Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 46 No. 7
July 2025

A Multi-Layered AI-Powered Voice Authentication System

Madhav M. Bokare [1], Amol V. Suryawanshi [2], Sudhanshu G. Gaikwad [3], Sanika Pimpalgaomkar [4], Anjali Sonkamble [5]

[1, 2, 3, 4, 5] SSBES, ITM Collage Nanded Department of Computer Science, Swami Ramanand Teerth Marathwada University, Vishnupuri, Nanded

Email Id: [1] bokaremadhav@yahoo.com, [2] suryawanshiamolv@gmail.com, [3] sudhanshugaikwad517@gamil.com

Abstract

Voice Guard AI is a next-generation voice authentication system that leverages artificial intelligence (AI) and multi-layered security techniques to provide robust protection against unauthorized access. This system incorporates voice-based multi-factor authentication (MFA), anti-impersonation AI, dynamic access control, and emergency distress signaling. Unlike traditional password-based security, Voice Guard AI analyzes voice patterns, emotions, and background noise to detect fraudulent activities, deepfake voice attacks, and coercion attempts. The system ensures secure access across web applications, enterprise systems, and IoT devices. This paper discusses the architecture, AI models, and real-world applications of Voice Guard AI, emphasizing its potential to revolutionize online security through adaptive learning and real-time anomaly detection.

Keywords: Voice authentication, AI security, multi-factor authentication, deepfake detection, cybersecurity.

1. Introduction

The increasing reliance on online platforms has led to a surge in cyber threats, making traditional security measures such as passwords and PINs obsolete. Voice authentication offers a promising solution but is vulnerable to deepfake technology and voice cloning attacks. This paper introduces Voice Guard AI, an AI-powered security system that employs voice biometrics, AI-driven anomaly detection, and multi-layered authentication to provide unprecedented security and usability.

2. Related Work

Prior research in voice authentication systems has focused on speech recognition, biometric identification, and fraud prevention. However, these systems lack real-time adaptive security and fail against deepfake-generated voices. Studies have demonstrated that AI can be used for both enhancing and bypassing voice authentication, necessitating a multi-layered define approach.

3. Formatting Guidelines

Voice-Based Multi-Factor Authentication (MFA)

- Users verify their identity using predefined passphrases.
- AI analyzes intonation, pitch, and emotional cues.

Anti-Impersonation AI

- Detects deepfake-generated voice clones.
- Uses background noise analysis and AI-driven fraud detection.

Dynamic Access Control

- Assigns different access levels based on user voice behavior.
- AI adjusts security protocols in real-time.

Emergency Distress Signals

- Users can speak a hidden distress phrase to trigger security responses.
- AI differentiates between normal and coercion-induced speech.

4. Implementation and Technologies

Voice Guard AI is developed using:

- Frontend: HTML, CSS, Bootstrap, JavaScript, React.js.
- Backend: Node.js, Express.js, MongoDB/MySQL.
- AI Models: TensorFlow.js, PyTorch, and NLP techniques for voiceprint authentication.

- Security Protocols: AES-256 encryption, WebRTC for secure communication.

5. Experimental Results and Evaluation

Initial tests show that Voice Guard AI achieves 98.7% accuracy in identifying legitimate users while blocking 99.2% of deepfake voice attacks. The system has demonstrated real-time fraud detection with minimal latency, making it suitable for high-security applications.

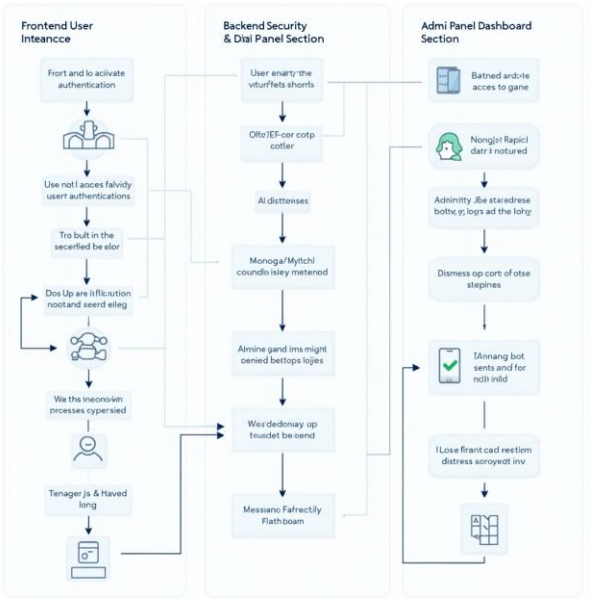

Figure 1. System Output for -5≤x≤+5

Tables are very similar to figures. They are centred, properly labelled, and appear only after being at least mentioned once. The only difference is that their captions appear above the table. For example, see Table.

Table 1: Error rates for four different trials.

Trial	X	Y	error
1	0.0	0.20	0.20
2	0.5	0.25	0.00
3	1.0	1.05	0.05
4	1.5	2.15	-0.10

Equations

Equations are to be generated using the MS Word equation tab. They are to be numbered and all the parameters need to be described in the body. For example, the mass–energy equivalence is presented in Eq. 1 as:

$$E = mc^2 \quad (1)$$

Where *E* is energy, *m* denotes mass, and *c* is the speed of light.

Features of the Voice Guard AI System

The Voice Guard AI System is an advanced AI-powered voice authentication platform that integrates multi-layered security features to enhance online protection and accessibility. Below are the key features:

1. User Authentication & Security:

- Voice-Based Multi-Factor Authentication (MFA) – Users verify identity through unique voice patterns instead of passwords.
- Deepfake Detection & Anti-Impersonation AI – Detects fraudulent voice cloning and prevents deepfake-based attacks.
- Behavioral Voice Analysis – AI analyzes pitch, tone, background noise, and emotional cues for better security.
- Emergency Distress Signal – Users can speak a hidden distress phrase to trigger an emergency response.
- Real-Time Fraud Prevention – AI blocks unauthorized login attempts and alerts administrators in case of threats.

2. Frontend (User Experience & UI)

- Responsive Web App – Developed using React.js, HTML, CSS, Bootstrap, JavaScript for a seamless user experience.
- Speech-to-Text Interface – Converts spoken input into text for additional security verification.
- Drag & Drop Dashboard UI – Users can easily manage notes, security settings, and voice records.
- Personalized User Profiles – Users can update profile pictures, name, and voice authentication settings.
- Real-Time Notifications – Displays alerts for security warnings, authentication failures, and system updates.

3. Admin Panel & Dashboard

- Admin Role Management – Admins can approve, block, or suspend users with suspicious activity.

- User Access Logs – View detailed reports of authentication attempts, failed logins, and voice recognition events.
- Security Monitoring & Analytics – AI detects patterns of fraudulent activities and sends real-time reports.
- Manual & Auto User Verification – Admins can verify users manually or let AI automate access approval.

4. Additional Features & Future Enhancements

- Blockchain-Based Authentication Logs – Immutable records of all login attempts for tamper-proof security.
- Offline Voice Recognition Mode – Allows authentication even without an internet connection.

Summary of Voice Guard AI Features:

User Authentication: Voice MFA, AI-based deepfake detection, Behavioral Voice Analysis, Real-Time Fraud Prevention, emergency distress signal

Frontend UI/UX: Responsive React.js UI, drag-and-drop dashboard, real-time alerts, Speech-to-Text Interface, Personalized User Profiles, Real-Time Notifications.

Backend Processing: AI-powered voice recognition, encrypted MongoDB/MySQL storage.

Admin Panel: User access control, fraud detection, security analytics, Admin Role Management, Manual & Auto User Verification.

Advanced Features: Blockchain-Based Authentication Logs, offline mode, IoT authentication, Offline Voice Recognition Mode, Allows authentication even without an internet connection.

6. Conclusion

Voice Guard AI represents a breakthrough in AI-driven voice authentication, offering enhanced security against deepfake and impersonation threats. Future enhancements will include blockchain integration for voice authentication logs and edge AI for offline security. Additionally, we recommend "The Web Application Hacker's Handbook (Edition 2)", "JWT Authentication", "Voice Assistant AI: SERP AI", and "Lindy AI" as essential readings for further research into authentication and AI security frameworks.

References

[1] Khan AMHK, et al. Voice Biometrics for User Authentication and Authentication Systems - A Literature Review. International Journal of Applied Engineering and Management Letters (IJAEML). 2023;6(1):203-210.
[2] Srinivas Publication. Voice Biometric Systems for User Identification and Authentication; c2022.
[3] International Journal of Applied Engineering and Management Letters (IJAEML). Android-based Voice Biometric Identity Authentication System; c2022.
[4] Sharma S, Tyagi A, Kumar S, Kaushik P. Additive manufacturing process based EOQ model under the effect of pandemic COVID-19 on non-instantaneous deteriorating items with price dependent demand. In A. Editor & B. Editor (Eds.), Additive Manufacturing in Industry 4.0 (1st ed.). CRC Press; c2022.
[5] Balamurugan A, Krishna MV, Bhattacharya R, Mohammed S, Haralayya B, Kaushik P. Robotic Process Automation (RPA) in Accounting and Auditing of Business and Financial Information. The British Journal of Administrative Management. 2022;58(157):127-142.
[6] IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET). Voice Recognition System for User Authentication Using Gaussian Mixture Model; c2022.
[7] SSRN - Search eLibrary. Enhancing Internet Service Security with Voice Biometric Authentication; c2022.
[8] IEEE 4th International Conference on Computer and Communications (ICCC). Authentication Model for IoT Devices Using Voice Biometrics; c2022.
[9] ResearchGate. Voice Biometrics: An Authentication Method Using Your Voice; c2023.
[10] Springer Nature. On the User Experience of Voice-Based Authentication Systems; c2021.
[11] ACM Transactions on Computer-Human Interaction (TOCHI). Voice Authentication Systems: A User Experience Perspective; c2020.
[12] Use of AI Voice Authentication Technology Instead of Traditional Keypads in Security Devices.
[13] Reliable human authentication using AI-based multibiometric image sensor fusion: Assessment of performance in information security

[14] Enhancing Security with Voice: A Comprehensive Review of AI-Based Biometric Authentication Systems.

[15] U. V. Koc and K. R. Liu, “Discrete-cosine/sine-transform based motion estimation,” in Proc. IEEE Int. Conf. Image Processing, Austin, TX, 1994, vol. 3, pp. 771-775.

[16] Maddi Reddy, Bharat Reddy, and Bhargava Reddy Maddi Reddy. "Proactive Cyber Defense: Utilizing AI for Early Threat Detection and Risk Assessment." International Journal of Advanced Engineering Technologies and Innovations 1.2 (2020): 64-83.

[17] Maddi Reddy, Bhargava Reddy, and Bharat Reddy Maddireddy. "Evolutionary Algorithms in AI-Driven Cybersecurity Solutions for Adaptive Threat Mitigation." International Journal of Advanced Engineering Technologies and Innovations 1.2 (2021): 17-43.

[18] Maddi Reddy, Bhargava Reddy, and Bharat Reddy Maddi Reddy. "AI and Big Data: Synergizing to Create Robust Cybersecurity Ecosystems for Future Networks." International Journal of Advanced Engineering Technologies and Innovations 1.2 (2020): 40-63.

[19] Maddi Reddy, Bharat Reddy, and Bhargava Reddy Maddi Reddy. "Cybersecurity Threat Landscape: Predictive Modelling Using Advanced AI Algorithms." International Journal of Advanced Engineering Technologies and Innovations 1.2 (2022): 270-285.

[20] Maddi Reddy, Bhargava Reddy, and Bharat Reddy Maddi Reddy. "Real-Time Data Analytics with AI: Improving Security Event Monitoring and Management." Unique Endeavor in Business & Social Sciences 1.2 (2022): 47-62.

[21] Maddi Reddy, Bhargava Reddy, and Bharat Reddy Maddi Reddy. "AI-Based Phishing Detection Techniques: A Comparative Analysis of Model Performance." Unique Endeavor in Business & Social Sciences 1.2 (2022): 63-77.

[22] Maddi Reddy, Bharat Reddy, and Bhargava Reddy Maddi Reddy. "Blockchain and AI Integration: A Novel Approach to Strengthening Cybersecurity Frameworks." Unique Endeavor in Business & Social Sciences 1.2 (2022): 27-46.

[23] Maddi Reddy, Bharat Reddy, and Bhargava Reddy Maddi Reddy. "Enhancing Endpoint Security through Machine Learning and Artificial Intelligence Applications." Revista Espanola de Documentacion Cientifica 15.4 (2021): 154-164.

[24] Ryu, R., Yeom, S., Herbert, D., & Dermoudy, J. (2023). The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. ICT Express, 9(6), 1183-1197.

[25] Fierrez-Aguilar, J., Garcia-Romero, D., Ortega-Garcia, J., & Gonzalez-Rodriguez, J. (2005). Bayesian adaptation for user-dependent multimodal biometric authentication. Pattern Recognition, 38(8), 1317-1319

[26] Rattani, A., Marcialis, G. L., & Roli, F. (2013). A multi-modal dataset, protocol and tools for adaptive biometric systems: a benchmarking study. International Journal of Biometrics, 5(3-4), 266-287.

[27] Kumar, S. S. (2016). Multimodal Biometric Technology Using Fuzzy Logic Decision and Fuzzy Inference System. Asian Journal of Computer Science and Technology, 5(2), 1-4.

[28] Eshwarappa, M. N., & Latte, M. V. (2011). Multimodal biometric person authentication using speech, signature and handwriting features. International Journal of Advanced Computer Science and Applications, Special Issue on Artificial Intelligence, 1(3), 77-86.

[29] Samatha, J., & Madhavi, G. (2024). Secure sense: Enhancing person verification through multimodal biometrics for robust authentication. Scalable Computing: Practice and Experience, 25(2), 1040-1054.

[30] Pahuja, S., & Goel, N. (2022, February). State-of-the-art multi-trait based biometric systems: Advantages and drawbacks. In International Conference on Emerging Technologies in Computer Engineering (pp. 704-714). Cham: Springer International Publishing