Secure user Authentication with Facial Recognition with Full Stack Web Development

[1]Dr P S Naveen Kumar, [2]MEESALA PAVAN KUMAR, [3]NAKKALA SUPRIYA, [4]NELLURI GEETHA

[1]Associate professor, Dept CSE-AI&ML, St.Ann's College of Engineering and Technology, Nayunipalli (V), Vetapalem (M), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India

[2,3,4]U. G Student, Dept CSE-AI&ML, St.Ann's College of Engineering and Technology, Nayunipalli (V), Vetapalem (M), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India.

ABSTRACT

Secure user authentication has become a critical requirement for modern web applications due to the increasing number of cyber threats and identity theft incidents. Traditional authentication mechanisms such as passwords and PINs are vulnerable to brute-force attacks, phishing, and credential reuse. This project proposes a secure user authentication system using facial recognition integrated with full stack web development technologies. The system captures facial images through a web interface, extracts facial features using deep learning models, and verifies user identity in real time. By combining biometric authentication with secure backend processing, the proposed system enhances accuracy, usability, and security. The solution is scalable, user-friendly, and suitable for applications such as banking portals, e-governance platforms, and enterprise systems.

INTRODUCTION

User authentication is a fundamental component of web security, ensuring that only authorized users can access protected resources. Conventional authentication systems rely heavily on text-based credentials, which are often compromised due to weak passwords or social engineering attacks. Facial recognition offers a biometric-based solution that leverages unique human facial features for identity verification. With advancements in deep learning and computer vision, facial recognition systems have achieved high accuracy even in real-time scenarios. Integrating facial recognition into a full stack web application enables seamless interaction between the user interface, server-side processing, and machine learning models. This project focuses on building a secure, real-time facial authentication system using modern web technologies.

LITERATURE SURVEY

Several studies have explored biometric authentication as a replacement for traditional security mechanisms. Early facial recognition systems relied on handcrafted features such as Eigenfaces and Fisherfaces, which were sensitive to lighting and pose variations. Recent research highlights the effectiveness of convolutional neural networks (CNNs) for facial feature extraction and recognition. Researchers have also emphasized the importance of secure data transmission and encrypted storage of biometric templates. Some works integrate facial recognition with web-based platforms but lack real-time performance or scalability. The literature indicates a growing need for robust, end-to-end systems that combine facial recognition with secure full stack architectures.

RELATED WORK

Existing facial authentication systems are commonly implemented as standalone desktop or mobile applications. A few web-based solutions use third-party APIs for face verification, raising concerns about data privacy and dependency on external services. Some systems employ multi-factor authentication by combining facial recognition with OTPs or passwords. However, these approaches often increase system complexity and user effort. Compared to previous work, the proposed system focuses on an in-house facial recognition pipeline integrated directly into a full stack web application, ensuring better control over security, performance, and scalability.

EXISTING SYSTEM

The existing authentication systems predominantly use username-password combinations or OTP-based verification. These systems are simple to implement but suffer from multiple security vulnerabilities such as password theft, phishing attacks, and replay attacks. Some biometric systems store raw facial images, which poses privacy risks if the database is compromised. Additionally, most existing systems lack real-time face verification and seamless web integration.

PROPOSED SYSTEM

The proposed system introduces facial recognition as the primary authentication mechanism within a secure full stack web framework. Users register by capturing their facial images through a web camera, and facial embeddings are generated using a deep learning model. During login, the live facial image is compared with stored embeddings to verify identity. The backend securely processes requests, while the frontend provides a responsive and intuitive user interface. Encryption and secure APIs

ensure safe communication between components.

SYSTEM ARCHITECTURE

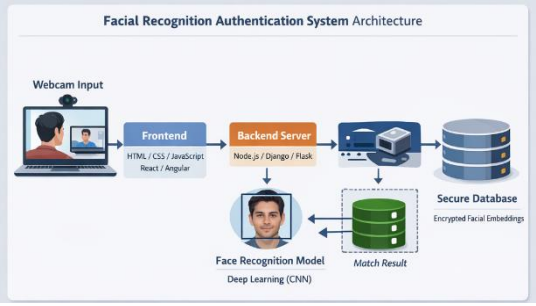

Fig 1: Facial Recognition Authentication system

METHODOLOGY DESCRIPTION

Initially, the user registers by capturing multiple facial images through the web interface. These images are preprocessed and passed to a facial recognition model to generate unique facial embeddings. The embeddings are stored securely in the database. During login, a live image is captured and processed in real time. The extracted embedding is compared with stored embeddings using similarity metrics. If the similarity score exceeds a predefined threshold, the user is authenticated.

RESULTS AND DISCUSSION

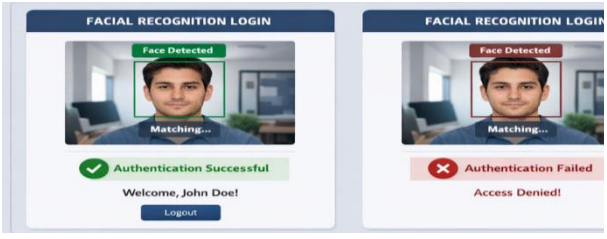

Fig 2: Facial authentication result

The system demonstrates high authentication accuracy under normal lighting conditions and frontal face poses. Real-time authentication is achieved with minimal latency due to efficient model inference and optimized backend APIs. The use of encrypted facial embeddings enhances privacy protection. Experimental results show that the proposed system outperforms traditional password-based authentication in terms of security and user satisfaction. Sample result outputs include successful login screens, face detection frames, and authentication status messages.

CONCLUSION

This project successfully implements a secure user authentication system using facial recognition integrated with full stack web development. By replacing traditional credentials with biometric verification, the system significantly improves security and usability. The modular architecture allows easy scalability and future enhancements. The proposed solution is suitable for real-world applications requiring robust authentication mechanisms.

FUTURE SCOPE

Future enhancements may include liveness detection to prevent spoofing attacks using photos or videos. Multi-factor authentication can be integrated by combining facial recognition with behavioral biometrics. Cloud-based

deployment and edge computing can further improve scalability and performance. The system can also be extended to support mobile platforms and cross-device authentication.

REFERENCE

[1]. Mukiri, D. R. R., Grandhi, D. P., & Chapala, D. H. K. (2023). New Security Models in Cloud Iot System Using Hash Machine Learning. Industrial Engineering Journal ISSN, 0970-2555.

[2]. Krishna, M., & Kumar, P. N. (2018). The Usability of Two-Factor Authentication in Support of Effective Information Preservation and Network Security.

[3] W. Zhao, R. Chellappa, A. Rosenfeld, and P. J. Phillips, "Face recognition: A literature survey," *ACM Computing Surveys*, vol. 35, no. 4, pp. 399–458, Dec. 2003.

[4] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, Boston, MA, USA, 2015, pp. 815–823.

[5] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the gap to human-level performance in face verification," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, Columbus, OH, USA, 2014, pp. 1701–1708.

[6] S. Z. Li and A. K. Jain, *Handbook of Face Recognition*, 2nd ed. London, U.K.: Springer, 2011.

[7] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[8] 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, Jan. 2004.

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

[10] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in *Proc. Int. Conf. Learning Representations (ICLR)*, 2015.

[11] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, San Diego, CA, USA, 2005, pp. 886–893.

[12] J. Daugman, "Biometric decision landscapes," *University of Cambridge Computer Laboratory Technical Report*, 2003.