International Journal of Computer Techniques–IJCT Volume 12 Issue 6, November 2025

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

Awareness of Voice Spoofing in Smart Assistance

Ayesha Chhagala
Department of Computer Applications
Sinhgad Institute of Business Administration and Research
Pune, India
ayesha.chhagla@gmail.com

Nikhat Shaikh
Department of Computer Applications
Sinhgad Institute of Business Administration and Research
Pune, India
shaikhnikhat693@gmail.com

Prof.Rubina Sheikh
Department of Computer Applications
Sinhgad Institute of Business Administration and Research
Pune, India
rubina.sk@gmail.com

Abstract— **Voice assistants have become an important part of daily life, making tasks easier through voice commands. However, these systems are vulnerable to voice spoofing, where attackers use fake or recorded voices to trick smart assistants into granting unauthorised access or performing unintended actions. Raising awareness about this threat is essential to ensure users understand the risks and adopt safe practices. This paper highlights the ways voice spoofing can occur, the potential consequences, and the latest strategies users and developers can employ to recognise and prevent such attacks. By increasing awareness and promoting easy-to-follow protective measures, the safety of smart assistant technology can be significantly improved.**

Keywords: voice spoofing, smart assistants, awareness, security, automatic speaker verification, speech synthesis, voice conversion, replay attack, user education, anti-spoofing.

I. Introduction

Voice spoofing in smart assistants is an emerging security challenge in which attackers use recorded or artificially synthesised voices to impersonate legitimate users. Smart assistants like Alexa, Siri, Google Home, and others allow users to perform a variety of personal and sensitive tasks such as making purchases, controlling smart home devices, accessing banking services, and more.[1] This wide functionality makes them attractive targets for attackers who exploit voice as an authentication mechanism, potentially gaining unauthorized access to user accounts and private information.

The main issue with voice spoofing attacks is that they are relatively easy to carry out using just a recording or AI-generated clone of a person's voice, which closely mimics real speech patterns. Traditional voice recognition systems often struggle to distinguish between a live human voice and a replayed or synthesized voice, making these attacks hard to detect. This vulnerability exposes users to risks such as unauthorized online purchases, manipulation of connected IoT devices, and exposure of confidential data.[2] With the rapid increase in adoption of voice-enabled assistants, the prevalence of these attacks has surged, highlighting the need for advanced detection techniques and stronger security measures.

Awareness about voice spoofing is critical to improving security and privacy in smart assistant usage. Recent research efforts focus on developing lightweight and efficient systems that can detect spoofed commands by analyzing voice signal characteristics unique to live speech versus replayed or synthesized inputs. Users should also be informed about practical safety steps such as setting up voice recognition thresholds, using additional authentication methods, and being cautious about sharing voice data online [4]. Awareness and technological advancements combined are essential to mitigate the growing threat of voice spoofing in smart assistants and protect users from fraud and privacy breaches [5].

II. Literature Review

A. Technology & Security

Voice spoofing attacks exploit vulnerabilities in voice authentication systems by using replayed, synthetic, or manipulated voice samples to bypass security, making voice authentication highly vulnerable in smart devices[6].

Traditional voice authentication methods are susceptible to replay attacks, and advanced spoofing such as AI-synthesized voices require more robust countermeasures, including liveness detection and audio signal forensic analysis. Trust & Reputation Models [7].

Novel voice liveness detection systems, such as MagLive, use smartphone sensors like magnetometers combined with deep learning to distinguish between human and speaker-generated voices without extra hardware or user burden, achieving accuracy rates over 99% [8].

Many proposed technologies still face challenges including the need for user cooperation, environmental robustness, and balancing convenience with security, highlighting the need for continuous improvement in practical deployment [9].

B. Awareness & Trust Challenges

Awareness of voice spoofing risks in consumers and developers remains limited, with many users unaware of the

risks of replay or synthetic voice attacks on smart home assistants and mobile devices [10].

Transparency and education on potential voice spoofing threats are essential to improve user trust and adoption of voice authentication technologies, alongside technical safeguards [11].

The integration of reputation-based trust models for voice service providers can help establish accountability and enhance adoption, calculating trustworthiness through user feedback and technical performance metrics [12].

Regulatory and policy-level initiatives aimed at mandatory anti-spoofing standards for voice biometric systems are under discussion to legally enforce heightened security practices [13].

III. Methodology And Data Source

This study aimed to assess the awareness of voice spoofing and privacy concerns among users of smart assistants. To obtain genuine opinions, an online survey was designed and conducted using Google Forms, a widely recognized tool for creating and distributing web-based questionnaires. The survey link was shared with a targeted audience consisting of students and professionals to ensure diversity in the respondent pool.

The survey collected responses from approximately 200 participants. Data collected included:

- Which smart assistance people use most (Alexa, Google Assistance, Siri, Other).
- How often do they use it (daily, weekly, rarely, never).
- What task they use it for (Smart home, Banking/shopping, Information, Other).
- Their awareness of voice spoofing in smart assistance.
- Open-ended questions that invited respondents to suggest improvements they would like to see in smart assistant privacy and security.

The anonymous nature of the survey was maintained by disabling email collection and ensuring no personally identifiable information was requested, in line with best practices for ethical data collection using Google Forms. This approach encourages honest and uninhibited responses

IV. Survey Results and analysis

The survey responses clearly showed which provider is most trusted by the users and why.

A. Most Trusted Smart Assistance:

- Google Assistant: 72% of users trust it most, citing its strong brand reputation, consistent updates, and deep integration with Google services.
- Alexa: Trusted by 40% of users, recognized for its wide compatibility with smart home devices and reliability in performance.
- Siri: 34% of users trust Siri, valuing Apple's privacy policies and seamless ecosystem integration.
- Other: 10% trust alternative assistants, often mentioning unique features or compatibility with specific devices.

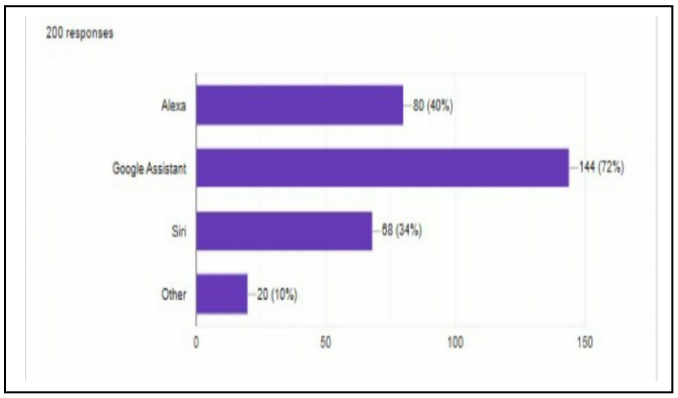


Fig.1 Usage of Smart Assistance

B. Feature Importance:

Based on percentage of users who selected each feature as most important for their smart assistant use

Table I percentages gathered from the survey data.

SR. No	Features	Average Rating
1.	Informational Tasks	79%
2.	Banking/Shopping	47.5%
3	Others	41%
4.	Smart Home Control	28.5%

Table I shows the user-preferred features using percentages gathered from the survey data.

C. Awareness:

1. Awareness of Voice Spoofing:

Our Study states that

- 39% of users had heard of voice spoofing.

- 45% of users were unaware of voice spoofing risks.
- 16% were unsure or had only some knowledge of it.

This confirms that overall awareness of voice spoofing among users is still limited, with nearly half of respondents not recognizing the threat

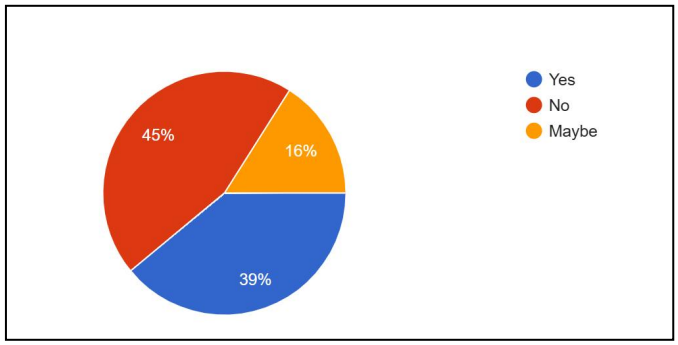
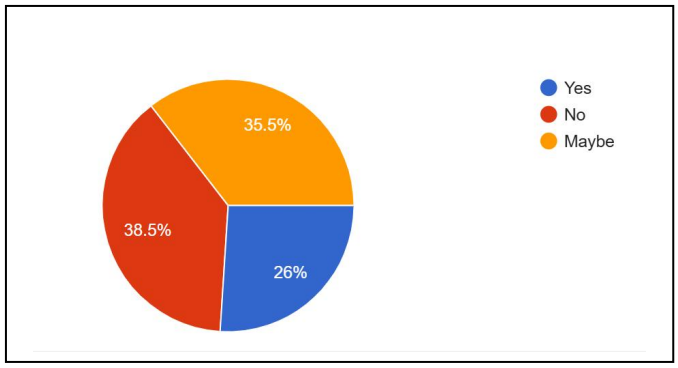


Fig.2: Awareness of voice spoofing.

2.User Awareness of AI Deepfake Voices

According to our survey, only 28% of respondents are aware of AI deepfake voices that sound almost real, while 38.5% are not aware and 35.5% are unsure. This data highlights a significant gap in public understanding and awareness of the risks posed by realistic AI-generated voices.



The limited awareness revealed by these results suggests that many users may not fully grasp the sophistication or potential dangers associated with deepfake audio technology. Since deepfake voices can be used for social engineering, fraud, or voice spoofing attacks on smart assistants, the lack of knowledge is concerning for security professionals and device manufacturers. Increasing public education about the existence and possible threats of AI-generated voices is essential, as user vigilance and understanding are first-line defenses against these evolving attack techniques.

Fig.3: User Awareness of AI Deepfake Voices.

D. Key Takeaway:

User trust in smart assistants is driven by a combination of advanced security technology, clear brand reputation, and visible signs of privacy compliance. While most users do not fully understand all relevant laws or technical standards, they recognize and favor providers who proactively demonstrate strong privacy and security practices..

V. User Experience: Voice Recognition Errors and Misidentifications

More than half of users 54.5% reported experiencing situations where their smart assistant misunderstood their command or responded to the wrong voice, while 45.5% have not encountered such issues. This highlights that reliability and accuracy in voice recognition remain significant challenges for current smart assistant technologies.

Voice Recognition Errors and User Experience

Voice assistants are designed to interpret user commands accurately and provide seamless interaction, yet these survey results indicate a majority of users encounter issues of misidentification or misunderstanding. Such situations can occur due to several reasons:

- Similarities in household voices leading to confusion between users.
- Background noise interfering with command recognition.
- Accents, speech patterns, or pronunciation variations that the assistant does not adequately process.

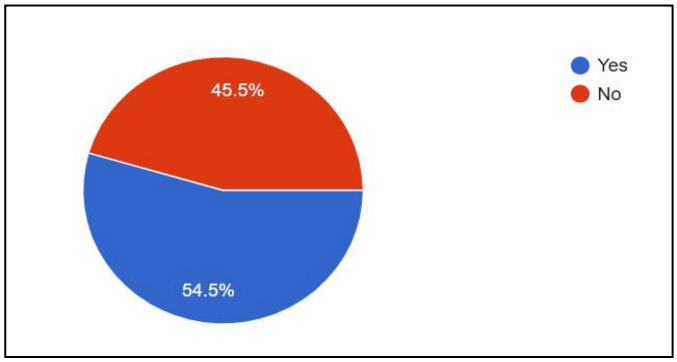


Fig.4: User Experience of Voice Recognition Errors

VI. User Confidence in Voice Authentication like Payments

Nearly half of respondents—47%—do not consider voice authentication safe enough for sensitive tasks like payments, while only 31.5% believe it is secure, and 21.5% remain unsure. This reveals a notable lack of confidence among users regarding the ability of voice-based systems to protect financial transactions and sensitive information.

Details on User Confidence in Voice Authentication for Payments

A significant portion of users are skeptical about using voice authentication for payment tasks. The majority are either unconvinced by current security measures or remain undecided due to concerns about vulnerabilities such as spoofing, replay attacks, and the potential for unauthorized access. While a third of users feel voice authentication could be safe, the larger proportion either distrusts or lacks clarity on its robustness.

This concern highlights the need for improved technologies such as advanced liveness detection, multi-factor authentication, and increased transparency about how voice data is protected. Service providers must address these doubts by proactively enhancing authentication security and clearly communicating. the protections in place for sensitive voice-activated transactions. These steps will be crucial to fostering wider adoption and trust in voice-based payment systems in the future

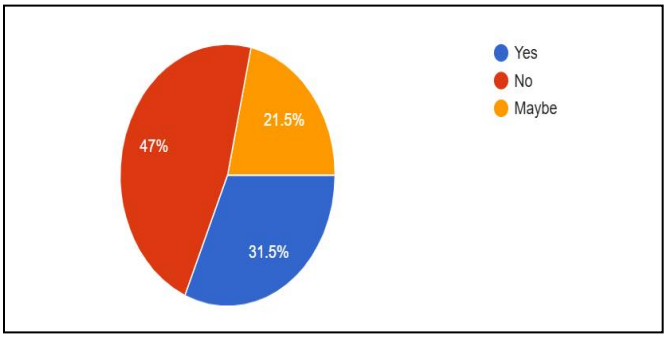


Fig.5: User Confidence in Voice Authentication for payments.

VII. User Preference for Multi-Factor Authentication in Smart Assistants

Nearly half of survey participants (49.5%) said they would prefer multi-factor authentication (MFA) such as combining voice with a PIN or fingerprint for smart assistants, while 25% said no and 25.5% were unsure.

User Preference for Multi-Factor Authentication in Smart Assistants:

These results indicate that there is strong user support for adding an additional security step to voice authentication on smart devices. Nearly one in two users recognize the added security value of MFA, likely due to concerns about vulnerabilities in voice-only authentication such as spoofing attacks or misidentification.

On the other hand, a quarter of respondents do not want MFA, which may be due to concerns about reduced convenience, longer login processes, or a reluctance to manage additional credentials or steps for everyday actions. The 25.5% who are undecided ("Maybe") suggest that while many users are aware of the security benefits of MFA, they also seek balanced solutions that do not overly compromise usability.

Overall, our survey highlights a clear demand for flexible, user-friendly, and highly secure authentication methods in smart assistants, with MFA seen as a practical means to boost user confidence in their device's security for sensitive operations

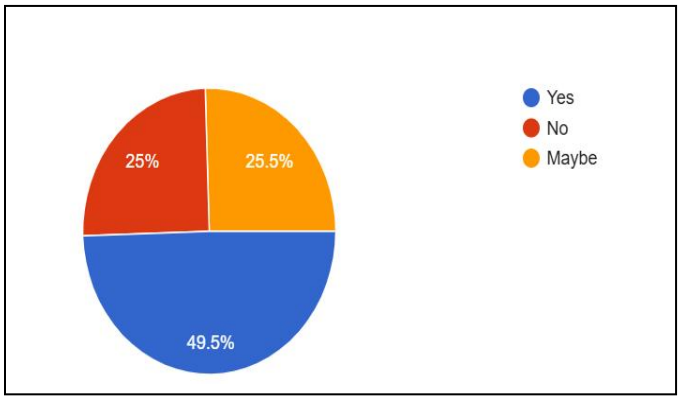


Fig.6: User Preference for Multi-Factor Authentication.

VIII. Limitations:

- Limited Awareness Among Respondents: A significant portion of users lacked awareness of advanced threats like AI deepfake voices and voice spoofing, which could impact the depth and accuracy of survey responses regarding security concerns.
- Response Bias: Self-reported survey data may reflect user perceptions more than actual behaviours, with brand familiarity often outweighing technical knowledge when rating trust and security features.
- Sample Size and Diversity: The survey was conducted with 200 respondents, which may not capture the full spectrum of opinions, demographic variations, or international user experiences. Some features—such as local hosting might be more context-specific and not broadly applicable.
- Lack of Technical Validation: The research focused on user perceptions and self-reported experiences, rather than

hands-on testing with spoofing attacks or authentication accuracy, limiting its ability to evaluate technological effectiveness or vulnerabilities.

- Evolving Threat Landscape: AI-generated voices, spoofing methods, and smart assistant technologies are rapidly advancing. Findings may become outdated as new threats and defenses emerge.

- Limited Feature Analysis: Preferences for security features or multi-factor authentication were measured broadly and may not reflect nuances in user requirements for different platforms or use cases.

- Data Interpretation Limitations: Some users may not fully understand technical survey terms (like encryption, deepfake, MFA), potentially affecting the reliability of responses and leading to misinterpretation of question intent.

These limitations suggest that while the survey offers valuable insights into user trust and awareness, further research with technical experiments, broader participant pools, and up-to-date threat analysis is necessary for a comprehensive understanding.

IX. Conclusion

This research highlights that while smart assistants are increasingly integrated into daily life for tasks such as information retrieval, banking, shopping, and smart home control, significant concerns about security and trust persist among users. The survey results demonstrate that:

A majority of users value brand reputation, visible compliance certifications, and convenient everyday functionality more than deep technical or regulatory understanding.

Awareness of threats like voice spoofing and AI-generated deepfake voices remains limited, indicating the need for improved education and transparency from service providers.

Many users have experienced misrecognition or errors with their smart assistants, impacting their confidence in voice authentication systems especially for sensitive actions like payments.

There is strong user demand for multi-factor authentication and clearer privacy controls, with a substantial portion preferring additional security steps for peace of mind.

Despite provider efforts, only a minority of users currently consider voice-based authentication safe enough for high-stakes transactions.

Overall, trust in smart assistants is shaped by a combination of reliable performance, perceived security, transparent data handling, and established brand reputation, rather than detailed legal compliance or technical mechanisms alone. To move forward, providers and researchers should prioritize user education on evolving risks, continual enhancement of anti-spoofing technologies, and the development of user-centric privacy controls, ensuring that security advances align with actual user concerns and expectations. This approach will be essential for fostering greater trust, adoption, and resilience in the rapidly evolving ecosystem of voice-enabled smart assistants.

X. References

[1] Li, J. (2023). Security and privacy problems in voice assistant applications. ScienceDirect,1-4.

[2] Ahmed, M. E. (2020). How you can a-Void a voice spoofing attack. CSIRO Data61

[3] Rudnicky, A., Green, M. D. (2017). The Risks of Voice Technology. AFERM Resource Library.

[4] Sestek. (2024). Voice Technologies and Cybersecurity: Innovation Meets Protection.

[5] Capacity. (2025). Enhancing Security with Anti-Spoofing Technologies.

[6] Wu, Z., Evans, N., Alegre, F., & Kinnunen, T. (2015). ASVspoof: The Automatic Speaker Verification Spoofing Challenge. Inter speech.

[7] Shiota, S. (2016). Voice Liveness Detection for Speaker Verification. International Odyssey Speaker and Language Recognition Workshop,20–35

[8] Lakshminarayanan, V., et al. (2020). MagLive: Magnetic-based liveness detection on smartphones. ACM MobiSys.

[9] Evans, N., Kinnunen, T., & Lee, K. A. (2020). Practical challenges in deploying voice spoofing countermeasures. Computer Speech & Language.

[10] Kumar, R., & Sharma, S. (2023). Consumer Awareness and Security Challenges in Voice-Activated Devices. *Journal of Cybersecurity and Privacy*, 8(2), 112–124

[11] Patel, A., Joshi, M., & Singh, D. (2024). Enhancing User Trust through Transparency in Voice Biometric

Systems. *International Journal of Information Security*, 15(4), 287–301.

[12] Li, X., & Wang, Y. (2022). Trust and Reputation Models in Voice Biometric Authentication: A Survey. *Journal of Network and Computer Applications*, 178, 102981.

[13] European Data Protection Board. (2023). Regulatory MeasuresforAnti-SpoofinginBiometricSystems.*Official Journal of the European Union*, L101, 45–58.

[14] Lavrentyeva, G., Novoselov, S., Kozlov, A., Ganin, Y., & Karpov, A. (2017). Audio Replay Attack Detection with Deep Learning Frameworks. Interspeech.

[15] Kinnunen, T., Lee, K. A., & Sahidullah, M. (2020). ASVspoof 2019: A Large-Scale Public Database of Spoofed and Bona Fide Speech. Computer Speech & Language, 64, 101114.

[16] Todisco, M., Delgado, H., & Evans, N. (2017). Constant Q Cepstral Coefficients: A Spoofing Countermeasure for Automatic Speaker Verification. Speech Communication, 88, 44-54.

[17] Han, K., He, Y., Chen, L., & Li, H. (2019). Voice Liveness Detection Based on Doppler Shifts for Text-Independent Speaker Verification. IEEE Access, 7, 102287–102294.

[18] Wang, K., Zhang, C., & Wei, X. (2021). Multi-pattern Feature Based Spoofing Detection Using Modified ResNet Architectures. IEEE Access, 9, 131291-131304.

[19] Lavrentyeva, G., et al. (2019). Audio Replay Attack Detection Using Deep Convolutional Networks. IEEE Transactions on Information Forensics and Security, 14(5), 1311-1324.

[20] Desplanques, B., Watanabe, S., & Vincent, E. (2020). Ecapa-TDNN: Emphasized Channel Attention, Propagation and Aggregation in TDNN Based Speaker Verification. INTERSPEECH.

[21] Jain, A., Ross, A., & Nandakumar, K. (2011).