Cybersecurity and Innovative Technology Journal, Vol.3, No.2, 2025, pp. 54-57
e-ISSN 3025-6682. DOI: 10.53889/citj.v3i2.836

Artificial Intelligence Voice Cloning in Healthcare Cybersecurity: Challenges, Opportunities, and Protective Strategies

Submitted 31 December 2024, Revised 31 December 2025, Accepted 31 December 2025

William J. Triplett[1,2]*

[1]Department of Information Systems, Health Information Technology,
University of Maryland, Baltimore County, Baltimore, United States

[2]Department of Healthcare Technology, Cybersecurity Leadership,
Capitol Technology University, Laurel, United States
Corresponding Email: *wjtriplett@captechu.edu

Abstract

AI voice cloning has been one of the most transformative technologies in the health sector, improving patient-provider communication and enhancing operations in telehealth and remote monitoring. However, it comes with its own unique cybersecurity risks, including identity theft and unauthorized access. This paper focuses on the risks of cybersecurity threats in healthcare with relation to the use of AI voice cloning and assesses the efficiencies of current protective measures before proposing additional recommendations for enhanced security for data in the health sector. Based on mixed-method research, the study includes a systematic literature review and interviews with HCI and IT professionals, cybersecurity experts, and AI technology developers. It also accents current threats as well as possible solutions to the emerging vulnerabilities. The study shows that even though the use of AI for voice cloning has massive benefits, it creates significant security issues. These are: the use of voice phasing, unauthorized operations, and falsification of patient identity. The study calls for integrated security measures to fashion out secure AI systems, embrace enhanced modes of authentication, and conduct AI system check-ups frequently to avoid compromised voice cloning technology in healthcare.

Keywords: AI Voice Cloning, Healthcare Cybersecurity, Identity Theft, Voice Phishing, Patient Privacy

INTRODUCTION

AI voice cloning technology that imitates human voices with a very high accuracy is under more adoption in the healthcare sector for increasing patients' interactions and convenience (Genelza, 2024). Such uses include voice assistants, telemedicine talking-to and telemedicine counseling, and automatic follow-up alerts that enhance patient satisfaction as well as operational productivity. But it also means that while these advancements are made, the same technology can become a tool for cybercriminals, greatly jeopardizing the trust placed in healthcare systems.

Despite the benefits, AI voice cloning in healthcare has brought new security challenges into the healthcare sector, with few studies addressing these specific concerns (Genelza, 2024). Most of the past work discusses the moral and technical intricacies of AI but fails to provide a detailed discussion of the security vulnerabilities of voice cloning in the health care sector. This paper aims to help fill this gap by identifying the security risks associated with voice cloning in healthcare and providing protective measures.

The study's main objectives are as follows:

1. To systematically evaluate risks that threat actors might use AI voice cloning against healthcare, it is necessary to know what adversaries are likely to do with this new capability.

2. To assess the effectiveness of the various existing protective measures.
3. To offer recommendations that can help in eliminating all these risks and protecting healthcare data.

In addressing these objectives, the research seeks to offer guidance and best practices to healthcare decision-makers with the view to enhancing their protection of patient information and fortifying their AI voice cloning risks.

METHOD

Participants

Twenty participants were selected for this study, including:

1. **Healthcare IT Specialists:** Being familiar with the process of managing healthcare technologies, they shared valuable observations concerning the issues related to technology implementation from which the adoption of AI can be derived.
2. **Cybersecurity Analysts:** Experts in defending electronic healthcare organizations against cyber security risks brought in their views on possible risks.
3. **AI Technology Developers:** Software developers and engineers who are dealing with voice cloning AI, giving input regarding the AI device and its innovation alongside security.

Instruments

A semi-structured interview schedule was followed, which included AI voice cloning applications and cybersecurity and security measures in practice today. The interview questions were designed to provide a detailed description of the participants' experience with AI voice cloning, the types of vulnerabilities that involve AI voice cloning, and the participant's opinion on possible protection measures.

Data Collection

The interviews were accomplished by using the secure video calls; the interviews were recorded by obtaining participants' permission, and the recordings were transcribed. Primary data was collected from the IEEE Xplore, PubMed, Google Scholar, articles, case studies, and reports of related research of the last five years on the themes of AI voice cloning and cybersecurity.

Data Analysis

Thematic analysis was applied to determine the key threats posed by voice cloning and methods of protection. Software for conducting qualitative analysis helped to code the source material, which helped the identification of some of the greater themes such as 'voice phishing', 'identity theft', and 'multi-level authentication' (O'Kane et al., 2021). The data was divided into two segments: primary risks and proposed solutions, and it gave a methodology for analyzing cybersecurity threats unique to AI voice cloning.

Cybersecurity and Innovative Technology Journal, Vol.3, No.2, 2025, pp. 54-57
e-ISSN 3025-6682. DOI: 10.53889/citj.v3i2.836

RESULTS AND DISCUSSION

Key Cybersecurity Threats Identified

1. **Voice Phishing (Vishing):** Perhaps the largest threat of applying voice cloning is phishing attacks, in which a victim will receive a phone call from what seems to be a friend or critical coworker (Alabdan, 2020). In a healthcare organization, voice cloning enables the attackers to pretend to be a doctor or any worker trusted to gain information that they ought not to disclose.
2. **Unauthorized System Access:** The negative consequences of AI voice cloning shall enable wrongdoers to unlock restricted voice-driven systems with patient data or significant operational information.
3. **Identity Theft and Privacy Violations:** When the imitation of a patient's or provider's voice is possible, an attacker is able to steal an identity or sell the patient's personal health information for monetary benefits, all at the detriment of patient loyalty and trust.

The results are consistent with other industries, including the banking sector, that has counterpart risks that are associated with voice cloning technology. The healthcare sector is specially exposed due to the nature of the information it deals with and due to the trust factor between the patient and the health care provider (Lewandowski et al., 2021). Current strategies used in health care organizations for security include basic protection of passwords and two-factor authentication, which do not defend the organization against advanced AI-incorporated threats. Previous studies have illustrated that there is a significant problem of the lack of identity confirmation and that there is a need for more stringent identity checking in digital health systems. In parallel with these discoveries, the current research provides evidence that unless multi-factor and biometric-based authentication are integrated, healthcare organizations are vulnerable to AI phishing and impersonation. Table 1 showed the comparison of AI voice cloning threats and protective strategies.

Table 1. Comparison of AI Voice Cloning Threats and Protective Strategies

Threats	Description	Recommended Protective Strategies
Voice Phishing (Vishing)	Use of cloned voices for deception	Voice biometrics, multi-factor authentication
Unauthorized System Access	Accessing systems using voice-activated technology	Audits, biometric recognition, anomaly detection systems
Identity Theft and Privacy	Cloning voices for identity fraud	Real-time AI monitoring, secure voice storage protocols

CONCLUSION

The study reveals that AI voice cloning would be useful to create the patient experience and operations but comes hand-in-hand with cybersecurity threats. Interpretation Based on Results: These results underscore the importance of utilizing the best type of security to cover

voice- activated systems and other health care data.

SUGGESTIONS

1. **Adopt Multi-Layered Authentication Protocols:** Use voice biometrics as a stronger supplementary to facial recognition or token base system to ensure that only authorized persons gain access (Koffi, 2023).
2. **Regular Security Audits of Voice-Activated Systems:** This way, AI systems that would have been compromised by the latest threat will be discovered during such audits and re-certified.
3. **Develop real-time monitoring tools:** Develop powerful monitoring systems that would be able to identify irregularities in using voice, which may point at phishing or unauthorized access (Jimmy, 2024).

ACKNOWLEDGMENT

The author is grateful to the healthcare practitioners, artificial intelligence developers, and cybersecurity professionals who volunteered to be part of this research.

REFERENCES

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*, 12(10), 168.

Genelza, G. G. (2024). A systematic literature review on AI voice cloning generator: A game-changer or a threat? *Journal of Emerging Technologies*, 4(2), 54-61.

Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General science* (JAIGS) ISSN: 3006-4023, 2(1), 129-171.

Koffi, E. (2023). VOICE BIOMETRICS FUSION FOR ENHANCED SECURITY AND SPEAKER RECOGNITION: A COMPREHENSIVE REVIEW. *Linguistic Portfolios*, 12(1), 6.

Lewandowski, R., Goncharuk, A. G., & Cirella, G. T. (2021). Restoring patient trust in healthcare: medical information impact case study in Poland. *BMC Health Services Research*, 21(1), 865.

O'Kane, P., Smith, A., & Lerman, M. P. (2021). Building transparency and trustworthiness in inductive research through computer-aided qualitative data analysis software. *Organizational Research Methods,* 24(1), 104-139.