Scientific Research Publishing

Journal of Computer and Communications, 2023, 11, 137-150
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Securing User Authentication with Server-Side Voice Verification

Deepak R. Chandran[1], Sanath Kumar[2], S. Deepashri[2]

[1]Emergence Technologies LLC, Willow Grove, PA, USA
[2]Iris Energy LLC, Edison, NJ, USA
Email: cdr22@me.com

How to cite this paper: Chandran, D.R., Kumar, S. and Deepashri, S. (2023) Securing User Authentication with Server-Side Voice Verification. *Journal of Computer and Communications*, **11**, 137- 150.
https://doi.org/10.4236/jcc.2023.115010

Received: April 9, 2023
Accepted: May 27, 2023
Published: May 30, 2023

Abstract

User authentication is critical to the security of any information system. The traditional text-based passwords and even biometric systems based on face and fingerprint validation suffer from various drawbacks. Voice-based authentication systems have emerged as an effective alternative method. Within the user authentication systems, the server-side voice authentication systems added advantages. The purpose of this paper is to present an innovative approach to the use of voice verification for user authentication. This paper describes a new framework for the implementation of server-side voice authentication, ensuring that only the users who are authenticated and validated can access the system. In addition to providing enhanced security and a more pleasant user experience, this technology has potential applications in a wide range of fields.

Keywords

Voice Authentication, Data Security, Voice Biometrics, Automatic Speech Recognition

1. Introduction

Authentication of users is a critical component of information security, as it ensures that only authorized individuals can access sensitive data and systems [1]. Traditionally, authentication has relied on knowledge-based (passwords) or possession-based (tokens) mechanisms. These methods, however, are increasingly vulnerable to attacks such as phishing and brute force [2]. The use of biometric authentication has emerged as an effective and convenient alternative to traditional authentication methods [3]. The use of voice authentication has gained traction due to its non-invasive nature, ease of use, and widespread

availability of microphones in devices [4]. The purpose of voice authentication is to identify and verify a particular individual based on their unique vocal characteristics, thereby making it nearly impossible to impersonate or fabricate [5]. Figure 1 summarizes the traditional and biometric methods in use for user authentication.

The purpose of this paper is to present an innovative approach to the use of voice biometrics for user authentication. The current literature on user authentication through voice biometrics is reviewed in this paper. The importance of server-side voice authentication and its use cases are discussed. Thereafter, a new framework is proposed for the implementation of the server-side voice authentication system. The advantages of the proposed system are also discussed.

2. Literature Review

This section captures the existing literature on the user authentication methods. This review does not amount to a systematic and exhaustive review of the literature on the subject [6]. This paper adopts the narrative approach to the review of literature [7] for exploring the current knowledge that informs the author in the ongoing research in the field of user authentication. The findings of the review are utilized in preparing and presenting the innovative approach to implementing a server-side voice verification for enhanced user authentication.

2.1. Existing Solutions for User Authentication

The traditional methods used for user authentication suffered from many issues and inefficiencies. These issues included having to correctly remember multiple passwords and user ids and susceptibility to duplication and misuse [8]. Biometric based authentication systems came up in response to the issues faced by the traditional methods. Face recognition, fingerprints, iris recognition, and hand

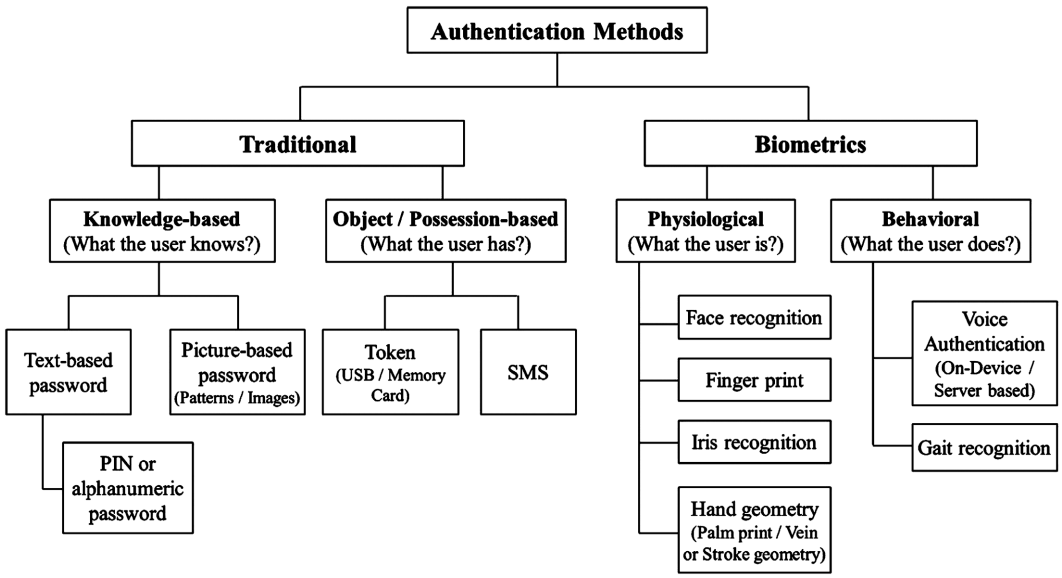

Figure 1. Authentication methods.

geometry were some of the biometrics adopted for user verification.

Biometrics like face and fingerprint are capable of providing strong security at the device level. However, these biometrics are not suitable for all the situations. There are occasions when hand-free access to their devices would be beneficial to the users. Accessing a locked device while driving a vehicle is an apt example. Methods like PIN or use of biometrics like face and fingerprint may not be suitable for accessing a device while one is driving a vehicle. Attempting to access a device by using the touchscreen or placing the face in front of a camera could be both inconvenient and dangerous under such circumstances. Many other similar situations also exist where a user would find hand-free access to their devices beneficial and convenient [9]. **Table 1** contains a comparison of traditional authentication methods and the voice authentication method.

An alternative that can address the above drawbacks of other authentication systems is voice authentication. Voice authentication allows the user to access

Table 1. A comparison of traditional authentication methods and voice authentication.

Metrics	Traditional authentication	Voice authentication
Authentication Factor	Single-factor authentication	Single or multi-factor authentication
Usability (Ease of use)	**Moderate** Easy to use but not always user-friendly	**High** Easy to use and user-friendly
Security	**Low** Vulnerable to password cracking or object theft	**High** Difficult to fake or replicate voice characteristics, protection from voice spoofing attacks
Accuracy	**Low** Can be prone to errors or forgotten passwords	**High** Advanced algorithms ensure accuracy. False Acceptance Rate below 1 in 50,000
Spoofing Detection	**Low** Passwords or objects can be easily spoofed	**High** Advanced algorithms can detect and protect from voice spoofing attacks
Convenience	**Low** Requires remembering and entering passwords, carrying objects or possession	**High** Convenient as it only requires a user's voice
Cost	**Low** Relatively inexpensive to implement	**Moderate** Requires specialized technology and software
User Acceptance	**Low** Due to inconvenience and complexity	**High** Due to easy and convenient use
Reliability	**Moderate** Can be affected by human errors	**High** Consistent and reliable
Privacy	**Low** Can be compromised if the password is shared or the object is lost or stolen	**High** Voice samples can be kept encrypted
Adoption	**Moderate** Widely adopted and understood, but becoming increasingly outdated in terms of security	**High** Increasingly adopted, but still not as widely used as traditional methods

the secured devices without diverting the focus of attention. It only requires speaking a short instruction such as "Hey Device, Play the music." The added advantage of voice authentication is that it allows the instructions to act in a dual capacity of commands for execution and ensuring security. This dual role is possible because the execution command itself is processed for voice authentication as well.

Another advantage of voice authentication is that unlike other security methods, it doesn't require any special sensors or equipment to capture the biometric. Voice authentication can be adopted even with low end devices. There is no hardware costs involved in adopting voice authentication. The existing devices can be easily configured to use voice authentication for security unlock. The voice authentication also provides a suitable alternative for situations where camera or fingerprint scanner might not work due to conditions like inadequate light or wet fingers etc. [9].

2.2. Voice Authentication Process

A comparison of the voice authentication method with other traditional and biometric methods clearly establishes the advantages of adopting the voice-based system for user authentication. The steps involved in the voice authentication process are detailed in this section.

2.2.1. Voice Recording and Storage

The voice authentication process begins with the collection of voice samples from users during the registration and enrolment process. Users are typically asked to provide a set of phrases, ensuring consistency, and reducing environmental influences on the quality of voice samples [10]. **Figure 2** contains the process of user registration and enrollment process. The system records and extracts the voice signatures from the samples and creates a unique voiceprint. These voiceprints are then stored securely in the system and used as a reference for future authentication attempts. As a result, it is very important that these voiceprints are maintained confidentially and with integrity to avoid the risk of unauthorized access and fraud [11].

2.2.2. Feature Extraction and Comparison

To get access to a system, users must give a sample of their voice as part of an authentication process. Using advanced signal processing methods and machine learning algorithms [13], the system then pulls out important features from the voice sample, such as pitch, frequency, and formants. Using the extracted features,

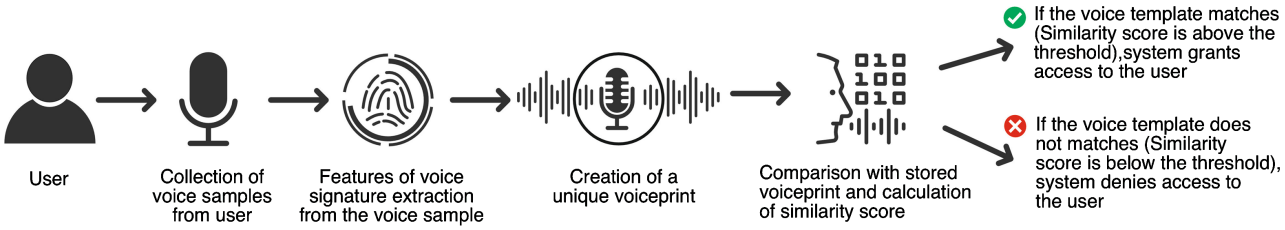

Figure 2. Voice authentication User Registration and Enrollment process—Model Training [12].

the voice sample is then compared with the stored reference voiceprints, calculating a similarity score that reflects the degree of correspondence between the two samples [14].

2.2.3. Decision-Making Process

Based on the uploaded voice samples, the system calculates a similarity score, which lets it figure out if a particular input belongs to the claimed user. To distinguish between genuine and imposter attempts, a threshold value is set. Users get access to the system only if the system determines their similarity score as above the set threshold. If the score is lower than the threshold, the system denies access, potentially triggering additional safeguards or alerts [4]. To balance security and usability, threshold values need to be tuned to minimize both false acceptances and false rejections. **Figure 3** captures the decision-making process.

2.2.4. Voice Authentication Scheme

According to a white paper published by ID R&D [9], there are two types of methods for authenticating the unique voiceprint of a user. These are text-dependent and text-independent methods. The first type of method uses pre-defined messages for voice analysis and authentication. The second type of method is text-independent and can use any words or sentences spoken by the user for voice authentication.

One essential requirement of a robust voice authentication system is an effective protection against voice spoofing attacks. ID R&D [9] identified the spoofing attacks under the following categories:

Text-to-Speech attacks: Text to speech attack is carried out by generating synthesized voice and using it to overcome the authentication system.

Voice Conversion attacks: Voice conversion attack uses a software tool for converting a message or phrase in person's voice into that of another person's voice to present it to the authentication system.

Replay attacks: Replays attacks merely record the user's voice or text and then play it through a speaker to gain access to the device.

Mixed attacks: Mixed attacks use a combination of one or more of the above methods to attack a voice authentication system.

To ensure the robustness of a voice authentication system, there must be effective defense against spoofing attacks. There are algorithms available to ensure protection against voice spoofing attacks.

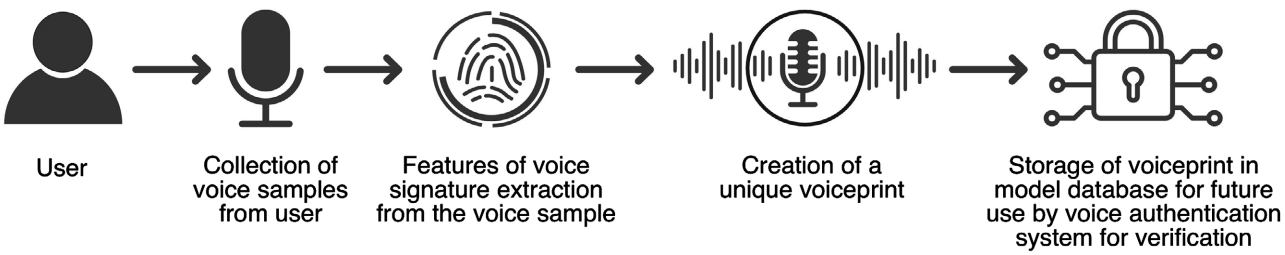

Figure 3. Voice authentication Decision-making Process—Model Inferencing [12].

By combining the authentication system and anti-spoofing algorithms it is possible to attain high accuracy levels. Industry claims that it is feasible to achieve a false acceptance rate of less than 1 is 50,000, spoofing acceptance rate of less than 3%, and false rejection rate at below 10% by adopting a combination of user verification and anti-spoofing methods [9]. Use of Common Deep Neural Network processing allows the authentication systems to extract the identifying features of voices for authenticating the text-dependent, text-independent, and anti-spoofing systems from the same network. **Figure 4** contains a scheme of voice authentication.

2.3. Importance of Server-Side Verification

To maintain the integrity and security of authentication systems, server-side verification is essential. A centralized, controlled, and monitored authentication process can be achieved by validating user credentials on the server side, which reduces the risk of unauthorized access [15]. Further, server-side verification allows users to authenticate continuously as well as implement advanced security measures, such as multi-factor authentication and risk-based authentication, allowing for continuous authentication and enhanced security [16].

2.4. Ensuring Authenticated and Validated User Access

Steps involved in ensuring access to only the authenticated and validated users are detailed in this section.

2.4.1. Registration and Enrolment

During enrollment and registration, a user's account is set up and their biometric data collected for authentication. This process is essential for ensuring the accuracy and security of the authentication system. Reference [17] recommended

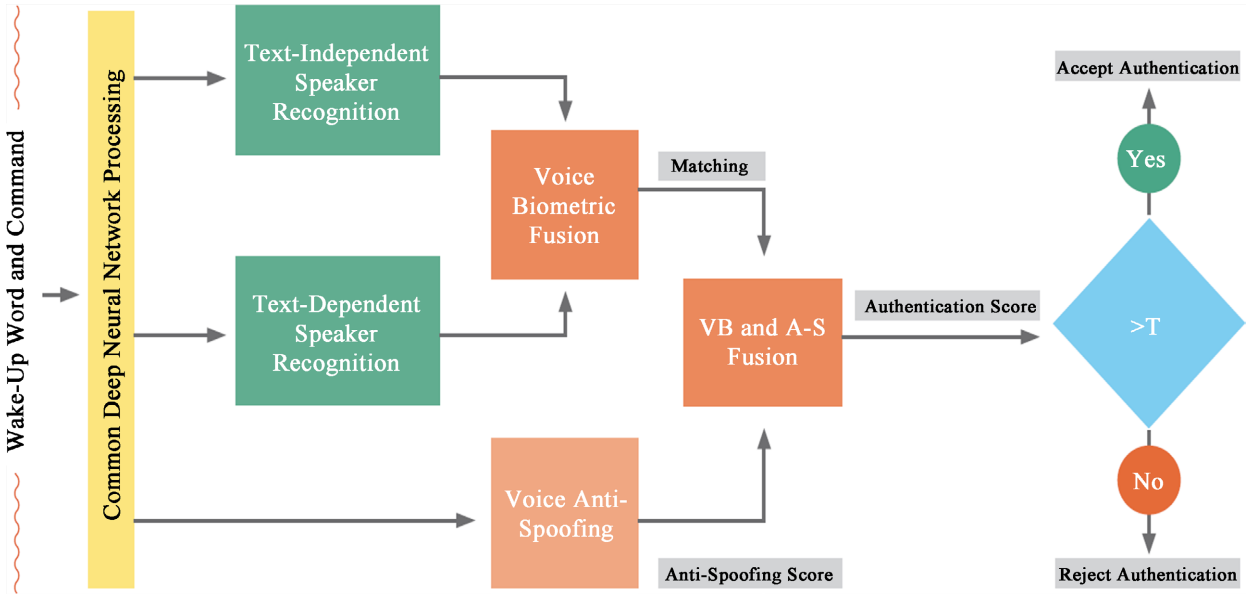

Figure 4. Voice authentication scheme [9].

that the registration and enrollment process must involve multiple factors of authentication. These factors could be what user knows (password, PIN), user has (smart card, token), or user is (biometric). This can prevent spoofing or other forms of fraud. It is vital to gather and securely store biometric data to ensure the user's privacy. According to [18], an access restricted secure environment is recommended for storing biometric data. Use of secure protocols and channels of communication for any transmission of biometric data is also imperative to ensure the integrity of the data.

2.4.2. Continuous Authentication and Monitoring

The continuous authentication and monitoring serve the purpose of continually verifying the user's identity to ensure that the user remains authorized to access the system or data. This is crucial to preventing unauthorized access or data breaches. Continuous authentication can use multiple authentication factors, including biometric data and location data, to establish and maintain a user's identity [19]. As a result, spoofing or other forms of fraud may be detected and prevented. The use of machine learning algorithms is also effective in detecting anomalies or suspicious behavior that could indicate a security threat. As described by [19], machine learning is useful for analyzing the user behavior to identify deviations from normal trends, which can then trigger additional authentication checks or alerts to security personnel.

2.4.3. Managing False Positives and Negatives

Achieving accuracy and usability requires managing false positives and negatives in the authentication system. A false positive occurs when an authorized user is denied access, whereas a false negative occurs when an unauthorized user is granted access [20].

Adaptive authentication, which emphasizes the balance between security and usability, may be used to manage false positives and negatives [21]. Additionally, feedback mechanisms can improve the accuracy of the authentication system over time. It is possible to improve accuracy by using feedback from users and reduce false positives and negatives by adjusting based on feedback from users [22].

2.4.4. Digital Signature Certificate (DSC) for Added Security

A digital signature certificate (DSC) can be used as another factor of authentication during the enrollment and registration process. A DSC is a digital certificate that contains information about the identity of the signer, which can be verified using public key infrastructure (PKI). By using a DSC, the user can prove their identity and authenticate the information they are providing during the registration process.

In addition, a DSC ensures the integrity and authenticity of biometric and location data along with timestamp transmitted over a network. The DSC is useful to digitally sign the biometric data, which assures that the data is not tampered with or altered during transmission. Furthermore, a DSC is useful to securely

store and protect biometric data that is collected during the registration. The DSC can be used to encrypt and digitally sign the data, which provides confidentiality, integrity, and non-repudiation. Only authorized users with the correct public key can access the biometric data. This ensures the security of the private information of a user.

Overall, a DSC can be used to increase integrity and security during the enrolment and registration process. A DSC can also secure biometric data and protect the privacy during its transmission.

2.5. Use Cases and Applications

There are many domains and sectors where server-side user authentication can play an effective role. Some of the representative use cases are discussed in this section.

Figure 5 below contains an infographic of the domains and sectors that can potentially make use of server-side voice authentication for enhancing their efficacy and user experience.

2.5.1. Banking and Financial Services

Banks and financial services can greatly benefit from voice authentication by improving security and the customer experience. With voice authentication, bank accounts, trading platforms, and other financial services can be protected

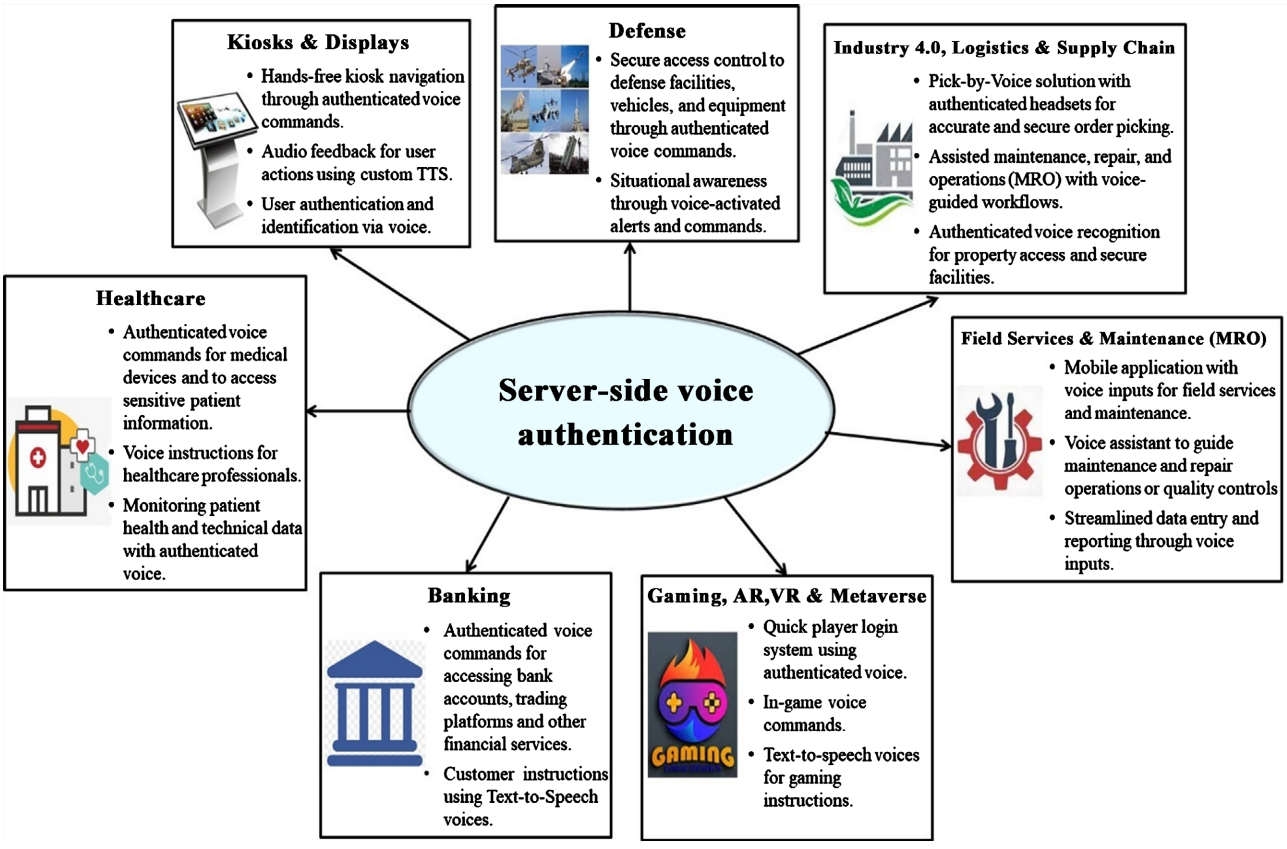

Figure 5. An infographic of the potential industries that can benefit from server-side voice authentication.

against unauthorized access by replacing password-based systems and enhancing multi-factor authentication [23]. The use of voice authentication can also streamline the customer service experience by providing secure, efficient, and convenient access to telephone-based support [24].

2.5.2. Healthcare

Voice authentication systems are useful in healthcare settings to make sure that only authorized people can have access to protected information of the patients. A healthcare provider can improve patient privacy and comply with relevant data protection regulations by implementing voice authentication in electronic health records (EHRs) and telemedicine platforms, such as those covered by the Health Insurance Portability and Accountability Act (HIPAA) [25].

2.5.3. E-Commerce and Retail

Voice authentication is useful to make e-commerce and retail stores safer. It can also improve the customer experience. The risk of fraudulent transactions can be reduced by the Businesses. They can also protect their systems against identity thefts through voice authentication [26]. This is in addition to making shopping easy and safe. Also, voice authentication makes it easier for chatbots and virtual assistants to help customers in a smooth way [27].

2.5.4. Enterprise and Government Services

Enterprises and governments can utilize voice authentication to protect sensitive data and systems. Data breaches can be prevented, and security enhanced by implementing voice authentication for employee logins and remote access [28]. Additionally, voice authentication can be used by government agencies to verify citizens' identities when they access online services, including submitting tax returns, filing benefit claims, and registering to vote [29].

3. Implementing Server-Side Voice Authentication

A review of the existing literature showed the advantages and use cases of a server-side voice authentication system. To successfully integrate server-side voice authentication into existing infrastructure, the implementation process must be carefully planned and evaluated to ensure compatibility with existing authentication mechanisms. This paper now presents a new framework for implementing a server-side voice authentication system and integrating it with the existing systems. **Figure 6** captures a high-level architecture flow diagram for the suggested server-side voice authentication system.

3.1. Choosing the Right Voice Authentication Technology

In choosing voice authentication technology [30] many factors play critical roles. These factors include accuracy, scalability, ease of use, and cost. There are many commercial and open-source solutions in the market, and each has its pros and cons. Organizations need to weigh these options based on their specific needs, compliance needs, and available resources [31]. It is also important to think

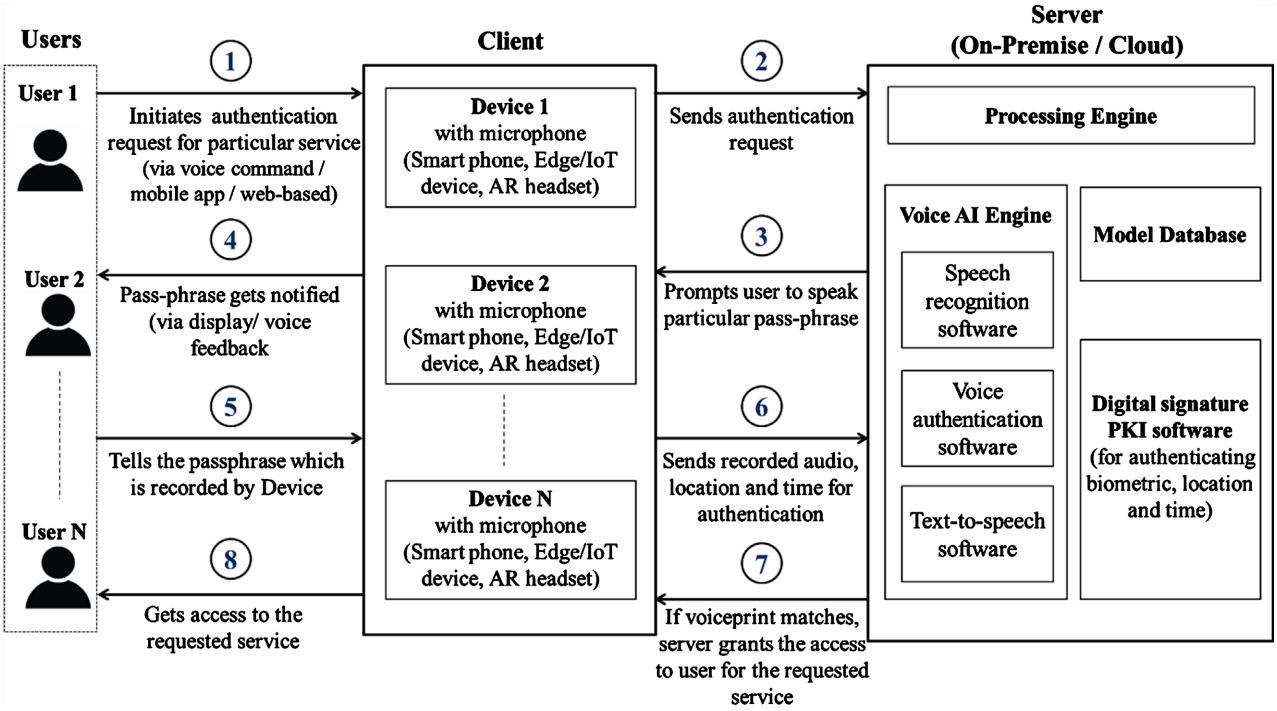

Figure 6. High-level architecture flow diagram for server-side voice authentication.

about the technology's ongoing maintenance and support to make sure that it can keep up with emerging threats.

3.2. Integration with Existing Systems

Before attempting the integration, a comprehensive assessment of the current systems is necessary to identify potential bottlenecks and to determine the parts that need to be upgraded [21]. All relevant stakeholders such as IT administrators, security experts, and end users are to be involved in the process of decision-making to ensure seamless integration and adoption [23]. The steps involved in integration of a server-side voice authentication system with the existing system are captured in **Figure 7** below.

3.3. Addressing Privacy and Security Concerns

It is imperative to address privacy and security concerns when implementing server-side voice authentication. Voiceprints should be encrypted and stored securely by organizations to ensure their confidentiality and integrity [11]. A strict access control mechanism and audit trail should be implemented to ensure that only authorized personnel and applications have access to voiceprints [32]. Regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are to be taken into consideration while handling voice data [33] [34].

4. Conclusion and Future Directions

Server-side voice authentication can enhance security and user experience in a

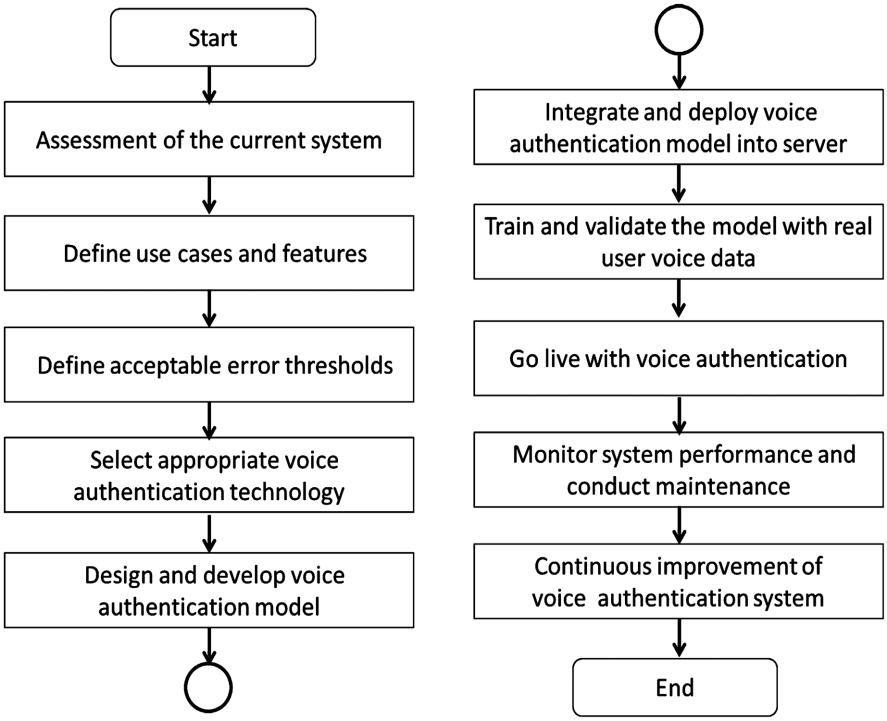

Figure 7. Steps to integrate server-side voice authentication.

variety of applications and industries. Using advanced technologies, digital certificates, and location data, organizations can implement robust and context-aware authentication systems that effectively protect against unauthorized access and security threats. Research and development are still needed to address privacy concerns, address demographic factors, and counter sophisticated attacks.

Voice authentication systems can be further strengthened by incorporating continuous authentication and adaptive security measures. Voice authentication technology is always evolving, so organizations need to remain vigilant and proactive in addressing these challenges while ensuring that they work equally across diverse user populations. Hence, server-side voice authentication holds great promise for improving security and user experience in an increasingly connected world. With the adoption of right practices and addressing of the challenges, organizations can provide secure and seamless access to their systems and services through voice authentication.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Juels, A. and Rivest, R.L. (2013) Honeywords: Making Password-Cracking Detectable. *Proceedings of the* 2013 *ACM SIGSAC Conference on Computer & Communications Security*, Berlin, 4-8 November 2013, 145-160. https://doi.org/10.1145/2508859.2516671

[2] Bonneau, J., Preibusch, S. and Anderson, R. (2012) Does a Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs. In: Keromytis, A.D., Ed., *Financial Cryptography and Data Security*, Springer, Berlin, 25-40. https://doi.org/10.1007/978-3-642-32946-3_3

[3] Jain, A.K., Ross, A. and Prabhakar, S. (2004) An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, **1**, 4-20. https://doi.org/10.1109/TCSVT.2003.818349

[4] Reynolds, D.A. and Torres-Carrasquillo, P.A. (2005) Approaches and Applications of Audio Diarization. 2005 *IEEE International Conference on Acoustics, Speech, and Signal Processing* (*ICASSP*), Philadelphia, 23-23 March 2005, 953-956. https://doi.org/10.1109/ICASSP.2005.1416463

[5] Furui, S. (1997) Recent Advances in Speaker Recognition. *Pattern Recognition Letters*, **18**, 859-872. https://doi.org/10.1016/S0167-8655(97)00073-1

[6] Massaro, M., Dumay, J. and Guthrie, J. (2016) On the Shoulders of Giants: Undertaking a Structured Literature Review in Accounting. *Accounting, Auditing & Accountability Journal*, **29**, 767-801. https://doi.org/10.1108/AAAJ-01-2015-1939

[7] Rother, E.T. (2007) Systematic Literature Review X Narrative Review. *Acta Paulista de Enfermagem*, **20**, 5-6. https://doi.org/10.1590/S0103-21002007000200001

[8] Zheng, Y. and Zhao, S. (2016) A Usable Authentication System Based on Personal Voice Challenge. 2016 *International Conference on Advanced Cloud and Big Data* (*CBD*), Chengdu, 13-16 August 2016, 194-199.

[9] ID R&D (2021) Voice Biometric Revolution: Why Voice ID Is Now Secure Enough for Device Unlock. https://www.idrnd.ai/wp-content/uploads/2021/02/IDRD-VoiceBiometric-DeviceUnlock-Whitepaper-.pdf

[10] Reynolds, D.A. (2000) An Overview of Automatic Speaker Recognition Technology. 2000 *IEEE International Conference on Acoustics, Speech, and Signal Processing* (*ICASSP*), Orlando, 13-17 May 2002, 4072-4075.

[11] Yampolskiy, R.V., Govindaraju, V. and Reznik, L. (2013) Behavior-Based Biometrics: A Survey and Classification. *International Journal of Biometrics*, **5**, 197-221.

[12] Chandran, D.R. (2022) Use of AI Voice Authentication Technology Instead of Traditional Keypads in Security Devices. *Journal of Computer and Communications*, 10, 11-21. https://doi.org/10.4236/jcc.2022.106002

[13] Kinnunen, T. and Li, H. (2010) An Overview of Text-Independent Speaker Recognition: From Features to Supervectors. *Speech Communication*, **52**, 12-40. https://doi.org/10.1016/j.specom.2009.08.009

[14] Kinnunen, T., Wu, Z.Z., Sedlák, F. and Lee, K.A. (2012) Non-Parametric and Parametric Score Calibration for Biometric Authentication. *Pattern Recognition Letters*, **33**, 387-393.

[15] Wang, R. and Liu, Y. (2013) Scalable Web-Based User Authentication Using Server-Side Verification. *International Journal of Security and Its Applications*, **7**, 329-342.

[16] Menezes, A., van Oorschot, P.C. and Vanstone, S.A. (2020) Handbook of Applied Cryptography. CRC Press, Boca Raton.

[17] Gao, X., Liu, Y., Zhang, Q. and Li, Y. (2020) Biometric Authentication Systems: A Comprehensive Review. *IEEE Access*, **8**, 104420-104445.

[18] Hu, Y., Zhang, H. and Liu, Y. (2020) Biometric Authentication for Secure Mobile Cloud Computing: A Comprehensive Review. *IEEE Access*, **8**, 97612-97627.

[19] Shin, D., Lee, J., Lee, S. and Lee, S. (2021) Continuous Authentication Using Machine Learning for Mobile Devices: A Comprehensive Review. *IEEE Access*, **9**, 32813-32831.

[20] Muckenhirn, H., Magimai-Doss, M. and Marcel, S. (2018) Long-Term Speaker Verification: The Case of Telephone Speech. 2018 *IEEE International Conference on Acoustics*, *Speech and Signal Processing* (*ICASSP*), Calgary, 15-20 April 2018, 5239-5243.

[21] Ratha, N.K., Connell, J.H. and Bolle, R.M. (2001) Enhancing Security and Privacy in Biometrics-Based Authentication Systems. *IBM Systems Journal*, **40**, 614-634. https://doi.org/10.1147/sj.403.0614

[22] Li, Y., He, X., Zhao, X. and Yang, X. (2019) Enhancing User Experience of Continuous Authentication with Feedback. *IEEE Transactions on Mobile Computing*, **18**, 310-322.

[23] Ratha, N.K., Connell, J., Sasse, M.A., Brostoff, S. and Weirich, D. (2001) Transforming the 'Weakest Link'—A Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, **19**, 122-131. https://doi.org/10.1023/A:1011902718709

[24] Gupta, P., Mehrotra, H. and Verma, A. (2019) Voice Biometric-Based User Authentication in Banking: A Literature Review. *Journal of Internet Banking and Commerce*, **24**, 1-13.

[25] Sundararajan, M. and Rajamani, V. (2016) A Secure Voice-Based Authentication for Accessing EHRs Using Smart Phones. *Journal of Medical Systems*, **40**, 186.

[26] Gupta, P. and Sivakumar, A.I. (2019) Voice Biometrics in E-commerce: Applications, Benefits, and Challenges. *Journal of Electronic Commerce in Organizations*, **17**, 1-17.

[27] Nayak, S.K., Sahoo, S. and Mohapatra, A.G. (2018) A Secure E-Commerce Application Using Voice Recognition. 2018 2*nd International Conference on Inventive Systems and Control* (*ICISC*), Coimbatore, 19-20 January 2018, 1036-1040.

[28] Dey, S., Samanta, D. and Pal, A. (2019) A Reliable Voice-Based Authentication System for Enhancing Enterprise Security. *Journal of Ambient Intelligence and Humanized Computing*, **10**, 3579-3592.

[29] Krishna, Y., Kumar, M.A. and Sekhar, C.C. (2018) Speaker Recognition for E-Governance Security. In: Shrivastava, G., Kumar, P., Gupta, B.B., Bala, S. and Dey, N., Eds., *Handbook of Research on Network Forensics and Analysis Techniques*, IGI Global, Hershey, 255-277.

[30] Jain, A.K., Nandakumar, K. and Ross, A. (2015) 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. *Pattern Recognition Letters*, **79**, 80-105. https://doi.org/10.1016/j.patrec.2015.12.013

[31] Korshunov, P., Ramírez, G.R. and Fierrez, J. (2016) Voice Presentation Attack Detection: Current Progress and Challenges. 2016 *IEEE* 8*th International Conference on Biometrics Theory*, *Applications*, *and Systems* (*BTAS*), Niagara Falls, 6-9 September 2016, 1-7.

[32] Zheng, N., Bai, K., Huang, H. and Wang, H. (2011) You Are How You Touch: User Verification on Smartphones via Tapping Behaviors. 2014 *IEEE* 22*nd International Conference on Network Protocols* (*ICNP*), Raleigh, 21-24 October 2014, 221-232. https://doi.org/10.1109/ICNP.2014.43

[33] European Parliament and Council (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons about the Processing of Personal Data and the Free Movement of Such Da-

ta and Repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[34] California Legislature (2018) California Consumer Privacy Act of 2018 [AB-375]. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375