IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

An Enhanced Database Security System using Dynamic Time-Warping Voice Recognition Technique

Chukwudi Joseph Chukwuluba[1], Omede Gracious Chukwunweike[2], Edje E. Abel[3], Okaro Frank[4]
Post Graduate Student, Department of Computer Science, Delta State University, Abraka, Nigeria[1]
Lecturer, Department of Computer, Delta State University, Abraka, Nigeria[2]
Head of Department, Department of Computer Science, Delta State University, Abraka, Nigeria[3]
Researcher, IT Department, White dove web world, Abraka, Nigeria[4]
jdahilan@ssct.edu.ph, rencarnacion@ssct.edu.ph

Abstract: *In the rapidly evolving digital landscape, ensuring the security of personal and corporate data stored in Database Management Systems (DBMS) is a top priority. Current data protection methods, primarily reliant on passwords and UserID/PIN protection, are vulnerable to hacking and unauthorized access. This project addresses these shortcomings by introducing an advanced secured database system that utilizes dynamic time-warping voice recognition technology to enhance security. Existing data protection methods have significant limitations, necessitating a more robust and intuitive authentication system. The proposed system employs voice recognition with dynamic time-warping algorithms, which can discern unique voice patterns to offer a sophisticated and secure authentication method. By analyzing distinct vocal attributes, the system adds an extra layer of security, reinforcing data protection against potential threats. The project uses an Object-Oriented Analysis and Design Methodology (OOADM) with a Prototyping development approach, allowing for continuous refinement based on evolving requirements. The front end, designed using ASP.NET C#, provides an accessible and user-friendly interface for administrators. The back end utilizes SQL Management Studio 2014, ensuring efficient and secure data storage and retrieval. Integrating voice recognition technology enhances security, reduces reliance on traditional passwords, and improves user experience. System evaluation findings demonstrate a significant improvement in data protection with the implementation of voice recognition technology. Performance metrics, including accuracy, precision, and sensitivity, indicate that dynamic time-warping algorithms effectively authenticate users based on their unique vocal attributes, mitigating risks associated with conventional methods. In conclusion, the proposed system shows promising results in reinforcing database security and enhancing user authentication. It is recommended to implement this advanced secured database system in real-world scenarios, providing organizations with a reliable and innovative solution to bolster data protection in today's dynamic digital landscape*

Keywords: Dynamic Time-Warping (DTW), Voice Recognition, Database Security and Authentication Systems

I. INTRODUCTION

In the digital era, databases play a crucial role in storing and managing vast amounts of information for various purposes. Relational databases, which organize data in a tabular form, are widely used to support data storage and retrieval processes. With the increasing reliance on databases, the need for robust security measures to protect the confidentiality and integrity of stored data has become paramount [1].

Databases play a crucial role in modern information management, providing efficient storage and retrieval of data. The relational database model, with its tabular structure, is widely adopted for organizing and accessing data in various industries. Additionally, distributed databases allow data to be replicated and shared across multiple network points, enhancing accessibility and availability (Sweety and Dhande, 2020). Databases enable authorized users to access, enter,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

or analyze data quickly and easily. They consist of queries, views, and tables, with data organized to support information storage and retrieval processes. A Database Management System (DBMS) is computer software designed to manage all the databases installed on a system's hard drive or network [2].

Biometric technology uses unique feature parameters as a password. These parameters are distinct for each individual, even for twins. Therefore, the voice recognition system is secure for the administrator user. Voice recognition is a natural means of communication for humans. In this project, we study voice recognition and develop a voice recognition system to enhance database security. To address these security challenges, researchers and practitioners have explored alternative authentication methods that offer stronger protection against unauthorized access. One such method is voice recognition, which leverages the unique characteristics of an individual's voice to verify their identity. Voice recognition systems analyze factors such as pitch, tone, and pronunciation to create voice templates for authentication. Voice recognition technology has gained significant attention due to its potential to provide a more secure and convenient authentication mechanism. By incorporating voice recognition into the database login process, organizations can enhance the security of their systems and mitigate the risks associated with password-based authentication [3].

This study builds upon existing research and aims to develop a secured database system using voice recognition technology. The goal is to create a system that combines traditional username and password authentication with voice recognition capabilities, providing a multi-factor authentication approach. The integration of voice recognition technology into the database login process offers the potential to enhance security, improve user experience, and mitigate the risks associated with password vulnerabilities.

II. STATEMENT OF THE PROBLEM

The conventional approach to database access, relying on usernames and passwords, introduces vulnerabilities as passwords are susceptible to compromise or theft, posing significant threats to the security and integrity of stored sensitive data. This imperative concern underscores the need for an enhanced login process, demanding a more secure and reliable authentication method.

While previous research, exemplified by [4], has delved into security threats associated with databases, it has failed to furnish a comprehensive model for safeguarding data security and integrity. Likewise, the work of [5], which proposed an authorization mechanism using One-Time Passwords (OTP) for relational databases, still leaves exploitable vulnerabilities open to malicious actors.

In response to these inadequacies, this project advocates for the integration of a voice recognition system into the login process. The objective is to overcome the identified challenges by proposing the development of a secured database login system. This innovative system merges traditional username and password authentication with the cutting-edge technology of voice recognition. Through the incorporation of voice recognition technology, the system aims to elevate security measures, enhance user authentication, and establish a more resilient and dependable login process for database access. This amalgamation of authentication methods strives to provide a holistic and effective solution to the existing vulnerabilities in the conventional login processes, ultimately fortifying the overall security posture of database systems.

III. REVIEW OF RELATED WORKS

[6] proposed the fusion of face and voice biometrics using the Dempster-Shafer theory for person verification. This fusion occurs at the score level and is applied to face and voice biometrics to address the limitations of single-modal biometric systems.

[7] introduced a multimodal biometric scheme for human authentication, combining voice and face recognition. The study explores the effectiveness of this approach using cepstral and statistical coefficients for voice recognition and various face extraction techniques, including Eigenface and Principal Component Analysis. Different classifiers are employed, such as the Gaussian Mixture Model, Artificial Neural Network, and Support Vector Machine. The results indicate that scores fusion offers promising results.

In a study by [8], an efficient Android-based multimodal biometric authentication system is developed, incorporating both face and voice. They propose an improved Local Binary Pattern (LBP) algorithm to enhance the robustness of face

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

feature extraction, coupled with a voice activity detection (VAD) method. The study demonstrates high accuracy authentication rates of 98% for face and 89% for voice on Android-based smart terminals.

In a more recent study, [5] proposed a Database Security Framework Design Using Tokenization. This work introduced the concept of tokenization, which involves replacing or substituting sensitive data with a token. The authors argued that tokenization could serve as an additional technique for protecting sensitive data in higher education institutions and other organizations that handle such data.

IV. METHODOLOGY ADOPTED

The methodology adopted for this research work is the Object-Oriented Analysis and Design Methodology (OOADM) with Prototyping. The system is designed and implemented using the C-Sharp Programming Language (C#) and Structural Query Language (SQL) Management Server. This system is developed on the .NET framework and runs on Microsoft Visual Studio 2022. Microsoft provides an API that allows developers to use speech recognition and speech synthesis engines in Windows applications. Speech-to-text conversion is accomplished with the Speech Recognition engine, while speech synthesis provides access to a text-to-speech conversion engine. The Speech API (SAPI) acts as an interface between the application and the speech recognition/text-to-speech engines.

V. PROPOSED SYSTEM

The proposed system is a secured database system that leverages a Voice Recognition System (VRS) to enhance user authentication. It is equipped with several major components, including an acoustic front-end, acoustic model, lexicon, language model, and decoder. The Dynamic Time Warping (DTW) algorithm enhances the functionality of the proposed secured database system using a Voice Recognition System (VRS) by aiding in the alignment of acoustic patterns during both feature extraction and recognition stages. DTW ensures that variations in speech timing and speed are accounted for, contributing to the system's accuracy and reliability in voice-based user authentication.

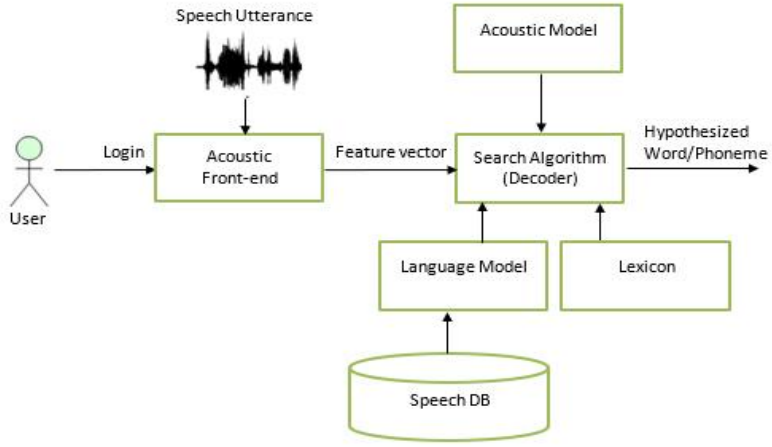

Fig. 1. High-level of the Proposed System

The algorithm of the proposed system is given thus:

Step 1: Data Preprocessing:

Record and digitize the input voice signal.

Divide the voice signal into frames (typically 10-30 milliseconds).

Extract features from each frame (e.g., MFCC coefficients, energy, pitch).

Create a feature matrix where each row represents the features of a frame.

Step 2: Training:

Collect a dataset of known voice samples (both positive and negative samples, i.e., speakers you want to recognize and those you don't).

Extract features from the training samples.

For each training sample, compute a distance matrix using DTW against all frames of the training sample.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

Step 3: Voice Recognition:
Record and digitize the input voice signal to be recognized.
Divide the input voice signal into frames and extract features, as in step 1.
For each test frame, compute a distance matrix using DTW against all frames of the training samples.
Step 4: DTW Algorithm:
Initialize a 2D matrix of size (M, N) where M is the number of frames in the input signal, and N is the number of frames in the training sample.
Initialize the first row and first column of the matrix with infinity (or a large value) to represent the cost of starting from any point.
For each cell in the matrix (excluding the first row and column):
Compute the local cost, which is a distance metric (e.g., Euclidean distance) between the feature vectors of the test frame and the training frame.
Update the cell with the minimum accumulated cost from the three neighboring cells above, left, and upper left, plus the local cost.
Traverse the matrix to find the minimum cost path from the bottom-right cell to the top-left cell. This represents the best alignment between the test frame and the training frames.
Compute the cumulative distance as the sum of the minimum path costs.
Step 5: Recognition Decision:
Calculate a recognition score for the input voice signal based on the cumulative distances for each test frame.
Compare the recognition score to a threshold to make a decision. If the score is below the threshold, consider it a rejection (unknown speaker); otherwise, it's recognition (known speaker).
Step 6: Output:
Return the recognized speaker's identity or a rejection result.

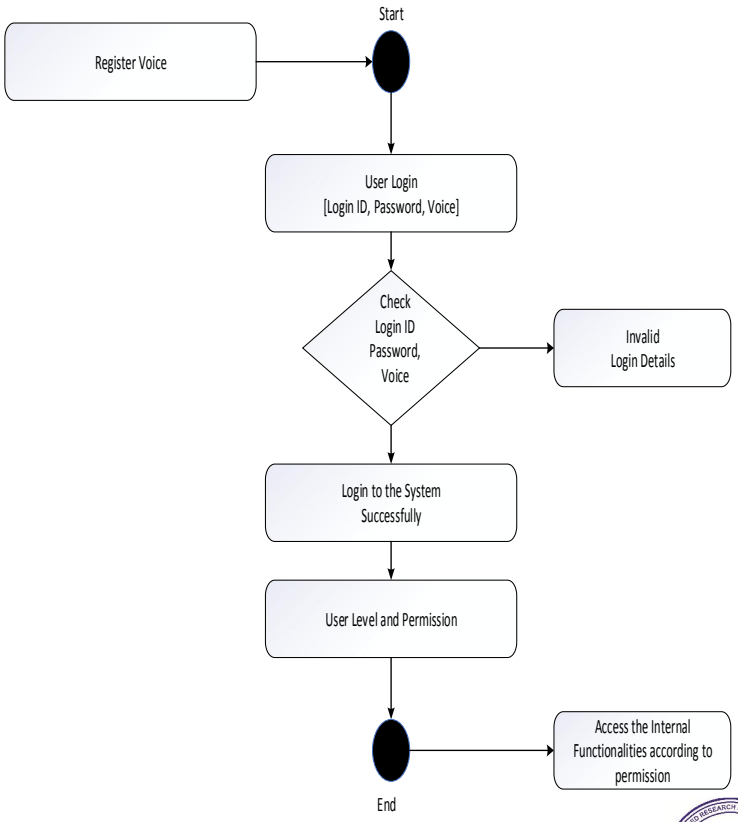

Fig. 2.Activity Diagram for voice recognition system

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

The activity diagram in Fig. 2 outlines the main steps involved in the login authentication process of a voice recognition system, from capturing the user's voice sample to granting access upon successful authentication.

VI. EXPERIMENTAL RESULT

The system operates through two distinct sessions: the user session and the admin session.

The user session commences with the user accessing the window application software installed on their computer system. Activation of the software application is initiated by clicking on the software icon displayed on the desktop.

Upon launching the application, the user is presented with the Voice Login page. This page serves as the gateway for users to authenticate themselves using their voice. The interface comprises various buttons, including the start voice authentication button, exit button, signup link button, and alternative login option. The appearance of the Voice Login page is illustrated in Fig.3.

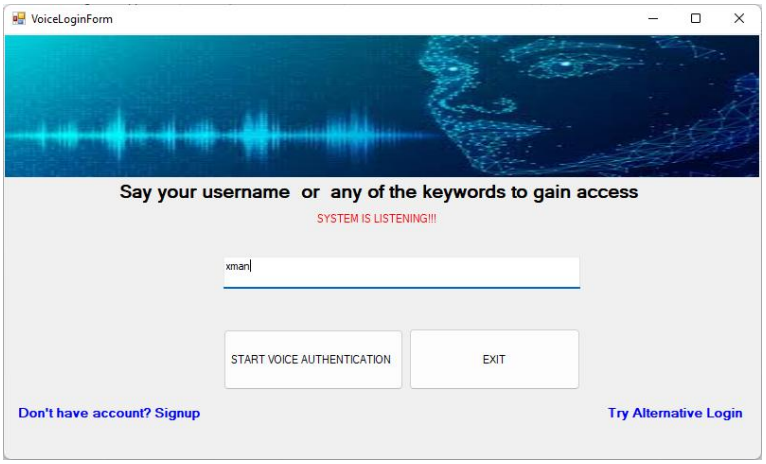

Fig. 3. Voice Login interface.

When users click on the "Signup" button on the Voice Login page, they are seamlessly redirected to the registration page, designed to streamline the account creation process within the system. Illustrated in Fig 4, this page functions as a comprehensive form where users can input their details.

The registration page is thoughtfully crafted with fields to accommodate essential user information, such as their preferred username and password. These details are crucial for establishing a distinctive user profile and unlocking access to the system's full range of features and functionalities.

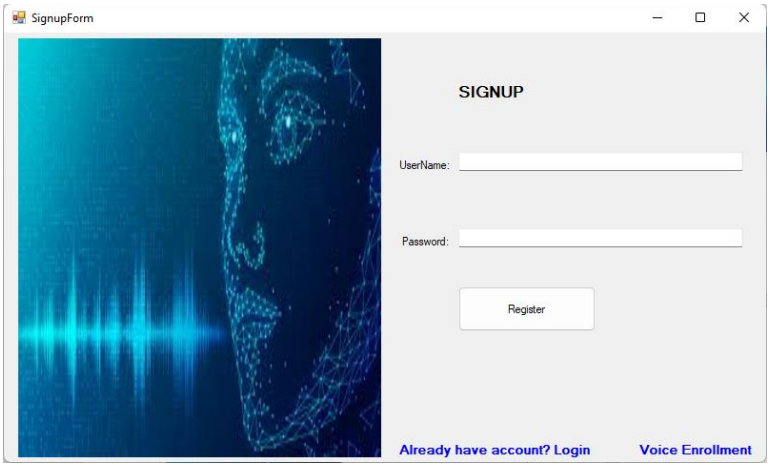

Fig. 4. User Account Registration Interface.

Following successful registration of user details, users proceed to voice enrolment to register their unique vocal patterns. Users have the flexibility to enroll their voice using keywords such as "Login," "Open," "Close," etc.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

Upon completion of the registration process, user accounts undergo verification by the administrator. This crucial step ensures the integrity and security of the system before granting users access to their respective dashboards. The appearance of the Voice Enrolment page is illustrated in Fig 5, serving as a visual reference for users interacting with the system.

Fig. 5. Voice enrolment interface.

Upon successful completion of the voice enrolment process, users are directed to the login page, as illustrated in Fig.6. This pivotal page prompts users to input their designated username and password, serving as the primary means for accessing the system.

Functioning as a secure gateway, the login page validates users' credentials against registered accounts within the system. By correctly entering their username and password, users authenticate their identity, thus gaining entry to the system's array of features and resources.

Alternatively, users have the option to utilize voice authentication for logging in. In the voice login method, users are prompted to articulate any of the keywords utilized during the voice enrolment process. Upon successful verification of the user's voice, access to their personalized account within the system is securely granted, ensuring a seamless and intuitive user experience.

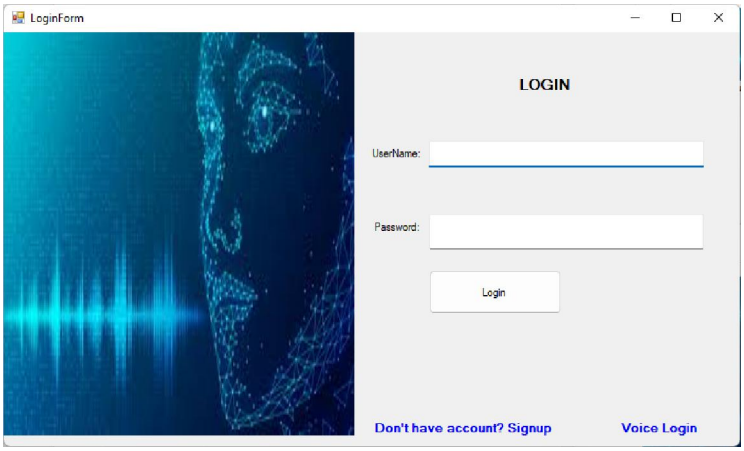

Fig. 6. Alternative Login Interface.

The user dashboard, depicted in Fig.7, stands as the central nexus facilitating user interaction with the system's diverse features and functionalities. Crafted with a user-centric design, it offers an intuitive interface empowering the user to seamlessly navigate through distinct sections, access pertinent information, execute administrative duties, and fine-tune their account settings.

Functioning as a dynamic control panel, the user dashboard empowers users to effectively harness the system's capabilities, ensuring efficient management of tasks and responsibilities. Whether accessing critical data, initiating

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

actions, or customizing preferences, the user dashboard serves as a pivotal tool for optimizing user experience and productivity within the system.

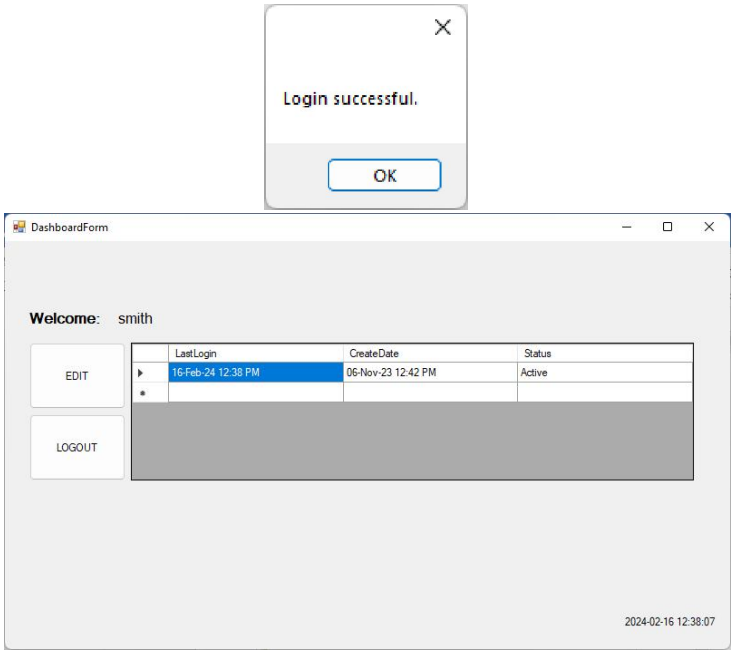

Fig. 7. User Dashboard Interface.

The password change process, depicted in Fig. 8, ensures a secure transition for users updating their credentials within the system. To initiate the change, users must first input their current password, followed by entering the new password. Upon successful verification of the old password and clicking the "Update Password" button, the system promptly activates the new password for the user's account.

This functionality serves a critical purpose in bolstering account security, empowering users to proactively safeguard their accounts. By mandating the input of the previous password, the system enforces strict authentication protocols, thereby limiting password changes to authorized individuals. This robust measure helps mitigate the risk of unauthorized access, reinforcing user confidence in the integrity of their account security.

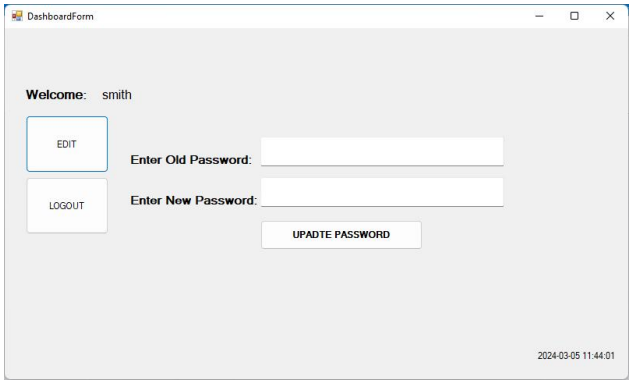

Fig. 8. Password Update.

The admin session commences with the administrator navigating to the login page to assert control over the system. Illustrated in Fig. 9, the admin login page presents a familiar interface, prompting the administrator to provide their designated username and password.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

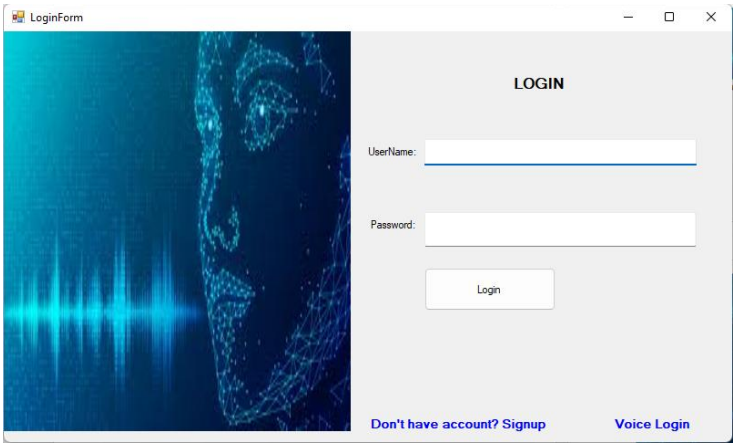

Fig. 8. Admin Login.

Upon successful authentication of the admin through the correct username and password, the admin dashboard is promptly presented, showcased in Fig. 9. This comprehensive dashboard furnishes the admin with a panoramic view of all users' logs captured within the system. Moreover, it hosts an array of four distinct buttons, each serving specific administrative actions.

The verification button empowers the admin to activate user accounts, ensuring seamless integration into the system. Conversely, the suspend button facilitates the temporary deactivation of user accounts when necessary. The delete account button offers a streamlined process for permanently removing accounts from the system if warranted. Finally, the logout button provides a convenient means for the admin to conclude their session securely.

Functioning as the nerve center of administrative operations, the admin dashboard not only provides insight into user activities but also furnishes tools for swift and decisive action. Equipped with an intuitive interface and robust functionalities, it enables the admin to effectively oversee system operations, monitor user interactions, and execute administrative tasks with precision and efficiency.

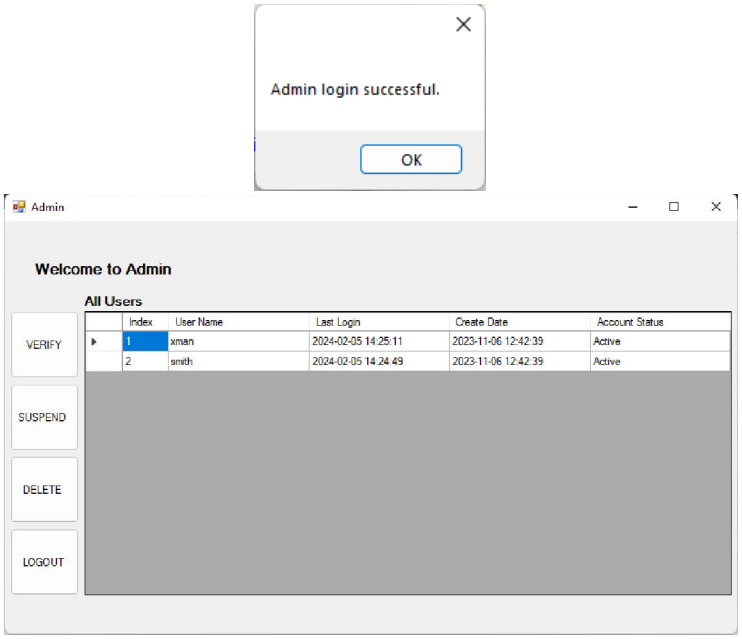

Fig. 9. Admin Login.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

TABLE I. 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

The results of the performance evaluation metrics provide valuable insights into the effectiveness of the proposed database security system utilizing dynamic time-warping voice recognition for authentication.

Accuracy: Across the scenarios, the accuracy values range from 0.6 to 0.8, indicating a moderate to high level of correctness in authentication predictions. The 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 that the system has a strong overall ability to accurately authenticate users based on their voice patterns.

Precision: Precision measures the accuracy of positive predictions made by the system, particularly relevant when minimizing false positives. The precision values range from 0.6 to 0.88 across scenarios, with Scenario 5 demonstrating the highest precision value of 0.88. This indicates that the system excels in accurately predicting positive authentication cases while minimizing false positives, which is crucial for maintaining security by avoiding unauthorized access.

Sensitivity (Recall): Sensitivity evaluates the system's ability to correctly identify 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.

Fig. 10. Admin Login.

Overall, the results suggest that the proposed 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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

VII. CONCLUSION

In conclusion, this research project presents a compelling solution to the persistent challenges in database security by introducing a robust database security system with dynamic time-warping voice recognition. Traditional username and password authentication methods have proven to be vulnerable to security risks, highlighting the need for innovative approaches. The integration of dynamic time-warping voice recognition offers a multi-factor authentication system that significantly enhances security, data integrity, and the user experience in accessing sensitive information. Through an in-depth exploration of existing research, the project has identified the limitations of traditional authentication methods, underscoring the critical need for improved security measures. Building upon prior research on One-Time Passwords (OTPs), the proposed system incorporates best practices to enhance security and reliability.

REFERENCES

[1]. Mubina and M. Trisha, "Enhancing Database Security with Voice Recognition," *International Journal of Information Security*, vol. 6, no. 3, pp. 231-245, 2016.

[2]. P. R. Sweety and M. K. Dhande, *Data Protection and Privacy in the Digital Age*. Wiley, 2020.

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

[4]. P. Vittori, "Ultimate password: Is voice the best biometric to beat hackers?," *Biometric Technology Today*, vol. 2019, no. 9, pp. 8-10, 2019.

[5]. A. Rihanat, S. I. Zaharaddeen, A. Jamilu, and N. S. Ibrahim, "Database Security Framework Design Using Tokenization," *Dutse Journal of Pure and Applied Sciences*, vol. 8, no. 1, pp. 16-26, 2022.

[6]. M. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Fusion of face and voice biometrics using Dempster-Shafer theory," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1268-1293, 2021.

[7]. Anter, M. Israa, and B. Alsaadi, "Multimodal biometric scheme combining voice and face recognition: A Review," *International Journal of Scientific & Technology Research*, vol. 1, no. 1, 2019.

[8]. L. Zhang, C. Tan, and F. Yu, "An improved rainbow table attack for long passwords," *Procedia Computer Science*, vol. 107, pp. 47-52, 2017.