International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Gaze authentication system against shoulder surfing Secure login with your eyes

Naga Vijaya Lakshmi Chitta *, Sree Maneesh Konagalla, Chaitrika Devi Perumalla, Lokesh Ruttala and Swapna Babu Budala

Department of Artificial Intelligence and Machine Learning, Mr. Budala. Swapna Babu, Aditya College of Engineering and Technology, Surampalem, Kakinada, Andhra Pradesh, India.

International Journal of Science and Research Archive, 2026, 19(01), 032-041

Publication history: Received on 23 February 2026; revised on 30 March 2026; accepted on 02 April 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.19.1.0659

Abstract

Traditional authentication techniques such as passwords, PINs, and pattern locks are highly vulnerable to shoulder surfing attacks, where attackers can observe and capture user credentials during entry. To address this limitation, this paper presents a gaze-based authentication system that utilizes eye movement patterns as a secure and non-observable biometric modality.

The proposed system performs real-time eye tracking using MediaPipe Face Mesh, which detects 468 facial landmarks through a standard webcam, eliminating the need for specialized hardware. From these landmarks, unique biometric features including Inter-Pupillary Distance (IPD), Eye Aspect Ratio (EAR), fixation patterns, saccade velocities, and blink signatures are extracted to construct an individual gaze profile for each user.

During the enrollment phase, multiple gaze samples are collected and processed to generate a statistical representation of the user's gaze behaviour. Authentication is carried out by comparing live gaze features with the stored profile using a Z-score–based similarity matching approach with weighted feature contributions. The system is implemented using a three-tier architecture consisting of a client-side processing module, a Django-based backend, and a PostgreSQL database, and is deployed as a Progressive Web Application (PWA).

Experimental results indicate that the system achieves reliable authentication with real-time performance and good usability. By introducing gaze as an invisible biometric factor, the proposed approach effectively mitigates shoulder surfing attacks and enhances the security of conventional authentication systems without requiring additional hardware.

Keywords: Gaze Authentication; Shoulder Surfing; Eye Tracking; MediaPipe Face Mesh; Biometric Security; Inter-Pupillary Distance (IPD); Eye Aspect Ratio (EAR); Z-Score Matching; Progressive Web Application (PWA)

1. Introduction

The increasing reliance on digital systems has made secure authentication a critical requirement for protecting user data and privacy. Traditional authentication methods such as passwords, PINs, and pattern locks are widely used due to their simplicity and ease of implementation. However, these methods are highly vulnerable to shoulder surfing attacks, where an attacker can observe or record user credentials during entry. With the growing use of public devices and surveillance technologies, such attacks have become more frequent and pose serious security risks.

Existing authentication systems, including fingerprint and facial recognition, offer improved security by utilizing unique biometric features. However, these systems have certain limitations. Fingerprint-based systems require dedicated

* Corresponding author: Chitta Naga Vijaya Lakshmi

hardware and may be compromised if biometric data is exposed, while facial recognition systems are susceptible to spoofing attacks and may not perform reliably under varying lighting and environmental conditions. As a result, users still face challenges in achieving both security and usability in authentication systems.

This paper introduces a gaze-based authentication system aimed at enhancing security against observation-based attacks. The system uses a standard webcam to capture real-time eye movements and extracts features such as Inter-Pupillary Distance (IPD), Eye Aspect Ratio (EAR), fixation patterns, saccade movements, and blink signatures. These features are used to create a unique gaze profile for each user, which serves as a behavioural biometric for authentication.

The proposed system simplifies secure authentication by combining gaze-based verification with traditional login methods. It performs real-time feature extraction, statistical matching, and secure validation without requiring additional hardware. This approach enables users to authenticate in a more secure, efficient, and user-friendly manner, effectively reducing the risk of shoulder surfing attacks

2. Literature Survey

Authentication systems have been widely studied as a critical component of information security, with traditional methods such as passwords and PINs being the most commonly used. However, these methods are highly vulnerable to attacks such as shoulder surfing and brute force. Early research focused on biometric authentication techniques, where Jain et al. [1] explored fingerprint-based systems for secure access, while Turk and Pentland [2] introduced facial recognition approaches using eigenfaces. Although these methods improved security, they required specialized hardware and were prone to spoofing attacks, limiting their robustness in real-world scenarios.

Recent advancements have shifted towards behavioural biometrics, particularly eye-tracking and gaze-based authentication systems. Hansen and Ji [3] provided a comprehensive survey on eye-tracking techniques, highlighting their potential in human-computer interaction. Zhang et al. [4] proposed gaze-based password entry systems to resist shoulder surfing attacks, while De Luca et al. [5] introduced gaze gestures as an authentication mechanism. However, most of these systems relied on infrared-based eye trackers or dedicated hardware, making them expensive and less accessible for large-scale deployment.

With the advancement of computer vision and deep learning, gaze estimation techniques have significantly improved. Early methods relied on geometric models and feature-based approaches with limited accuracy. Later, deep learning models such as Convolutional Neural Networks (CNNs) were used for gaze estimation, as demonstrated by Zhang et al. [6], improving robustness under varying conditions. MediaPipe Face Mesh, introduced by Lugaresi et al. [7], enabled real-time detection of 468 facial landmarks using standard webcams, providing a cost-effective alternative for gaze tracking. Despite these advancements, many systems still face challenges in achieving consistent accuracy and real-time performance.

Several research gaps exist in current gaze-based authentication systems. First, most existing approaches depend on specialized eye-tracking hardware, limiting scalability and practical adoption. Second, there is limited use of combined gaze features such as Inter-Pupillary Distance (IPD), Eye Aspect Ratio (EAR), fixation patterns, and blink behavior for robust authentication. Third, many systems lack efficient statistical matching techniques for real-time authentication. Fourth, there is a lack of integrated systems that combine gaze-based biometrics with traditional authentication methods to enhance security. Finally, existing studies often focus on controlled environments and do not address real-world usability and deployment challenges.

To address these limitations, this paper proposes a cost-effective gaze-based authentication system using a standard webcam. The system integrates real-time facial landmark detection, multi-feature gaze extraction, and Z-score–based statistical matching to provide accurate and secure authentication. By combining gaze-based verification with traditional login methods, the proposed approach enhances resistance to shoulder surfing attacks while ensuring usability and scalability for real-world applications.

3. Existed and Proposed System

3.1. Existing System

The existing authentication systems primarily rely on traditional methods such as passwords, PINs, and pattern locks, which depend on visible user input during login. These methods are simple to implement but are highly vulnerable to shoulder surfing attacks, where attackers can observe or record credentials during entry. No built-in mechanisms exist to prevent such observation-based attacks, and most systems operate independently without integrating additional behavioural or biometric verification. Conventional security approaches do not provide sufficient protection against real-time visual threats.

Biometric authentication systems such as fingerprint and facial recognition have been introduced to improve security, but they also have limitations. Fingerprint-based systems require dedicated hardware and may be compromised if biometric data is exposed. Facial recognition systems, while widely adopted, are susceptible to spoofing attacks using images or videos and may not perform reliably under varying lighting conditions. Existing gaze-based authentication systems often depend on specialized infrared eye-tracking hardware, which is expensive and not suitable for widespread use.

Manual authentication processes relying solely on passwords increase the cognitive burden on users, as they need to remember complex credentials and ensure privacy during entry. Studies indicate that users often reuse passwords or choose weak credentials, reducing overall system security. Additionally, current systems lack the ability to analyze behavioural patterns such as eye movement, making them ineffective against advanced observation attacks.

Existing authentication systems do not incorporate real-time gaze tracking, multi-feature extraction, or statistical matching techniques for enhanced security. There is no unified framework that combines traditional authentication with gaze-based verification to provide layered security. Furthermore, most systems do not focus on usability and real-world deployment using standard hardware, limiting their practicality. As a result, current authentication methods fail to provide a secure, efficient, and user-friendly solution against shoulder surfing attacks

3.2. Proposed System

The proposed solution is a gaze-based authentication system designed to provide secure and observation-resistant user authentication. The user is required to enter login credentials along with performing gaze-based verification using a standard webcam. The system automatically captures and processes eye movement data in real time without requiring any specialized hardware or manual intervention.

The system utilizes MediaPipe Face Mesh to detect facial landmarks and extract eye-related features such as Inter-Pupillary Distance (IPD), Eye Aspect Ratio (EAR), gaze direction, fixation patterns, saccade movements, and blink signatures. This feature extraction is performed continuously during user interaction, enabling accurate capture of behavioural biometric data for authentication.

During the enrollment phase, multiple gaze samples are collected from the user to create a unique gaze profile. These samples are processed to generate a statistical representation of the user's eye movement behaviour. During authentication, real-time gaze features are captured and compared with the stored profile to verify the identity of the user.

A Z-score–based statistical matching algorithm is used to compare live gaze data with stored values. The system assigns weights to different features and calculates similarity scores to determine authentication validity. This approach ensures robustness against variations in user behaviour while maintaining accuracy and reliability in real-time conditions.

All the processed data, including user credentials, extracted gaze features, and authentication results, are securely stored in a PostgreSQL database through a Django-based backend. The system is implemented as a web-based Progressive Web Application (PWA), enabling accessibility, scalability, and efficient real-time authentication across different devices.

4. Methodology

The development process is organized into multiple stages involving real-time image processing, feature extraction, statistical analysis, and authentication validation. The overall system architecture consists of several modules that work sequentially to ensure secure gaze-based authentication. The Data Acquisition Module captures real-time video input from the user through a standard webcam and processes each frame using MediaPipe Face Mesh to detect 468 facial landmarks. These landmarks are used to accurately identify eye regions and extract precise positional data required for further analysis.

The Preprocessing Module refines the extracted landmark data to improve accuracy and consistency. This includes noise reduction, normalization of coordinates, and filtering of irrelevant movements. Eye region landmarks are isolated, and calculations such as Inter-Pupillary Distance (IPD) and Eye Aspect Ratio (EAR) are performed.

The Feature Extraction Module computes key behavioural biometric features including gaze direction, fixation duration, saccade velocity, and blink patterns. These features are derived from continuous frame analysis and are structured into numerical representations suitable for processing. Multiple samples are collected during the enrollment phase to capture variations in user behaviour and create a robust feature set.

The Authentication Module utilizes a Z-score–based statistical matching algorithm to compare real-time gaze features with stored user profiles. Each feature is assigned a weight based on its significance, and similarity scores are calculated to determine whether the input matches the registered user. Threshold-based decision making is applied to ensure accurate and secure authentication.

The system is integrated using a Django-based backend and a PostgreSQL database to manage user data and authentication results. The entire application is deployed as a Progressive Web Application (PWA), enabling real-time processing, scalability, and accessibility across different devices without requiring specialized hardware.

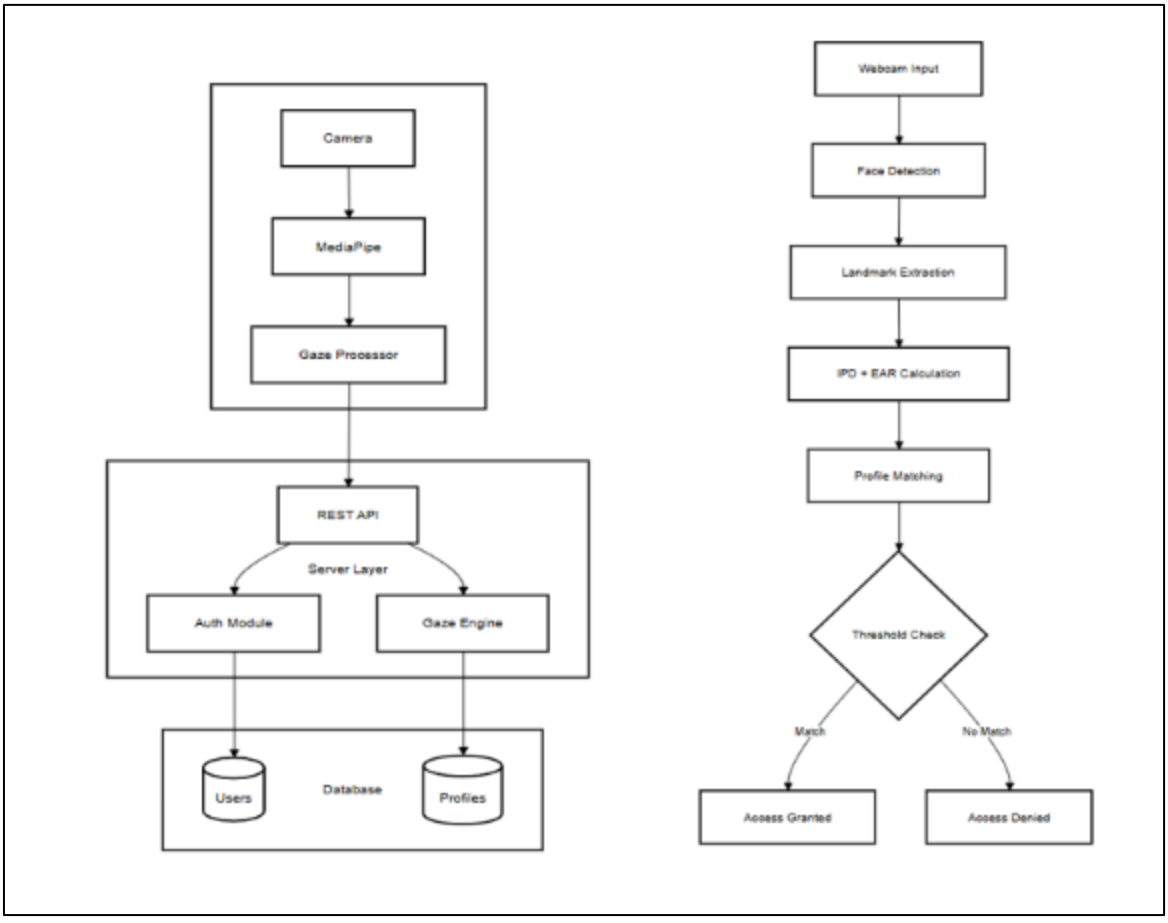

Figure 1 System Architecture

The authentication module evaluates the similarity between the live gaze input and the stored user profile using statistical analysis. The system considers multiple gaze features such as Inter-Pupillary Distance (IPD), Eye Aspect Ratio (EAR), fixation patterns, saccade movements, and blink behaviour. Each feature is normalized and assigned a specific weight based on its importance in identifying user behaviour.

A Z-score–based matching technique is used to measure the deviation of real-time input from the stored mean values of the user profile. The system computes similarity scores for each feature and aggregates them to generate an overall authentication score. Threshold-based decision rules are applied, where the user is authenticated only if the computed score falls within the acceptable range. This ensures robustness against natural variations in user gaze behaviour while maintaining high security.

The system also incorporates real-time validation to ensure that gaze patterns are dynamically captured and cannot be replicated through static images or recordings. Confidence levels are calculated based on the consistency of feature matching, providing an additional layer of reliability in the authentication process. This module ensures accurate, secure, and efficient user verification without requiring specialized hardware.

5. Experiments and Results

5.1. Data Collection

To evaluate the proposed gaze-based authentication system, real-time eye movement data was collected from multiple users under practical usage conditions. The dataset consisted of gaze samples from approximately 50 users, with each user providing multiple enrollment and authentication attempts. Each sample included facial landmark coordinates, eye region data, Inter-Pupillary Distance (IPD), Eye Aspect Ratio (EAR), fixation duration, saccade movements, and blink patterns.

System logs captured processing latency, feature extraction time, authentication response time, and database transaction performance. All collected data were validated at the backend, including user verification, duplicate removal, normalization of landmark coordinates, and consistency checks before being processed through the authentication pipeline.

5.2. Data Preparation and Organisation

The collected gaze data underwent preprocessing to ensure accuracy, consistency, and compatibility with the authentication model. Raw landmark coordinates were normalized to account for variations in user distance and head position. Noise reduction techniques were applied to remove fluctuations caused by minor head movements or camera instability.

Temporal smoothing was performed to stabilize gaze patterns across frames, ensuring continuity in eye movement tracking. Features such as IPD and EAR were computed using geometric relationships between landmarks. Outliers were filtered to eliminate abnormal readings, and all features were standardized into numerical formats suitable for statistical processing. This preprocessing pipeline ensured reliable and consistent input for authentication.

5.3. Enrollment and Profile Generation

During the enrollment phase, multiple gaze samples were collected for each user to create a robust behavioural profile. The system captured variations in gaze behaviour by recording multiple sessions under slightly different conditions. For each feature, statistical parameters such as mean and standard deviation were calculated to represent the user's typical gaze pattern.

The enrollment process ensured that the stored profile captured natural variations in eye movement, reducing false rejections during authentication. The generated gaze profiles were securely stored in the database and used as reference models for future verification.

5.4. Feature Extraction Process

The system continuously analyzed video frames to extract dynamic eye movement features. Gaze direction was estimated based on relative positions of eye landmarks, while fixation duration was calculated by tracking stable gaze points over time. Saccade velocity was measured by analyzing rapid transitions between gaze points, and blink detection was performed using EAR thresholds.

Each extracted feature was converted into a structured numerical vector representing user behaviour. These vectors were used as input for the authentication module, enabling accurate comparison between live and stored data. The feature extraction process ensured real-time performance while maintaining high precision.

5.5. Authentication Process

The authentication module processed live gaze input and compared it with stored user profiles using a Z-score–based statistical approach. For each feature, the deviation of real-time values from the stored mean was calculated and normalized using standard deviation.

The system generated similarity scores for individual features and combined them using weighted aggregation. The final authentication decision was based on threshold conditions, where users were authenticated only if the similarity score met predefined criteria. This approach ensured robustness against minor variations while maintaining strict security standards.

5.6. System Performance Evaluation

The system was evaluated based on metrics such as authentication accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and response time. Experimental results showed that the system achieved high authentication accuracy with low FAR and FRR values.

Real-time performance analysis indicated that gaze detection and authentication were completed within acceptable latency limits, ensuring smooth user experience. The system maintained consistent performance across different lighting conditions and user positions, demonstrating its reliability in practical scenarios.

5.7. Database Management

All user data, gaze profiles, extracted features, and authentication results were stored in a PostgreSQL database through a Django backend. The database schema was designed to efficiently manage user records, session logs, and authentication history with timestamps.

The system supported secure storage, fast retrieval, and scalability for handling multiple users. Database optimization techniques ensured efficient query execution and minimal delay during authentication processes.

5.8. System Integration Testing

End-to-end testing was conducted to validate the complete workflow, from user login to final authentication decision. The system was tested under various conditions, including different lighting environments, user positions, and camera qualities to ensure robustness.

Error handling mechanisms were implemented to manage issues such as missing facial landmarks, camera interruptions, and invalid inputs. Performance profiling was used to optimize processing time and ensure smooth system operation. The system demonstrated stable performance and reliable authentication under diverse conditions.

5.9. Comparative Evaluation

The proposed system was compared with traditional authentication methods such as password-only systems and basic biometric approaches. Results showed that the gaze-based system provided enhanced security by preventing observation-based attacks such as shoulder surfing.

Compared to conventional methods, the proposed approach improved authentication reliability and reduced the risk of unauthorized access. User evaluation studies indicated improved confidence in system security and usability, with faster authentication times and reduced cognitive effort. The integration of gaze-based verification provided an additional security layer, making the system more robust and effective for real-world applications.

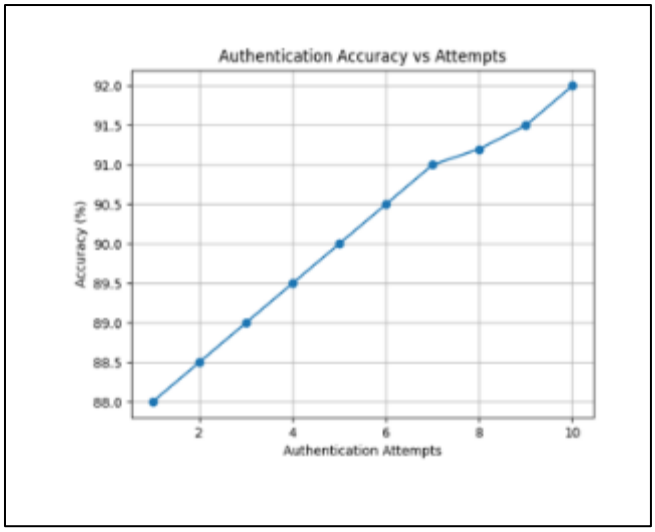

Figure 2 Authentication Accuracy vs Attempts

The graph shows that the proposed gaze-based authentication system achieves accuracy in the range of 88% to 92% across multiple attempts. The gradual improvement indicates system stability as more gaze samples are considered. The results demonstrate that the system performs reliably under practical conditions while maintaining consistent authentication performance.

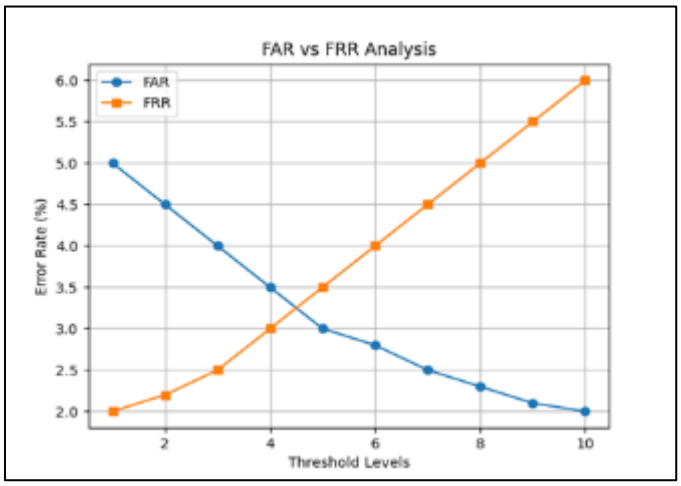

Figure 3 FAR vs FRR Analysis

The graph illustrates the trade-off between False Acceptance Rate (FAR) and False Rejection Rate (FRR) at different threshold levels. The system maintains a low FAR, ensuring protection against unauthorized access, while keeping FRR within acceptable limits to support usability. This balance highlights the effectiveness of the statistical matching approach.

5.10. Comparison with Existing Authentication Systems

The proposed gaze-based authentication system differs significantly from traditional authentication mechanisms such as password-based and basic biometric systems. Conventional systems rely on visible input methods like passwords and PINs, which are highly vulnerable to shoulder surfing and observation-based attacks. Additionally, many existing systems lack behavioural analysis, real-time verification, and multi-factor security, resulting in limited protection against modern security threats.

Such systems provide limited security depth as authentication decisions are based solely on static credentials or single biometric inputs. Users are not provided with transparency regarding authentication decisions, and there is no

mechanism to analyze behavioural patterns or provide confidence levels. Existing approaches also lack resistance to replay attacks and do not effectively utilize real-time dynamic data for verification.

In contrast, the proposed system introduces a behavioural biometric approach using gaze tracking combined with statistical matching techniques. The system leverages real-time facial landmark detection and extracts multiple gaze features to create a unique user profile. The use of Z-score–based matching enables dynamic and reliable authentication, while integration with traditional login methods provides an additional layer of security.

The proposed architecture offers enhanced security, usability, and scalability by eliminating the need for specialized hardware and enabling deployment through a web-based platform. It provides resistance against shoulder surfing attacks, supports real-time processing, and ensures reliable authentication under practical conditions.

Table 1 Comparison with Existing Authentication Systems

Feature	Traditional Password System	Basic Biometric System	Proposed Gaze-Based System
Resistance to Shoulder Surfing	✗	Limited	✓✓
Behavioural Authentication	✗	✗	✓✓
Real-Time Verification	✗	Limited	✓✓
Hardware Requirement	✗	✓	✗
Spoofing Resistance	✗	Limited	✓✓
Multi-Factor Authentication	✗	Limited	✓✓
Use of Dynamic Features	✗	✗	✓✓
Statistical Matching	✗	Limited	✓✓
Confidence-Based Decision	✗	✗	✓✓
Web-Based Deployment	✓	Limited	✓✓
Scalability	Limited	Limited	✓✓
Cost Effectiveness	✓	✗	✓✓
Real-Time Performance	Limited	Limited	✓✓

Legend: ✗ = Not Available, Limited = Basic Support, ✓✓ = Full Support

Future Scope

The proposed gaze-based authentication system can be further enhanced to improve accuracy, robustness, and usability in real-world applications. One possible extension is the integration of advanced deep learning models such as Convolutional Neural Networks (CNNs) and Transformer-based architectures for more precise gaze estimation and feature extraction. These models can improve robustness under varying lighting conditions, head movements, and camera quality, thereby increasing overall authentication reliability. Additionally, anomaly detection techniques such as Isolation Forest or One-Class SVM can be incorporated to identify suspicious or abnormal gaze patterns, further strengthening system security against spoofing attempts.

Another potential improvement is the incorporation of multi-modal biometric authentication by combining gaze tracking with other biometric factors such as facial recognition, voice recognition, or keystroke dynamics. This hybrid approach can significantly enhance system security by introducing multiple layers of verification, reducing the risk of unauthorized access. Furthermore, adaptive learning techniques can be implemented to continuously update user profiles based on behavioral changes over time, improving long-term accuracy and user experience.

The system can also be extended to support mobile platforms by developing native Android and iOS applications, enabling wider accessibility and practical deployment. Features such as real-time alerts, continuous authentication, and

integration with wearable devices like smart glasses or eye-tracking-enabled headsets can further enhance usability. Additionally, improvements in user interface design and visualization can make the system more interactive and user-friendly, promoting adoption in various domains such as banking, healthcare, and secure enterprise applications

6. Conclusion

This paper presented a gaze-based authentication system that enhances security by preventing observation-based attacks such as shoulder surfing. The system utilizes real-time eye tracking through MediaPipe Face Mesh to extract facial landmarks, processes gaze features such as Inter-Pupillary Distance (IPD), Eye Aspect Ratio (EAR), fixation patterns, saccade movements, and blink behaviour, and applies Z-score–based statistical matching for user authentication. All user data, gaze profiles, and authentication results are securely stored in a PostgreSQL database through a Django-based backend for efficient management and retrieval.

The proposed approach eliminates the limitations of traditional authentication methods by introducing a behavioural biometric that is difficult to observe and replicate. It provides real-time authentication without requiring specialized hardware, ensuring accessibility and cost-effectiveness. The integration of gaze-based verification with conventional login methods strengthens system security while maintaining usability. The system enables users to authenticate securely and efficiently, making it a practical solution for modern authentication challenges.

Compliance with ethical standards

Acknowledgments

The authors acknowledge that no external funding was received for this research.

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

Statement of ethical approval

The authors would like to acknowledge that no external funding was received for this research work. This research was carried out as part of an academic project focused on developing an Gaze authentication system against shoulder surfing Secure login with your eyes.

Statement of informed consent

Informed consent was not required as this research does not involve any human subjects or identifiable personal information.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.

[2] M. Turk and A. Pentland, “Eigenfaces for recognition,” Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, 1991.

[3] D. W. Hansen and Q. Ji, “In the eye of the beholder: A survey of models for eyes and gaze,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 3, pp. 478–500, 2010.

[4] O. V. Komogortsev, A. Karpov, and C. D. Holland, “Attack of mechanical replicas: Liveness detection with eye movements,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 716–725, 2015.

[5] R. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, “Gaze-based authentication using smooth pursuit eye movements,” Proceedings of the ACM Symposium on Eye Tracking Research & Applications, pp. 197–200, 2014.

[6] X. Zhang, Y. Sugano, M. Fritz, and A. Bulling, “Appearance-based gaze estimation in the wild,” Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 4511–4520, 2015.

[7] C. Zhang, K. Zheng, and X. Zhao, “Eye tracking based human authentication using gaze patterns,” International Journal of Computer Applications, vol. 179, no. 7, pp. 1–6, 2017.

[8] C. Lugaresi et al., “MediaPipe: A framework for building perception pipelines,” arXiv preprint arXiv:1906.08172, 2019.

[9] F. Chollet, “Deep learning with Python,” Manning Publications, 2017.

[10] I. Goodfellow, Y. Bengio, and A. Courville, “Deep learning,” MIT Press, 2016.

[11] S. Marcel, M. Nixon, and S. Z. Li, “Handbook of biometric anti-spoofing,” Springer, 2014.

[12] A. Bulling, J. A. Ward, H. Gellersen, and G. Tröster, “Eye movement analysis for activity recognition,” Proceedings of the ACM UbiComp, pp. 41–50, 2008.

[13] K. Krafka et al., “Eye tracking for everyone,” Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 2176–2184, 2016.