International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

A novel hybrid database security management technique

Margaret Dumebi Okpor [1], Kizito Eluemunor Anazia [2, *] and Daniel Ukpenusiowho [3]

[1] *Department of Cyber Security, Delta State University of Science and Technology, Ozoro.*
[2] *Department of Information Systems and Technology, Delta state University of Science and Technology, Ozoro.*
[3] *Department of Software Engineering, Delta state University of Science and Technology, Ozoro.*

International Journal of Science and Research Archive, 2024, 11(02), 1555–1565

Publication history: Received on 26 February 2024; revised on 15 April 2024; accepted on 17 April 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.11.2.0652

Abstract

Since the advent of the internet and the digitization of information, more individuals and organizations have gained access to the internet, leading to a significant expansion in the size of our database systems. These databases are relied upon for day-to-day activities by individuals and organizations. Furthermore, the advancements in technology have increased the vulnerability of database management systems and enforcing adequate database security measures is of paramount importance to individuals and organizations. In this study, we deployed a hybrid approach to database security system that integrates two techniques: dynamic time-warping algorithm and voice recognition methods. The implementation follows Object-Oriented Analysis and Design procedures, utilizing SQL Management Studio 2014 for the backend and ASP.NET C# for the frontend. Our hybrid approach demonstrates enhanced database security compared to previously employed authentication measures.

Keywords: Database Security; Hybrid; Noise Reduction; Dynamic Time-Wrapping; Voice Recognition

1. Introduction

With the increase of internet penetration and improved technological system, databases play a critical role in the storage and management of large volumes of data for various purposes. The contemporary landscape of information management heavily relies on databases, which offer efficient storage and retrieval capabilities. Database security, as defined by [2], encompasses methods, instrument and control designed to protect databases from accidental and deliberate threats. Its primary goals are to ensure data security and uphold trust, being available and the level of integrity in the database [3]. A range of techniques is employed to maintain database security, including physical security, network security, access control, biometric authentication, data encryption, auditing, and logging [4]. Physical security measures aim to safeguard databases from unauthorized access or theft using tangible methods [5]. This involves securing server rooms, implementing access controls in data centres, and deploying security cameras and alarms. In the work of [6], it was proposed that authorized users can efficiently access, input, or analyse data through structured databases, which utilize queries, views, and tables to facilitate information storage and retrieval processes. Traditionally, information and resource security relied heavily on password-based authentication [7]. However, this method has inherent vulnerabilities, such as weak passwords prone to attacks and the risk of password reuse across multiple accounts [8]. Biometric security, a modern authentication method, utilizes unique physical traits like fingerprints features, facial features recognition features, or iris scans features to verify identity, offering enhanced database security compared to usual passwords [9].

It was opined by [10] the importance of network security in safeguarding databases against unauthorized network access. Measures include using firewalls, intrusion detection systems, and encryption to ensure secure data transmission over networks, preventing interception or modification of data in transit [11]. Data encryption further

* Corresponding author: Anazia Eluemunor Kizito

enhances security by encrypting stored data using encryption algorithms, rendering it unreadable to unauthorized individuals [12]. Auditing and logging are essential for monitoring and tracing all database activities to identify and prevent security breaches [13]. While these techniques have contributed to enhancing database security over the years, they have also demonstrated vulnerability to certain database threats. In order to improve security in database systems, a hybrid approach combining dynamic time-warping and voice recognition authentication systems was developed.

2. Review of Related Literature

Database security holds immense significance due to the increasing confidence on databases systems for keeping and retrieving large quantity of important database. Databases is very important part in holding information in our day present day digital [14]. Security measures in databases encompass various techniques aimed at maintaining the quality, trust, and availability of information [15]. In [16], several methods for maintaining database security are proposed, including physical security, network security, password access control, biometric authentication, data encryption, auditing, and logging. While systems that uses password have a long history [17], a comparative analysis can highlight their advantages and disadvantages [18]. Despite their simplicity and prevalence, password-based authentication solutions pose security risks and challenges [19]. In the research carried out [20], they suggested implementing strong password rules, educating users on password best practices, and potentially adding extra authentication factors to enhance password security.

Password-based authentication relies on secret character strings for identity verification [21]. Encryption techniques play a crucial role in protecting data from unauthorized access during storage and transmission [22]. Evaluation of encryption techniques for data at rest and in transit, encryption algorithms, and cryptographic protocols is essential [23]. In biometric method of authentication, it implores a special personal traits like fingerprints, iris patterns, or facial features for identification [24]. Due to the difficulty in forging or replicating biometric features, it offers improved security features [25]. Users authenticate themselves using their own biometric data [26], saving time and effort by simply demonstrating their biometric features to establish identity [27].

In [28], a model is proposed for organizations to manage security in database systems. The intrusion detection model provides information to safeguard confidential data vulnerable to unauthorized access [29].

3. Method Adopted

The system is developed using the C-Sharp Programming Language (C#) and Structural Query Language (SQL) Management Server. This setup operates within the .NET framework and is compatible with Microsoft Visual Studio 2022. Microsoft provides an API that allows developers to incorporate speech recognition features into Windows applications. Speech-to-text conversion is accomplished using the Speech Recognition libraries, while speech synthesis enables access to a text-to-speech conversion engine. Serving as a bridge between the application and the speech recognition/text-to-speech engines, the Speech API (SAPI) facilitates seamless integration. The research methodology employed in this study is the Object-Oriented Analysis and Design Methodology (OOADM) with Prototyping.

4. Methods of Data Collection

In this work, the research methodology involves gathering information from a variety of sources, such as academic papers, internet websites, and articles, all focused on securing databases using a voice recognition system (VRS). This approach aims to offer users comprehensive insights into protecting themselves from potential threats, leveraging knowledge and findings from diverse credible sources.

5. Analysis of the System

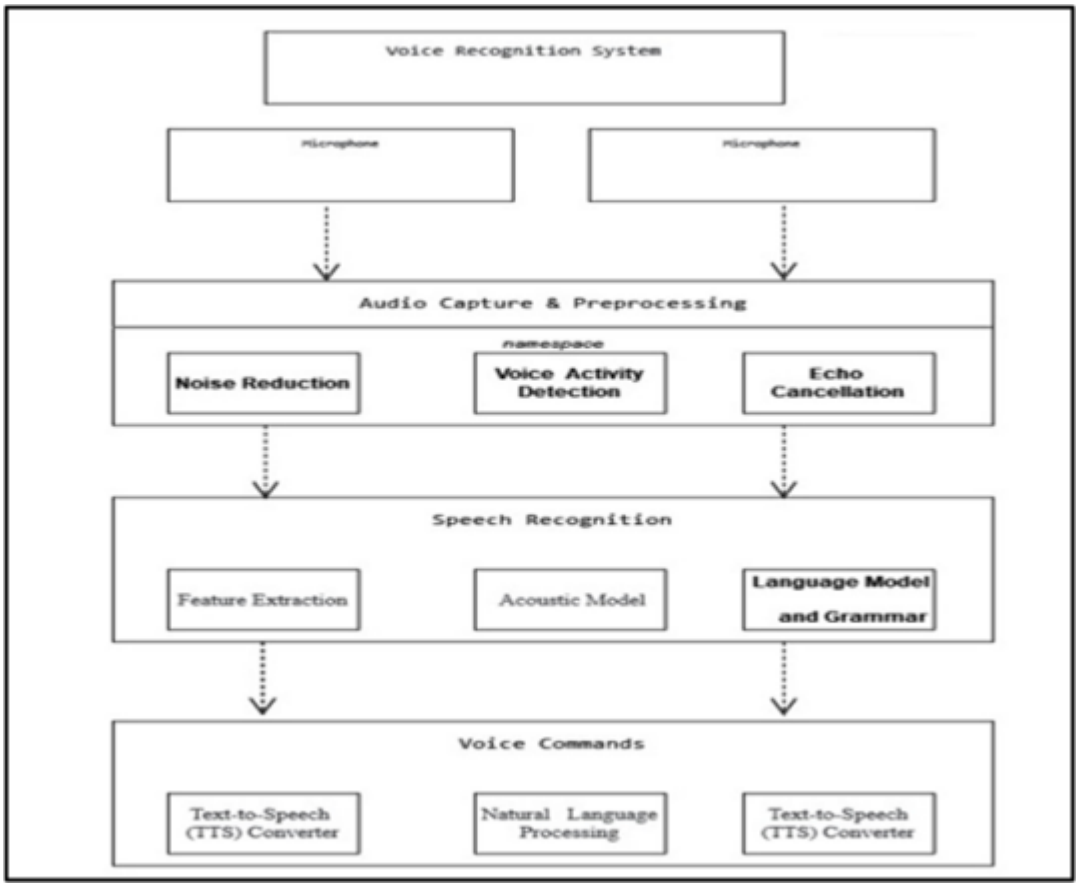

Figure 1 System Architecture Design

A voice recognition authentication system comprises several critical components that seamlessly work together to enable efficient voice-based interactions. The central components within this system include:

- Microphone: This captures the user's voice, serving as the entry point for voice commands and queries.
- Speaker: On the receiving end, the speaker provides voice output or responses to the user, ensuring effective communication.
- Audio Capture & Preprocessing: This segment includes essential functions such as:
  - Noise Reduction: Filters out background noise to enhance audio quality, enabling the system to focus on the user's voice.
  - Voice Activity Detection: Identifies when the user is speaking, activating the system to respond promptly.
  - Echo Cancellation: Removes unwanted echo from the audio, resulting in clearer voice communication.
- Speech Recognition: This is the core functionality of the system, involving several components:
  - Feature Extraction: Extracts relevant acoustic features from the voice input, laying the groundwork for understanding spoken words.
  - Acoustic Model: Matches extracted features with known speech patterns, accurately converting voice input into text.
  - Language Model and Grammar: These elements help the system understand the context and language used in voice commands, ensuring appropriate comprehension and responses.
- Voice Commands: This segment relates to the system's ability to respond effectively, including:

Text-to-Speech (TTS) Converter: Converts recognized text into spoken responses, enabling audible communication with the user.

Natural Language Processing (NLP): Processes and understands user commands more deeply, allowing the system to interpret and act on complex instructions and queries.

6. Mathematical Model Specification

6.1. Variables:

- A: Set of audio samples.
- T: Set of text transcripts corresponding to the audio samples.
- H: Set of hypotheses generated by the voice recognition system.
- $P(H|A)$: Probability of a hypothesis given the audio.
- $P(A|H)$: Probability of audio given a hypothesis.
- $P(H)$: Prior probability of a hypothesis.
- $P(A)$: Prior probability of audio data.
- $P(T|H)$: Probability of text transcripts given a hypothesis.

6.2. Equations

Bayes' Theorem: $P(H|A) = (P(A|H) * P(H)) / P(A)$

This theorem showed above indicts the probability of a hypothesis given the audio data is computed using the probability of audio given the hypothesis, the prior probability of the hypothesis, and the prior probability of audio data.

Hypothesis Generation: $H = f(A)$

This equation represents the process by which hypotheses are generated from the audio data using the voice recognition system. The function $f()$ represents the system's internal processes.

Text Transcript Probability: $P(T|H) = g(H)$

This equation defines how the probability of text transcripts is computed given the hypotheses generated by the system. The function $g()$ captures the mapping between hypotheses and text transcripts.

6.3. Constraints

Normalization Constraint: $\sum HP(H|A) = 1$

Probabilities of all available hypotheses given the audio data must sum to 1, ensuring that one of the hypotheses is correct.

Non-Negativity Constraint: $P(H|A) \geq 0$

The probability of any hypothesis given the audio data should be non-negative.

Consistency Constraint: $P(T|H) \geq 0$

The probability of text transcripts given a hypothesis should also be non-negative.

7. Program Module Specification

- The User Authentication Module: This module acts as the primary gatekeeper for the system, tasked with verifying user identities. It combines traditional username and password verification with voice recognition technology, allowing for secure system access.
- Voice Enrolment Module: In this module, users have the opportunity to enrol their voice patterns during the registration process. It captures and stores voice samples in the system's database, creating voice pattern templates for future comparisons.
- Database Management Module: Central to the system, this module handles a variety of database operations including user data, voice templates, and audit logs. It accepts database queries and requests as inputs, providing data retrieval, updates, and logging as outputs, ensuring data integrity and accessibility.
- Voice Recognition Module: At the core of the voice authentication process, this module performs voice pattern matching using the Dynamic Time Warping (DTW) algorithm. It compares captured voice patterns with

enrolled voice templates, generating DTW similarity scores and authentication results to determine if a user's voice pattern matches the enrolled template.

- User Interface Module: This module offers user-friendly interfaces for administrators and end-users alike. It manages user interactions and commands, presenting interface elements and providing feedback to enhance the user experience.
- Integration Interface Module: Facilitating integration with external systems and services through APIs, this module processes integration requests and data. It enables data exchange and interaction with external systems, expanding the system's capabilities

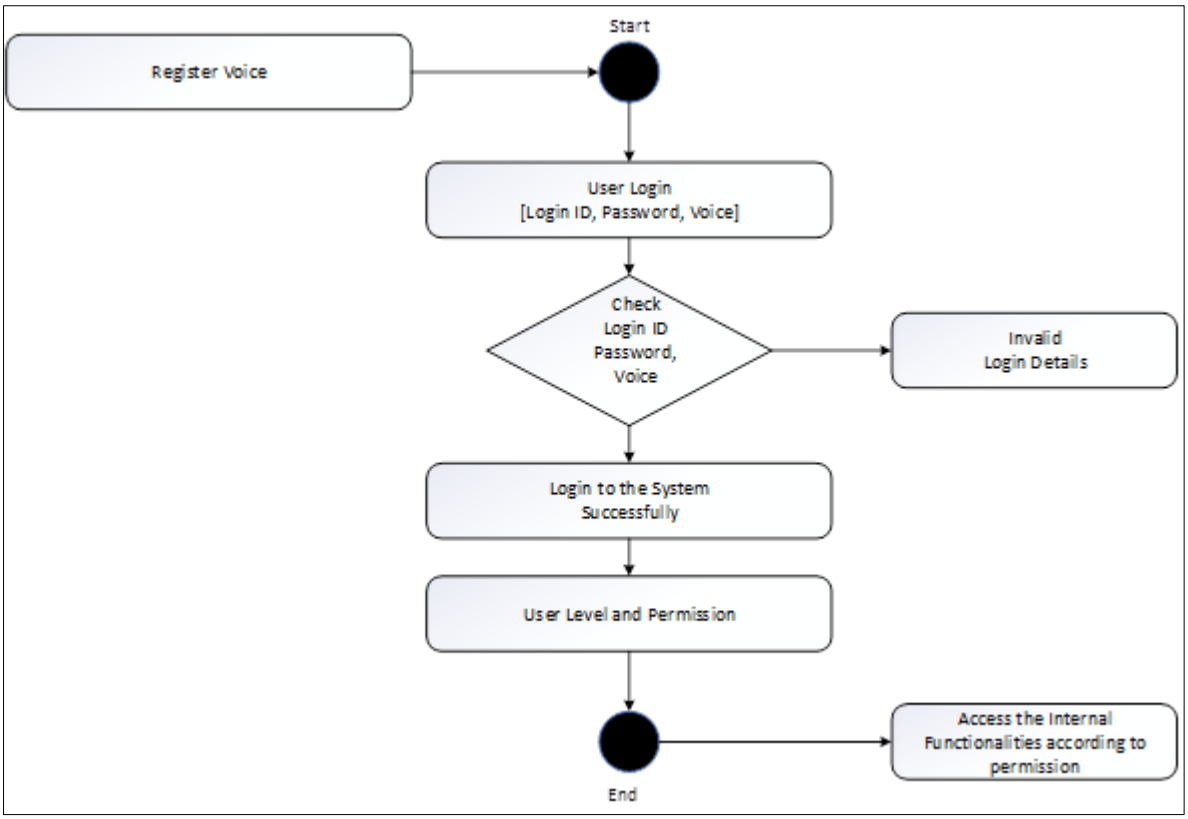

Figure 2 Activity Diagram

8. System Implementation

The System Implementation phase signifies the transition from conceptual design to a functional Examination Verification System. This phase involves several critical components and steps:

User Management Module: Developed to handle user registration, login, profile management, and access control.

Data Processing Module: Central to processing acquired biometric data and comparing it with stored data. This includes implementing biometric matching algorithms and setting matching thresholds for accurate user identity verification.

Voice and Verification Module: Responsible for the final steps of identity verification based on biometric data matching. This module is crucial for system security and must be fortified against potential threats.

User Interface (UI): Developed to interact effectively with users, including login screens, registration forms, and user dashboards. The UI design prioritizes user-friendliness and accessibility for a seamless user experience.

In Program Development Stage:

- Software Components: this is designed with precision and expertise by skilled developers utilizing the C-Sharp (C#) programming language within the .NET framework Core components include the user authentication module, voice recognition system, database management, access control, and audit logging.
- Database Implementation: The database structure, previously designed, is implemented using a Structured Query Language (SQL) Management Server. This ensures optimal storage and management of user data, access control policies, and security policies.
- Algorithm Integration: In this section, the merging of the voice patterns recorded and the sample of the voice sample collected are integrated by the Dynamic Time Warping algorithm. This requires developing voice processing and DTW calculation components to ensure effective functioning of the system's core security feature.

9. System Requirements

The database security system with voice recognition has specific requirements to ensure its effective and secure operation. These requirements cover various aspects, including hardware, software, security, and user experience. Here are the key system requirements:

9.1. Hardware Requirements

Microphone, audio input devices and user devices

Software Requirements: Operating system, database management system, speech recognition engine and speech synthesis engine:

Development Tools

10. Choice of Programming Environment

The selection of a programming language plays a pivotal role in shaping the development and performance of a system. In this context, Microsoft Visual Studio 2022 stands out as the designated integrated development environment (IDE). Its tight integration with the .NET framework, which serves as a fundamental component of the system, simplifies development tasks and guarantees compatibility. Notably, the inclusion of speech recognition and synthesis tools within Visual Studio enhances the system's voice recognition capabilities. These tools enable accurate processing of voice patterns and secure storage, thereby enhancing the system's efficiency and dependability.

10.1. Output Interface Result

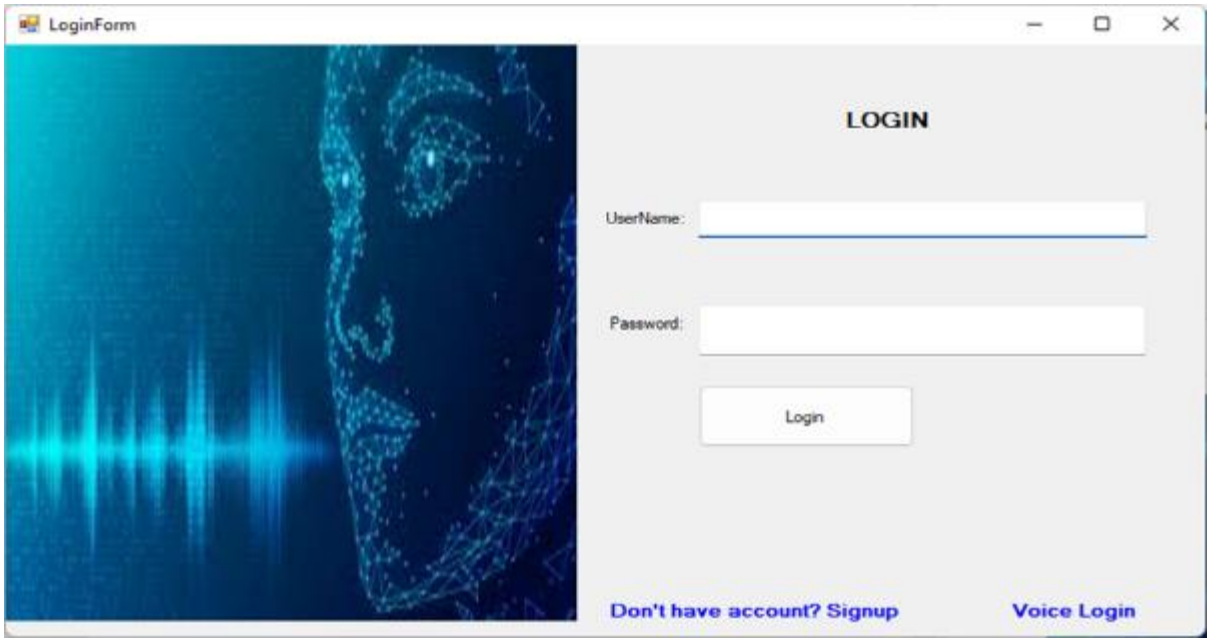

Figure 3 Alternative Login interface

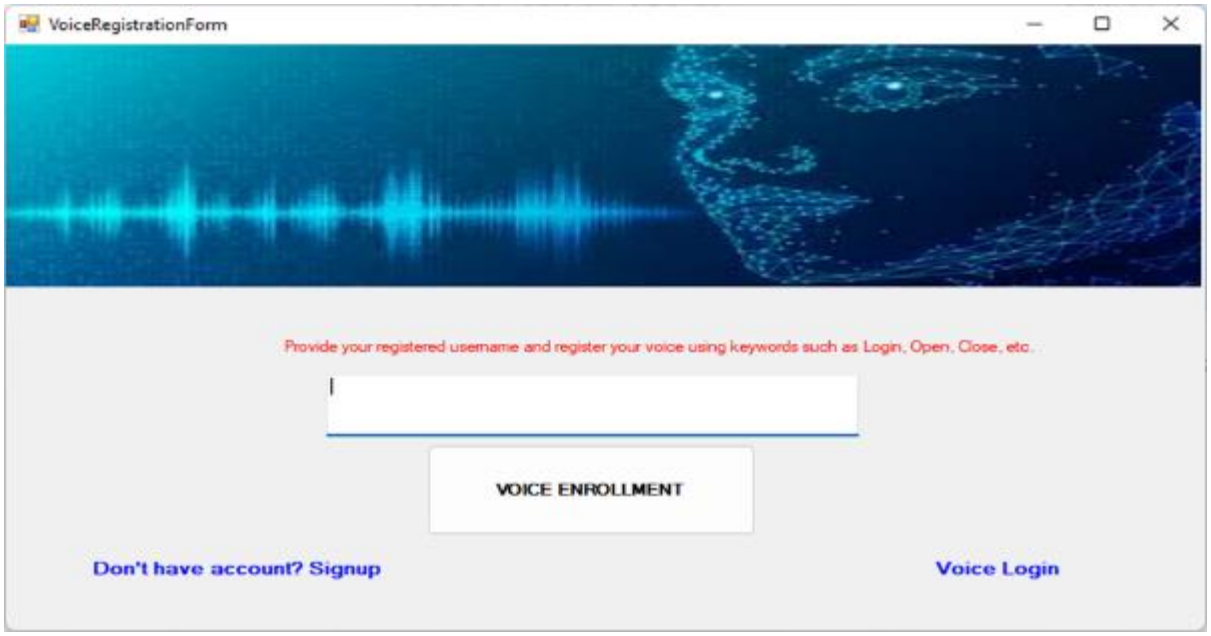

Figure 4 Voice Enrolment Interface

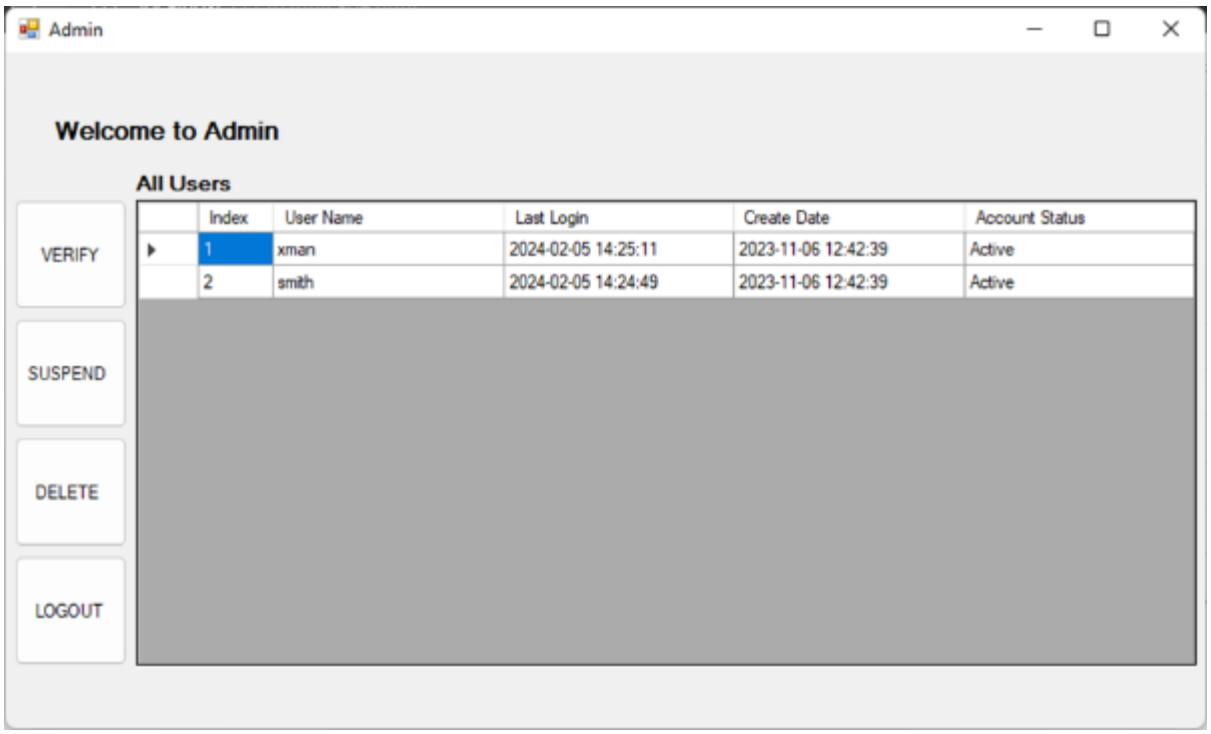

Figure 5 Admin Login successful to Dashboard Interface

11. Result Evaluation Performance

The table below with the performance metrics shows the evaluation performance of the system.

Where True Positives (TP) denote instances correctly authenticated, True Negatives (TN) represent instances correctly rejected, False Positives (FP) are instances incorrectly authenticated, and False Negatives (FN) are instances incorrectly rejected.

$$Accuracy = (True\ Positives + True\ Negatives) / (True\ Positives + True\ Negatives + False\ Positives + False\ Negatives)$$

$$Precision = True\ Positives / (True\ Positives + False\ Positives)$$

$$Sensitivity = True\ Positives / (True\ Positives + False\ Negatives)$$

$$F1\ Score: 2 * (Precision * Recall) / (Precision + Recall)$$

Table 1 Evaluation Metrics for the System's Performance

Scenario	True Positives (TP)	True Negatives (TN)	False Positives (FP)	False Negatives (FN)	Accuracy	Precision	Sensitivity
1	20	30	5	5	0.8	0.8	0.8
2	15	25	10	5	0.6	0.6	0.75
3	25	35	5	10	0.8	0.833	0.714
4	18	28	7	7	0.72	0.72	0.72
5	22	32	3	8	0.78	0.88	0.733

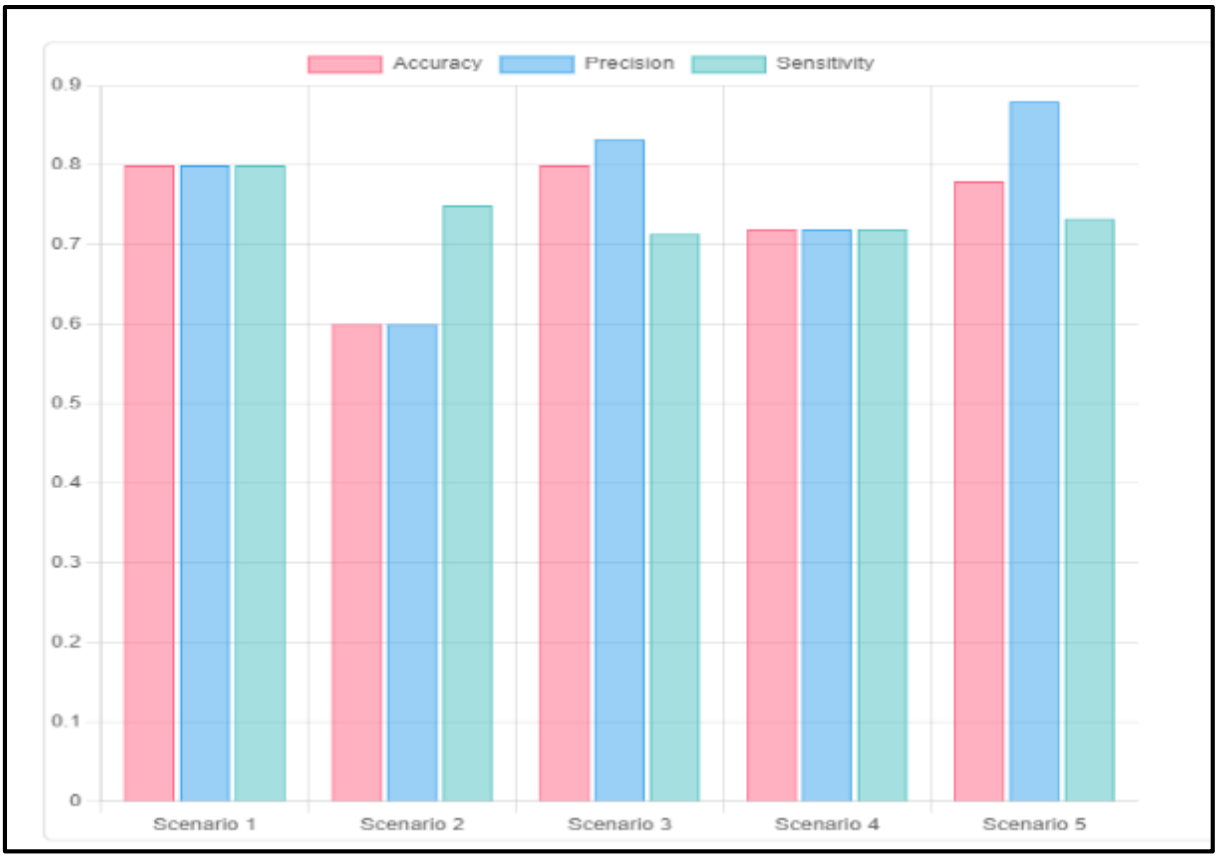

Figure 6 Bar Chart Showing the System Metric for Performance Evaluation

12. Discussion of Results

The output of the performance evaluation metrics shows how effective and efficient database security system is.

Accuracy: Across different scenarios, accuracy values range from 0.6 to 0.8, indicating a moderate to high level of correctness in authentication predictions. Higher accuracy values observed in Scenarios 1, 3, and 5 (0.8) suggest robust performance in correctly classifying both positive and negative authentication cases. This indicates a strong overall ability of the system to accurately authenticate users based on their voice patterns.

Precision: This detects the accuracy of positive indices displayed by the system, particularly relevant for minimizing false positives. Precision values range from 0.6 to 0.88 across scenarios, with Scenario 5 demonstrating the highest precision value of 0.88. This suggests that the system excels in accurately predicting positive authentication cases, crucial for maintaining security by avoiding unauthorized access.

Sensitivity (Recall): Sensitivity evaluates the system's power to predict positive authentication cases, crucial for minimizing false negatives. Sensitivity values range from 0.714 to 0.8 across scenarios, with Scenario 1 exhibiting the highest sensitivity value of 0.8. This indicates that the system effectively identifies positive authentication cases without missing them, ensuring a high level of security by preventing legitimate users from being falsely rejected.

Overall, the results suggest that the database security system incorporating dynamic time-warping voice recognition demonstrates promising performance in authentication. The system exhibits strong accuracy, precision, and sensitivity values across various scenarios, indicating its effectiveness in reliably authenticating users based on their voice patterns. These results are encouraging and suggest that the system could be a valuable tool for enhancing the security of database access through advanced authentication mechanisms. However, further testing and refinement may be necessary to address any potential limitations and optimize the system's performance for real-world deployment.

13. Summary

This work addresses the pressing need for enhanced database security by introducing a dynamic time-warping voice recognition database security system. Traditional username and password authentication methods have long been vulnerable to security risks. In order to manage these drawbacks, the project integrates voice recognition as an additional layer of authentication, promoting multi-factor authentication, data privacy, and seamless integration with existing login processes. Leveraging the Object-Oriented Analysis and Design Methodology with prototyping, the system utilizes C-Sharp (C#) and SQL Management Server on the .NET framework, alongside Microsoft's Speech Recognition engine for voice recognition.

The research methodology draws from a wide array of secondary sources, including papers, internet websites, and articles, to provide a comprehensive overview of the subject matter. System analysis highlights the limitations of traditional authentication methods, emphasizing the vulnerabilities associated with passwords. The work incorporates best practices, inspired by prior research efforts exploring the use of One-Time Passwords (OTPs) to bolster security. Additionally, the project introduces a mathematical model for dynamic time-warping voice recognition to match captured voices with enrolled voice templates.

System specifications encompass database development tools, data types, and field descriptions, ensuring that the system is constructed with security and usability in focus. The research project also introduces control centers, submenus, and subsystems, underlining the importance of a user-friendly interface. Mathematical specifications outline the technical intricacies of the DTW model, and dynamic time-warping calculations are detailed to elucidate how voice recognition is achieved.

14. Conclusion

In conclusion, this work presents a compelling solution to persistent challenges in database security by introducing a robust database security system deploying a hybrid security system of dynamic time-warping algorithm and voice recognition authentication mechanism. Traditional username and password authentication methods have demonstrated vulnerability to security risks, emphasizing the necessity for innovative approaches. Integrating dynamic time-warping algorithm and voice recognition authentication mechanism offers a multi-factor authentication system that significantly enhances security, data integrity, and user experience in accessing sensitive information. Through an in-depth exploration of existing research, the work identifies the limitations of traditional authentication methods, underscoring the critical need for improved security measures. Building upon prior research on One-Time Passwords (OTPs), the system incorporates best practices to enhance security and reliability.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Reference

[1] Blocki, J., Harsha, B. and Zhou, S. (2018). On the Economics of Offline Password Cracking. In: 2018 IEEE Symposium on Security and Privacy (SP).

[2] Sakshi, K., Anderson, R., and Moore, T. (2017). Information Security: The Complete Reference. McGraw-Hill Education.

[3] Erez, G. Mubina, M. Trisha, P. (2014). Database Encryption Architectures, International Journal of Scientific & Engineering Research, Volume 7, Issue 12, 313 ISSN 2229-5518

[4] Adigwe, W. and Anazia, E. K. (2020). Sentiment Analysis Using Neural Network, International Journal of Trend in Research and Development, Volume 7(1), ISSN: 2394-9333 www.ijtrd.com IJTRD | Jan –Feb 2020 Available Online@www.ijtrd.com

[5] Chen, Y. and Liginlal, D. (2017). Bayesian Networks for Knowledge-Based Authentication. IEEE Transactions on Knowledge and Data Engineering, 19 (5), pp.695-710.

[6] Harba, L. (2015). Multi-Tier Web Server System with a Focus on Security, International Journal of Computer Science and Information Technologies, page 374.

[7] Spitzner, L. (2019). Time for Password Expiration to Die [Internet]. Available from https://www.sans.org/security-awareness training/blog/time-password-expiration-die.

[8] Jain, A.K., Hong, L., Pankanti, S. and Bolle, R. (2012). An Identity Authentication System Using Fingerprints. Proceedings of the IEEE, 85 (9), pp.1365-1388.

[9] Thakkar, D. (2021). Unimodal Biometrics vs. Multimodal Biometrics [Internet]. Available from https://www.bayometric.com/unimodal-vs multimodal/

[10] Tiwari, A., Johnson, T. S., and Rodriguez, A. M. (2011). Enhancing Information System Security with Biometric Authentication. International Journal of Information Assurance, 15(3), 235-249.

[11] Karim, A. (2019). Full Encryption Model for Database Security Based on Encryption Classes. A Review, International Journal Of Scientific & Technology Research, Vol 1, Issue 1.

[12] Kuppuswamy, B. and Chandrasekhar, A. (2011). Development of an Encrypted Database System to Enhance Data Security. IEEE Transactions on Dependable and Secure Computing, 4(3), pp 165-179.

[13] Mohamed, M. A., and Martono, P. S. (2019). Enhancing Database Security with Multimodal Biometrics. In Proceedings of the International Symposium on Security (pp. 78-93). ACM.

[14] Abouelmehdi, K. Beni-Hssane, A. Khaloufi, H. and Saadi, M. J. P. C. S. (2017). Big Data Security and Privacy in Healthcare: A Review," vol. 113, pp. 73-80.

[15] Karimovich, G.S. and Turakulovich, K.Z. (2016). Biometric cryptosystems: Open issues and challenges. In: 2016 International Conference on Information Science and Communications Technologies (ICISCT).

[16] Hejase, .H. J. Fayyad-Kazan, H. F. Moukadem, I. J. J. O. E. and E. E. Research (2020). Advanced Persistent Threats (apt): An Awareness Review, vol. 21, no. 6, pp. 1-8.

[17] Toke, J. (2014). Implementing AES Encryption on FPGA for Efficient Encryption of Biometric Image Data. IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 21-30.

[18] Hann, M. (2021). Cryptography Implementation in a Database Using Java and MySQL to Prevent Unauthorized Access and Data Tampering. New Generations (ITNG), 2013 Tenth International Conference on, vol., no., pp.422-427, 15-17.

[19] Chen, J., and Wang, L. (2020). Improving Voice Authentication Through Dynamic Time-Warping. Journal of Applied Information Security, 12(3), 221-236.

[20] You, F. Zhang, C. Cao, Y. Gong, H. Zhang, C. and J. Liao, (2018). `Data Masking System Based on Ink Technology, Proc. 5th Int. Conf. Inf. Sci. Control Eng. (ICISCE), Jul. 2018, pp. 176_180, doi: 10.1109/ICISCE.2018.00046.

[21] Zheng, W. Zheng, Z. Chen, X. Dai, K. Li, P. and Chen,` R. (2019). Nutbaas: A Blockchain-as-a-Service Platform,'' *IEEE Access*, vol. 7, pp. 134422_134433.

[22] Chan, K. C. Zhou, X. Gururajan, R. Zhou, X. Ally, M. and Gardiner, M. (2019). `Integration of Blockchains with Management Information Systems, Proc. Int. Conf. Mechatronics, Robot. Syst. Eng. (MoRSE), pp. 157_162, doi: 10.1109/MoRSE48060.2019.8998694.

[23] Khan, N., and Zahid, M. (2021). The use of biometric technology at airports: The case of customs and border protection (CBP). International Journal of Information Management Data Insights, 1(2), 100049.

[24] [H. Cui, Z. Chen, Y. Xi, H. Chen, and J. Hao, ``IoT data management and lineage traceability: A blockchain-based solution, *Proc. IEEE/CIC Int. Conf. Commun. Workshops China (ICCC Workshops)*, Aug. 2019, pp. 239_244, doi: 10.1109/ICCChinaW.2019.8849969

[25] Albalawi, U. (2018). Countermeasure of Statistical Inference in Database Security, Proc. IEEE Int. Conf. Big Data (Big Data), Dec. 2018, pp. 2044_2047, doi: 10.1109/BigData.2018.8622241.

[26] Jing-wei, P. Min, Z. Ping, C. and Wei-guang, X. (2019). A Lightweight Vulnerability Scanning and Security Enhanced System for Oracle Database, Proc. IEEE 4th Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC), pp. 1699_1702, doi: 10.1109/IAEAC47372.2019.8997534.

[27] Chiew, A.A., Yong, S.A., and Tan, F.A. (2018). Biometric Approach as a Means of Preventing Identity. African Scholars Journal of Science Innovation & Tech. Research (JSITR-9), 24(9), 149-164.

[28] Egbunike C. and Rajendran, S. (2017). The Implementation of Negative Database as a Security Technique on a Generic Database System, Proc. Int. Conf. Circuit, Power Comput. Technol. (ICCPCT), pp. 1_8, doi: 10.1109/ICCPCT.2017.8074342.

[29] Odirichukwu, J. C. and Asagba, P. O. (2017). Security Concept in Web Database Development and Administration Review Perspective, Proc. IEEE 3rd Int. Conf. Electro-Technol. Nat. Develop. (NIGERCON), pp. 383_391, doi: 10.1109/NIGERCON.2017.8281910 [T. M. Zaw, M. Thant, and S. V. Bezzateev].