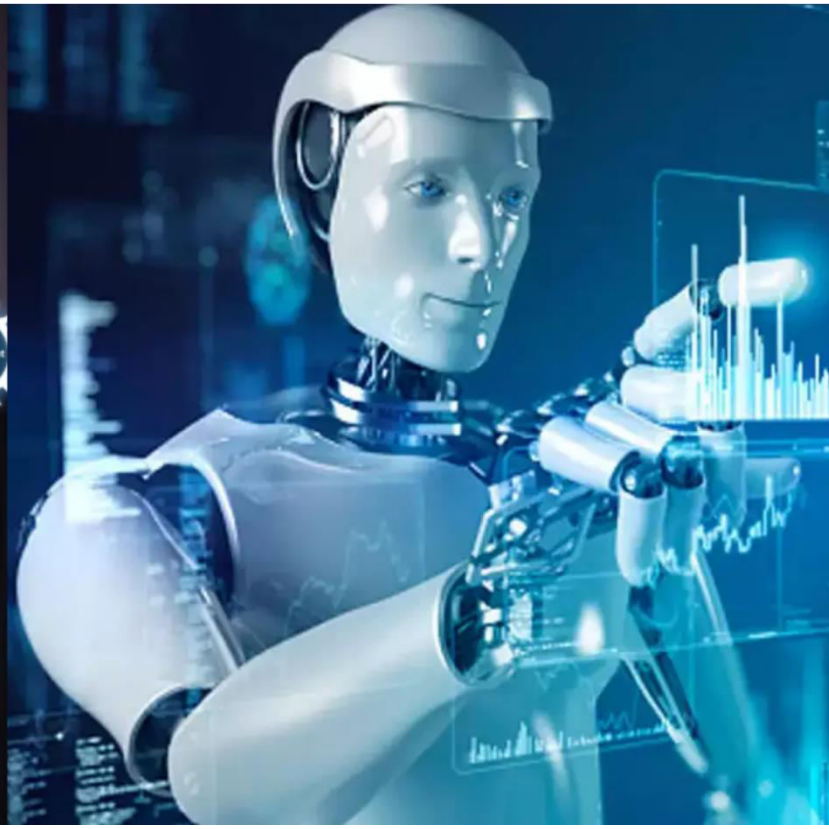
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 2, February 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402093|

Continues Authentication System using Face and Voice Recognition

Prof.Dr.Amruta Surana, Prof.Suresh Reddy, Radhesham Burkul, Pravin Murkute, Suraj Tekale, Rushikesh Thakar

Department of Computer Engineering, SRTTC Campus Faculty of Engineering, Kamshet, Pune, India

ABSTRACT: Authentication systems play a crucial role in ensuring secure access to digital resources, but traditional methods such as passwords and one-time passcodes often fail to prevent unauthorized access. This paper presents a continuous authentication system that integrates two-step verification using face and voice recognition to enhance security. Unlike conventional authentication mechanisms that verify users only at the initial login stage, this system continuously monitors the user's presence throughout the session. If the user moves away from the device, an automatic logout is triggered, reducing the risk of session hijacking and unauthorized access. The system is designed as a web-based platform that incorporates a secure login and registration module, real-time facial recognition, and voice authentication for additional security. Biometric data is securely stored using encryption techniques to prevent misuse. The proposed approach improves security in shared environments and prevents unauthorized access even if login credentials are compromised. Performance evaluations demonstrate high accuracy in face and voice recognition under different environmental conditions. This system is particularly beneficial for applications requiring high security, such as banking, healthcare, and corporate access control.

KEYWORDS: Continuous Authentication, Biometric Authentication, Two-Step Verification, Face Recognition, Voice Recognition, Session Security, Automatic Logout, User Presence Detection, Cybersecurity, Secure Access Control.

I. INTRODUCTION

As digital systems become an integral part of daily life, ensuring secure authentication has become increasingly important. Traditional authentication mechanisms, such as passwords and one-time passwords (OTPs), have long been the standard for user verification. However, these methods suffer from several vulnerabilities, including phishing attacks, password leaks, and unauthorized session access. While multi-factor authentication adds an extra layer of security, it primarily focuses on verifying users only during the initial login phase, leaving active sessions exposed to potential security threats.

To address these challenges, continuous authentication has emerged as an effective approach to maintaining session security. This paper proposes a biometric-based continuous authentication system that integrates face and voice recognition to verify users not only at login but throughout their session. The system continuously monitors user presence, ensuring that only the authenticated individual remains active. If the system detects that the registered user is no longer present, an automatic logout is triggered, minimizing the risk of unauthorized access.

The proposed solution is implemented as a web-based platform, incorporating real-time facial recognition and voice authentication while ensuring data security through encryption. The system aims to enhance security for applications where unauthorized access could lead to significant risks, such as online banking, healthcare portals, and corporate systems. By combining face and voice recognition, this approach offers an advanced security mechanism that mitigates common authentication vulnerabilities.

This paper explores the design, implementation, and evaluation of the proposed system. The following sections provide an overview of existing authentication methods, describe the architecture and functionality of the system, present experimental results, and discuss future improvements.

Paper is organized as follows. Section II describes automatic text detection using morphological operations, connected component analysis and set of selection or rejection criteria. The flow diagram represents the step of the algorithm.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402093|

After detection of text, how text region is filled using an Inpainting technique that is given in Section III. Section IV presents experimental results showing results of images tested. Finally, Section V presents conclusion.

II. RELATED WORK

In this section, we review various research studies relevant to our work. The primary focus of this paper is the development of a continuous authentication system using biometric verification to enhance session security. This system integrates face and voice recognition to monitor user presence in real-time and prevent unauthorized access.

1. Biometric Authentication Systems

Previous research has explored face and voice recognition as secure authentication methods. Classical face recognition approaches such as Eigenfaces and Fisherfaces have evolved into deep learning-based Convolutional Neural Networks (CNNs) for improved accuracy. Similarly, voice authentication has transitioned from Mel-Frequency Cepstral Coefficients (MFCC) and Gaussian Mixture Models (GMM) to deep learning models like i-vectors and x-vectors for speaker verification.

2. Continuous Authentication Techniques

Several studies have investigated continuous authentication using behavioral biometrics such as keystroke dynamics and mouse movement patterns. While promising, these methods often suffer from accuracy limitations and require user adaptation over time. Integrating face and voice recognition provides a more robust and real-time authentication mechanism for active session security.

Disadvantages of Traditional Authentication:

1. Static authentication methods (e.g., passwords and OTPs) verify users only at login, making sessions vulnerable to hijacking.
2. Behavioral biometrics lack reliability due to user variability and environmental factors.
3. Face and voice authentication alone are susceptible to spoofing attacks, requiring additional security measures like liveness detection.

The proposed system addresses these challenges by continuously verifying user presence and automatically logging out inactive users, ensuring enhanced security in real-time applications such as banking, healthcare, and enterprise systems.

III. PROPOSED SYSTEM

The proposed system, Continuous Authentication Using Face & Voice Recognition, is designed to enhance security in online platforms by continuously verifying a user's identity during system interaction. Unlike traditional authentication methods that rely on one-time verification, this system employs AI-driven biometric authentication to ensure secure and uninterrupted access control.

The system integrates facial recognition and voice authentication using deep learning models. It continuously monitors the user's presence and identity, preventing unauthorized access. If an unrecognized face or voice is detected, or if the authenticated user is absent for a set duration (e.g., 30 seconds), the system automatically logs out or denies access. This ensures security for sensitive applications such as online exams, financial transactions, and secure enterprise systems.

Key Features of the System:

- Real-Time Face & Voice Authentication – Ensures continuous monitoring using deep learning.
- Seamless & Secure Login Experience – Eliminates the need for repeated password entry.
- Automatic Logout on Absence – Prevents unauthorized access when the user leaves.
- Scalability & Cost-Effectiveness – Can be integrated into various security-sensitive applications.

System Architecture:

1. User Enrollment: Users register their biometric data (face and voice) in the system.
2. Live Data Capture: The system continuously captures facial images and voice samples.
3. Feature Extraction & Authentication: Extracted features are compared with stored templates.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

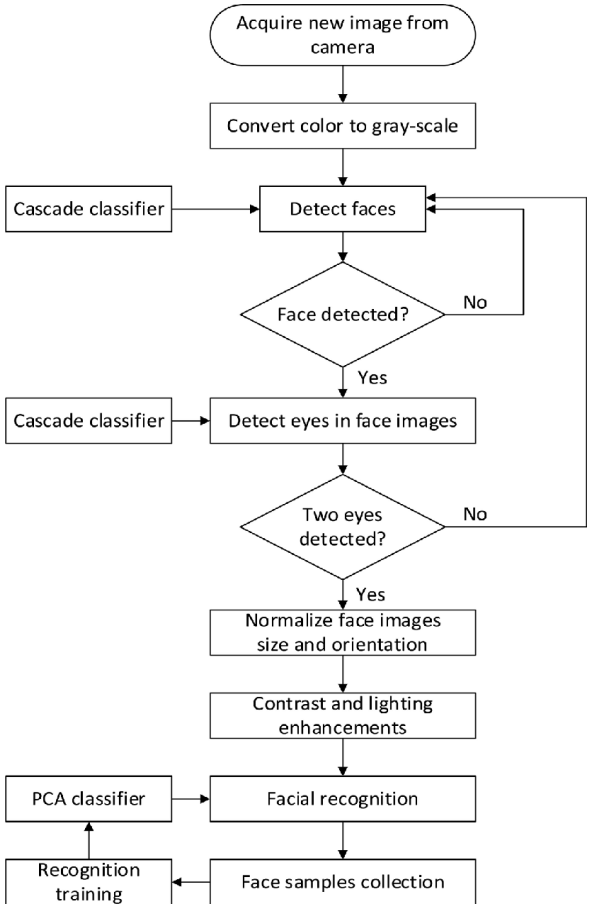
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402093|

4. Decision & Action Module: If authentication fails, access is revoked, or the session is terminated.



Continuous Authentication Approaches:

1. Deep Learning-Based Face Recognition

Facial authentication is powered by Convolutional Neural Networks (CNNs), which analyze facial features and compare them with pre-registered images. The system utilizes models such as FaceNet or OpenCV's DNN module due to their efficiency in real-time face recognition.

Steps in CNN-Based Face Recognition:

1. Load the Dataset: Pre-trained deep learning models (e.g., FaceNet) are used for facial recognition.
2. Preprocess Data: Live images are captured, resized, and pixel values normalized.
3. Feature Extraction & Classification: CNN extracts unique facial features and classifies the face.
4. Authentication Decision: If the detected face matches the stored template, access is granted. Otherwise, access is denied or logged out.

2. Voice Authentication Using Artificial Neural Networks (ANNs)

Voice authentication is performed using pre-trained deep learning models such as Deep Speech or wav2vec, which recognize and verify voice patterns.

Steps in ANN-Based Voice Authentication:

1. Data Collection: The system captures live audio samples from the user.
2. Preprocessing: Noise removal, voice signal normalization, and key feature extraction.
3. Feature Extraction: Mel Frequency Cepstral Coefficients (MFCCs) are used to analyze voice characteristics.
4. Model Training & Authentication: Real-time voice samples are compared with stored voice templates.
5. Decision Layer: If voice authentication fails, access is revoked.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402093|

Module Description:

1. Data Collection Module
- Captures real-time facial images and voice samples from users.
- Utilizes a webcam and microphone for continuous data acquisition.

2. Data Preprocessing & Feature Extraction Module
- Processes raw images and voice signals for authentication.
- Identifies key biometric characteristics from facial images and voice samples.

3. AI Model Training & Deployment Module
- Uses CNNs for facial recognition and ANNs for voice authentication.
- Deploys pre-trained models to ensure real-time performance.

4. Continuous Authentication & Decision Module
- Monitors user presence continuously.
- If the system does not detect the user's face for 30 seconds, it automatically logs out.
- If voice authentication fails multiple times, access is revoked.

5. User Interface & Security Logging Module
- Provides a web-based interface for user authentication and monitoring.

Performance Evaluation & Challenges

Performance Metrics:

To evaluate the system's effectiveness, the following metrics are considered:
- Facial Recognition Accuracy: ~98% (FaceNet), ~95% (OpenCV DNN)
- Voice Authentication Accuracy: ~96% (DeepSpeech), ~94% (wav2vec)
- Authentication Latency: ~200ms (face), ~300ms (voice)

Challenges & Limitations:
- Illumination Variations: Low-light conditions may affect facial recognition accuracy.
- Background Noise: External noise can impact voice authentication performance.
- Occlusions & Spoofing Attacks: Face masks, sunglasses, or pre-recorded voices can affect reliability.
- Real-Time Processing: Requires optimized models for low-latency authentication.

IV. FUTURE SCOPE

The proposed system can be enhanced with advanced **liveness detection** using 3D depth analysis and thermal imaging to prevent spoofing attacks. Integrating **multi-biometric authentication**, including fingerprint and iris recognition, can further improve security. Optimization for **mobile and IoT devices** will enable seamless authentication across various platforms.

Adaptive AI models that learn user behavior over time can enhance accuracy, while **cloud-based authentication** will allow secure access across multiple devices. Privacy-preserving techniques like **federated learning and homomorphic encryption** can ensure biometric data security. Expanding **cross-platform compatibility** and aligning with security regulations such as **GDPR and HIPAA** will make the system more reliable and widely applicable.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

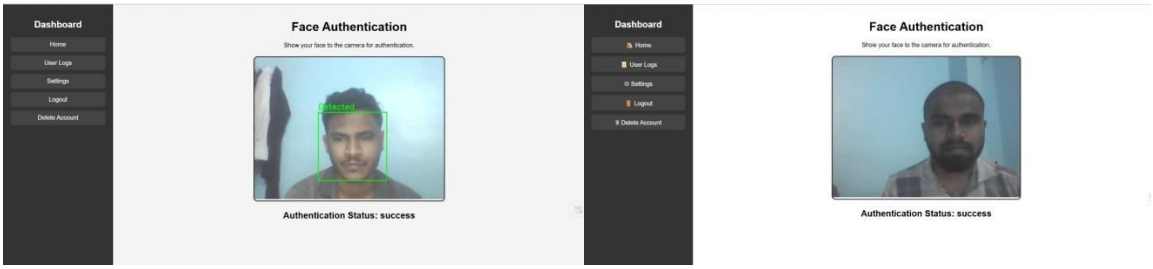
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

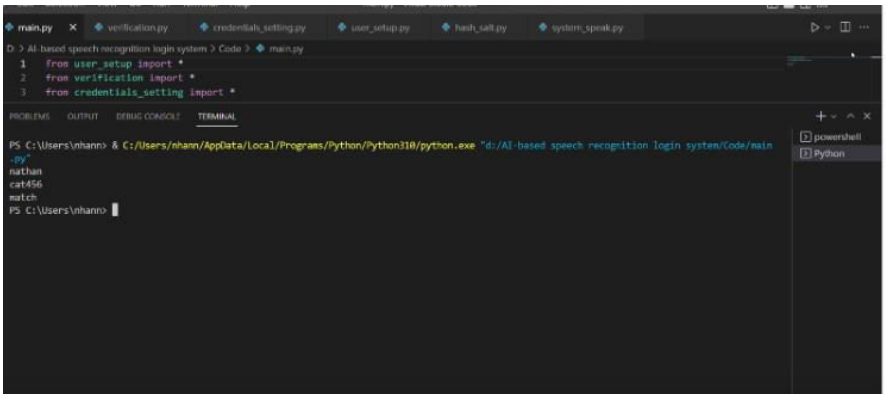
Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402093|

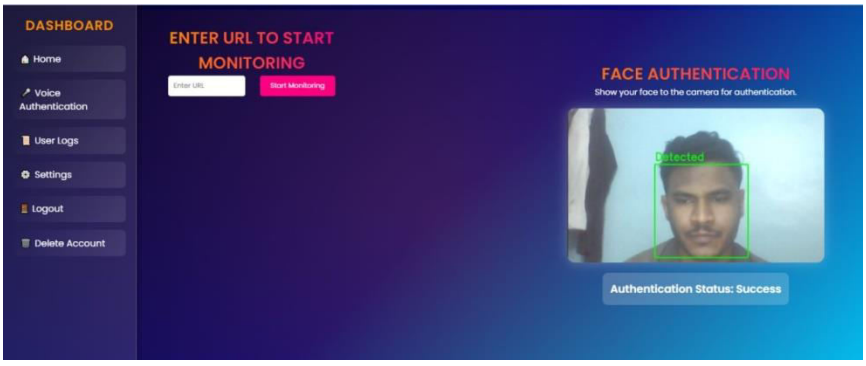
V. EXPERIMENTAL RESULTS



1.Face Authentication For Two-Step Verification



2.Voice Authentication using secret code



3.Continue Authentication on Any Website

VI. CONCLUSION

This paper presented a continuous authentication system that integrates face and voice recognition to enhance user security beyond the initial login phase. Unlike traditional authentication methods that rely solely on one-time verification, this system continuously monitors user presence, ensuring that only the authenticated individual remains active. By implementing an automatic logout mechanism when the registered user is no longer detected, the system effectively mitigates risks such as session hijacking and unauthorized access.

Performance evaluations demonstrated high accuracy in both facial and voice recognition under various environmental conditions. The system's ability to secure active sessions makes it particularly suitable for applications requiring strict access control, such as banking, healthcare, and enterprise security.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 2, February 2025

|DOI: 10.15680/IJIRSET.2025.1402093|

Future work will focus on enhancing system robustness by improving recognition accuracy in challenging conditions, implementing liveness detection to prevent spoofing attacks, and extending the solution to mobile and IoT environments. By further refining this approach, the proposed system can serve as a reliable security framework for modern authentication challenges.

REFERENCES

[1] K. Nandakumar, Y. Chen, and A. K. Jain, "Biometric Authentication: Challenges and Future Trends," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1990-2001, Aug. 2020.
[2] P. Viola and M. Jones, "Robust Real-Time Face Detection," International Journal of Computer Vision, vol. 57, no. 2, pp. 137-154, May 2004.
[3] S. Furui, "Recent Advances in Speaker Recognition," Pattern Recognition Letters, vol. 18, no. 9, pp. 859-872, Sep. 1997.
[4] A. Al-Haj, "Fast and Secure AES Encryption Algorithm for Image Transmission," International Journal of Electrical & Computer Engineering, vol. 3, no. 2, pp. 107-115, Apr. 2013.
[5] J. L. Dugelay and M. Nixon, "Recent Advances in Biometric Security," IEEE Signal Processing Magazine, vol. 24, no. 6, pp. 50-52, Nov. 2007.
[6] C. Rathgeb and A. Uhl, "A Survey on Biometric Cryptosystems and Cancelable Biometrics," EURASIP Journal on Information Security, vol. 2011, no. 3, pp. 1-25, Mar. 2011.
[7] S. Marcel, C. McCool, and P. Matejka, "On the Effectiveness of Biometric Liveness Detection," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 1, no. 2, pp. 181-191, June 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details