

Genuine Authentication: Centralized Infrastructure to Seamlessly Integrate Facial Recognition Capabilities into your Web Application

¹Santhosh M.; ²Naveen Prasad K.; ³Koshik Rishi M.; ⁴Jawaharsrinath M.N.
Department of Computer Science and Engineering, SNS College of Engineering,
Coimbatore-641035, Tamil Nadu, India

Abstract:- As cyberattacks grow in complexity, traditional authentication systems face increasing vulnerabilities. Generative Authentication offers a robust solution by integrating facial recognition as a secondary security layer. This paper discusses the implementation of a micro SaaS tool enabling businesses to adopt this technology through APIs. Testing has shown a marked improvement in access security and user satisfaction while maintaining cost-efficiency. By addressing critical issues in token-based authentication, Generative Authentication ensures a scalable, resilient framework for secure access.

Keywords:- Biometric Security, Facial Recognition, Generative Authentication, SaaS, Cybersecurity, Token Vulnerabilities, API Integration, Liveness Detection, Authentication Systems.

I. INTRODUCTION

The rise of digital services has increased the reliance on web applications for everyday operations, exposing sensitive user data to an array of sophisticated cyber threats. Authentication mechanisms, including OAuth and JSON Web Tokens (JWTs), have become the backbone of secure communication between users and servers. However, these systems are susceptible to vulnerabilities, such as token theft via browser exploitation or cross-site scripting (XSS). Generative Authentication introduces facial recognition as a biometric layer, addressing gaps in conventional methods. By requiring real-time user verification, this approach strengthens security even in scenarios where tokens are compromised. This paper presents the development of a scalable micro SaaS platform, allowing businesses to integrate facial recognition into their authentication flows. The tool aims to provide accessible, cost-effective security solutions for organizations of all sizes.

II. MATERIALS AND METHODS

A. Design Thinking Approach

The following stages were implemented to ensure the platform addressed real-world authentication challenges effectively:

➤ Empathy

To understand the challenges faced by end-users, surveys and interviews were conducted:

- Users: Expressed concerns over stolen tokens and cumbersome password systems.
- Administrators: Highlighted the complexity of implementing advanced security without affecting user experience.

➤ Define

Key requirements identified include:

- Seamless API integration for facial recognition.
- Real-time liveness detection to prevent spoofing.

➤ Ideate

Brainstorming sessions led to the development of:

- A micro SaaS platform supporting plug-and-play facial recognition.
- Tools for token verification and biometric authentication.

➤ Prototype

An initial prototype featured:

- A facial recognition engine leveraging AI and machine learning.
- API endpoints for authentication integration.
- Liveness detection capabilities to counter spoofing.

B. Technical Architecture

The architecture employs: Frontend: React.js for dynamic user interfaces. Backend: Node.js with Express.js for API handling. Database: MongoDB for secure storage of biometric templates. Cloud Integration: AWS for scalable processing.

III. RESULTS

A. System Performance

- Accuracy: False acceptance rate (FAR) reduced to 0.2%.
- Speed: Average verification time of 2.3 seconds.

B. User Feedback

- 90% of participants reported increased trust in system security.
- Administrators noted a 40% reduction in unauthorized access incidents.

C. Scalability

The tool handled up to 15,000 concurrent authentication requests during stress testing, showcasing readiness for large-scale deployments.

IV. DISCUSSIONS

Generative Authentication bridges the gap between user convenience and security. Its implementation addresses key vulnerabilities of token-based systems while providing a scalable and user-friendly solution. However, challenges such as user onboarding and privacy concerns require ongoing refinement. Future iterations will focus on expanding biometric modalities and enhancing data privacy mechanisms.

V. CONCLUSIONS

Generative Authentication represents a significant leap in cybersecurity, combining traditional methods with biometric innovation. The micro SaaS platform ensures cost-effective deployment, empowering organizations to adopt robust security measures without disrupting workflows. Future developments will explore integration with multi-factor authentication systems and deployment in high-security industries like healthcare and finance.

REFERENCES

- [1]. Bajpai S, Singh A and Karthik KV 2013 An experimental comparison of face detection algorithms Int J Computer Theory and Engineering 5 p 47
- [2]. Rath SK and Rautaray SS 2014 A survey on face detection and recognition techniques in different application domains Int J Modern Education and Computer Science 6 p 34.
- [3]. Chandrapala DN, Akshay G and Ravishankar M 2012 Face detection using a boosted cascade of features using OpenCV Int Conf Information Processing (Springer, Berlin, Heidelberg) pp 399-404
- [4]. Mori K, Masutani M and Suzuki T 2005 Face recognition using SVM fed with intermediate output of CNN for face detection MWA pp 406-113
- [5]. Ma S and Du T 2010 Improved Adaboost face detection Int Conf Measuring Technology and Mechatronics Automation (IEEE) 2 pp 434-37
- [6]. Cümezi L, Zhuqing Q, Nan J and Jinmab W 2017 Human face detection algorithm via Haar cascade classifier combined with three additional classifiers 3rd IEEE Int Conf Electronic Measurement & Instruments (ICEMI) pp 483-87
- [7]. Zhou H, Chen P and Shen W 2017 A multi-view face recognition system based on cascade face detector and improved Dlib MIPPR 2017: Pattern Recognition and Computer Vision 2018 (International Society for Optics and Photonics) 10609 p 1060908
- [8]. Cerna LR, Camara-Chavez G and Menotti D 2013 Face detection: Histogram of oriented gradients and bag of feature method Proc Int Conf Image Processing, Computer Vision, and Pattern Recognition (WorldComp I)
- [9]. Shavers C, Li R and Lekberg G 2006 An SVM-based approach to face detection Proc 38th Southeastern Symposium on System Theory (IEEE) pp 362-66
- [10]. Zhang K, Zhang Z, Li Z and Qiao Y 2016 Joint face detection and alignment using multitask cascaded convolutional networks IEEE Signal Processing Letters 23 pp 1499-503