RESEARCH ARTICLE OPEN ACCESS

DATABASE SECURITY SYSTEM USING DYNAMIC TIME-WARPING VOICE RECOGNITION AUTHENTICATION

Chukwudi J. Chukwuluba[1], Omede Gracious Chukwunweike.[2], Abel Edje[3], Anazia E. Kizito[4]

[1, 2, 3:]Department of Computer Science, Delta State University, Abraka
4:Department of Information Systems and Technology, Delta State University of Science and Technology, Ozoro

ABSTRACT

In the rapidly evolving digital landscape, ensuring the security of personal and corporate data stored in Database Management Systems (DBMS) remains a top priority. Current data protection methods, primarily reliant on passwords and UserID/PIN protection, have shown vulnerabilities to hacking and unauthorized access. This work addresses these shortcomings by introducing a Database Security System Using Dynamic Time-Warping Voice Recognition Authentication. These system possess the inherent capability to discern unique voice patterns, offering a sophisticated and secure authentication method. By analyzing the distinct vocal attributes of users, the system adds an extra layer of security, reinforcing data protection against potential threats. The methodology employed in this work is an object an Object-Oriented Analysis and Design Methodology (OOADM) with a Prototyping development approach. The front end, designed using ASP.NET C#, ensures an accessible and user-friendly interface, facilitating seamless interaction for administrators and the back end leverages the robust capabilities of SQL Management Studio 2014, ensuring efficient and secure data storage and retrieval. Findings from the system evolution demonstrate a significant improvement in data protection through the implementation of voice recognition technology.

Keywords: Database, Dynamic Time-Wrapping, Voice Recognition and Voice Pattern

1. Introduction

In the age of digitalization, databases play a vital role in the storage and management of extensive data for various purposes. Relational databases, which arrange data in tables, are commonly utilized to facilitate data storage and retrieval processes. As reliance on databases grows, ensuring robust security measures to protect the confidentiality and integrity of stored data has become increasingly important [1]. Modern information management heavily relies on databases, which offer efficient data storage and retrieval. The widely adopted relational database model structures data in tables, catering to diverse industries' needs. Moreover, distributed databases enable data replication and sharing across multiple network points [2], enhancing accessibility and availability [3]. Authorized users can swiftly access, input, or analyze data through databases, which consist of queries, views, and tables organized to support information storage and retrieval processes. A Database Management System (DBMS) is computer software designed to oversee all databases installed on a system's hard drive or network [4]. Despite the invaluable role of databases, safeguarding their security is paramount due to the critical and sensitive nature of the information they contain. Database security aims to prevent unauthorized access, loss, or misuse, thus preserving data integrity and confidentiality. Organizations encounter challenges in upholding database security amidst various threats like data breaches, unauthorized access, and sabotage. Strengthening database security is essential for organizational efficiency [5]. The primary goal of database security is to shield databases from accidental or deliberate loss, which threatens data integrity and reliability. Database security also regulates which users are permitted or denied access to execute actions on the database. Organizations establish policies and controls, including password and username usage, to manage user access. The resulting Database Management Security System stores user details and grants access upon proper authentication [6]. Various threats can compromise database systems, leading to a loss of availability when data or systems cannot be accessed due to hardware, application, or network sabotage. Such incidents can disrupt organizational activities and daily operations [7]. Traditional methods of database security primarily rely on username and password authentication, which are vulnerable to hacking, password cracking, and identity theft. As electronic commerce expands and concerns over security violations mount, organizations must enhance their database security measures to maintain trust and safeguard sensitive information [8]. The complexity of database security has grown with the widespread adoption of distributed client/server architecture and the escalating risks associated with internet and intranet access. Policies and procedures must be established to uphold the security and integrity of stored data. Database managers identify threats and implement controls, such as passwords and usernames, to regulate user access [9]. However, despite these efforts, database systems remain susceptible to security breaches. PIN codes can be hacked, and ID cards can be stolen or duplicated, posing significant risks to data confidentiality. To address these vulnerabilities, new security technologies like biometrics have emerged. Biometric technologies utilize unique physiological or behavioral characteristics, such as voice patterns, for identity verification. Voice recognition, in particular, offers a natural and secure means of authentication, as voice characteristics are highly distinctive and difficult to replicate [10].

2. Statement of the Problem

The traditional method of accessing databases, which relies on usernames and passwords, introduces vulnerabilities due to the susceptibility of passwords to compromise or theft. This poses significant threats to the security and integrity of stored sensitive data. This critical concern emphasizes the necessity for an improved login process, requiring a more secure and dependable authentication method.While previous research, exemplified by [11], he explored security threats related to databases, it has not provided a comprehensive model for safeguarding data security and integrity. Similarly, the work of [12], 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 shortcomings, this work advocates for the integration of a voice recognition system into the login process.

The goal is to address the identified challenges by proposing the development of a secure database login system. This innovative system combines traditional username and password authentication with the advanced technology of voice recognition. By incorporating voice recognition technology, the system aims to enhance security measures, improve user authentication, and establish a more resilient and dependable login process for accessing databases. This integration of authentication methods aims to offer a comprehensive and effective solution to the existing vulnerabilities in conventional login processes, ultimately bolstering the overall security of database systems.

3. Review of Related Literature

In the study carried out by [13], a fusion approach of multiple biometric systems is presented, enabling fusion at various levels, including sensor, feature extraction, matching score, and decision levels. It was proposed by [14] that a fusion-based multimodal biometric system, incorporating face and voice biometric features, which encompasses feature-level, match score-level, rank-level, and decision-level fusion. They utilize Log Gabor and LBP features for facial feature extraction and MFCC and LPC features for voice feature extraction. In the work of [15], they opined on the fusion of face and voice biometrics using the dempster-shafer theory for person verification, occurring at the score level and applied to face and voice biometrics to address the limitations of single-modal biometric systems.

A multimodal biometric scheme for human authentication, combining voice and face recognition [16]. 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. An efficient Android-based multimodal biometric authentication system is developed by [17], incorporating both face and voice with an improved Local Binary Pattern (LBP) algorithm to enhance the robustness of face feature extraction, coupled with a voice activity detection (VAD) method.

In the work of [18], they addressed database encryption by analyzing and comparing different architectures and proposed a novel architecture involving an encryption module within the database management software, achieving high data security levels with enhanced performance and application layer transparency. A designed a multi-tier web server system focusing on security, employing authorization, authentication, password hashing, and secure communication protocols to protect real-time data downloading [19].

An encrypted database system to enhance data security by protecting data integrity through encryption [20] while [21] introduced the "Full Encryption Model" for database security, based on encryption classes, providing a comprehensive set of security mechanisms. In the work of [22], he implemented AES encryption on FPGA to efficiently encrypt biometric image data, demonstrating high throughput, low latency AES for real-time encryption of biometric datawhile [23] focused on securing patient information in medical databases, introducing encryption and signature schemes to protect data integrity and confidentiality. A cryptography-based database system using Java and MySQL to prevent unauthorized access and data tampering. Was implemented by [24]. It was conducted [25] a comprehensive review of database security threats and their associated techniques, aiming to explore various database security issues, including data confidentiality, integrity, and availability requirements. In a more recent study, in the study carried out [26] they proposed a Database Security Framework Design Using Tokenization, introducing the concept of tokenization, which involves replacing or substituting sensitive data with a token.

4. Method Adopted

The system is designed and implemented using the C-Sharp Programming Language (C#) and Structural Query Language (SQL) Management Server. This setup operates on the .NET framework and is compatible with Microsoft Visual Studio 2022. Microsoft offers an API enabling developers to integrate speech recognition and synthesis engines into Windows applications. Speech-to-text conversion is achieved through the Speech Recognition engine, while speech synthesis allows access to a text-to-speech conversion engine. Acting as an intermediary between the application and the speech recognition/text-to-speech engines, the Speech API (SAPI) facilitates seamless integration.

The methodology employed for this research is the Object-Oriented Analysis and Design Methodology (OOADM) with Prototyping. Object-oriented analysis and design (OOAD) is a technical approach utilized for analyzing and designing applications, systems, or businesses by applying object-oriented programming principles. Visual modelling is extensively used throughout the software development process to enhance stakeholder communication and improve product quality.

During object-oriented analysis, this is typically accomplished through the creation of use cases and abstract definitions of crucial objects. Subsequently, in the design phase, the analysis model is refined, and necessary technology and implementation choices are made. Object-oriented design shifts the focus towards describing various objects, including their data, behavior, and interactions. The design model aims to provide all essential details for programmers to implement the design in code.

5. Methods of Data Collection

The research methodology relies on gathering information from diverse sources, including academic papers, internet websites, and articles, all related to securing databases through the utilization of a voice recognition system (VRS). Essentially, the research adopts a secondary research approach, compiling an overview of existing literature addressing the subject matter. This approach aims to provide users with comprehensive insights into safeguarding themselves from potential threats, drawing upon the knowledge and findings accumulated from various credible sources.

6. Analysis of the System

The system is a secure database system integrating a Voice Recognition System (VRS) to bolster user authentication. It comprises several key components, such as an acoustic front-end, acoustic model, lexicon, language model, and decoder. Collaboratively, these elements establish a resilient and dependable authentication process. Each component plays a pivotal role in the system's operation, utilizing the Dynamic Time Warping (DTW) algorithm to enhance functionality and security.

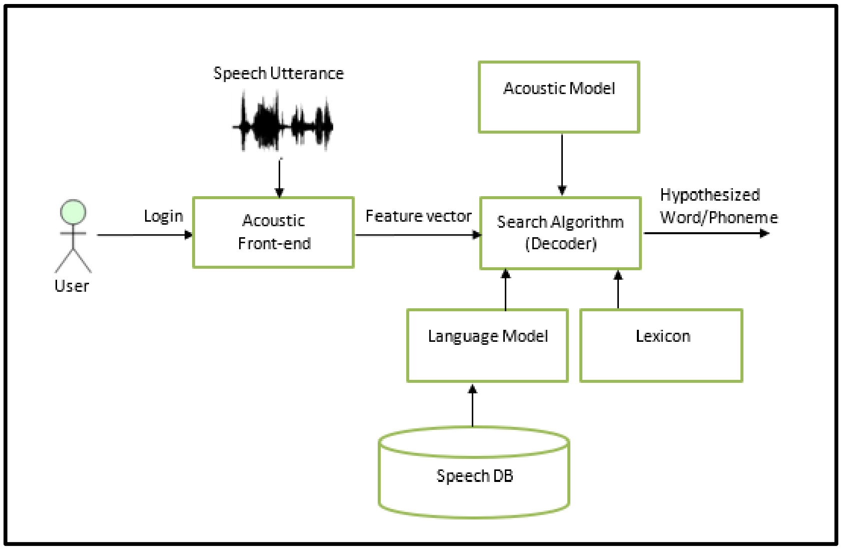


Fig: The Architecture of the System

i. Acoustic Front-End:

a. The acoustic front-end plays a crucial role in the system by converting the speech signal, captured via a microphone, into appropriate features. These features are essential for voice recognition. Here, the DTW algorithm can be employed during feature extraction.

b. DTW assists in comparing the input audio waveform (captured voice during login) with an enrolled voice template. It aligns the two sequences, accounting for variations in timing and speed, which is particularly useful in voice recognition.

ii. Acoustic Model:

a. The acoustic model is responsible for estimating the parameters of word or phone models based on the acoustic vectors extracted from training data. In this context, DTW may also be employed during the training phase to align reference voice patterns with known text or commands.

b. DTW-based alignment during training helps create accurate acoustic models that can be used to recognize words or phrases during the login process.

iii. Lexicon:

a. The lexicon component contains a database of phonemes, words, or phrases that the system can recognize. It provides a reference for mapping acoustic patterns to linguistic units.

b. DTW can assist in aligning acoustic patterns with entries in the lexicon, aiding in the recognition of spoken words or phrases.

iv. Language Model:

a. The language model defines the likelihood of word sequences in a given language. It helps the system determine the probability of a particular word sequence.

b. While DTW primarily deals with acoustic alignment, it complements the language model by ensuring that the recognized spoken words or phrases closely match the expected acoustic patterns.

v. Decoder:

a. The decoder is responsible for the final recognition step. It searches through all possible word sequences to find the sequence of words that is most likely to have generated the input speech signal.
b. DTW can be employed during this decoding process to match the captured voice to the enrolled voice templates and calculate the likelihood of a match.

7. Performance Evaluation of the System

The performance evaluation of the system is crucial to validate its effectiveness. This evaluation relies on three essential metrics: accuracy, precision, and sensitivity. These metrics provide valuable insights into the system's authentication capabilities, facilitating a comprehensive assessment of its performance.

Accuracy: Accuracy serves as a comprehensive measure, gauging the proximity of the system's predictions to actual authentication data. It provides an overall assessment of correctness and is calculated using the formula:

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

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.

Precision: Precision concentrates on the accuracy of positive authentication predictions, assessing how well the system predicts positive cases when it predicts them. Especially relevant when minimizing false positives, precision is calculated using the formula:

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

Sensitivity (Recall): Sensitivity, also known as recall, evaluates the system's ability to correctly identify positive authentication cases. Essential when minimizing false negatives, sensitivity is calculated using the formula:

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

Sensitivity quantifies the proportion of actual positives that were correctly predicted as positives.

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

These metrics provide a holistic evaluation of the system's authentication performance. The calculations utilize historical data not encountered during system training, ensuring the reliability and accuracy of the system in securing database access. Regular performance assessments based on these metrics contribute to refining and optimizing the system for heightened security and dependable user authentication.

8. System Specifications

The voice recognition component of the system adopts a client-server architecture. The server, hosted on a Windows Server environment, manages both the database and voice recognition services. Clients, including users operating on Windows, macOS, and Linux platforms, interact with the system through intuitive user interfaces. The backend of the system is developed using C# and the .NET framework, ensuring the incorporation of robust and secure components. Microsoft SQL Server acts as the primary Database Management System (DBMS), guaranteeing data integrity and reliability. Voice recognition, a critical aspect of the system, employs Dynamic Time Warping (DTW) for voice pattern matching. Integration with Microsoft's Speech Recognition and Synthesis APIs facilitates efficient voice data processing. Data security is prioritized, with the implementation of strong encryption for data at rest and in transit. Access control lists (ACLs) are utilized to manage and restrict data access based on user roles and privileges.

Scalability is carefully considered to accommodate a growing user base and expanding data requirements without compromising performance. Load balancing mechanisms distribute workloads effectively. The system's cross-platform web-based user interface caters to administrators and users, offering accessibility and compatibility across various operating systems. User interaction with the system begins with voice enrolment, where users provide voice samples securely processed and stored.

Authentication relies on a predefined threshold for voice pattern matching, ensuring users meet the necessary criteria for access. Detailed logging and auditing of user activities, including login attempts, data access, and configuration changes, enhance security and compliance.
Administrators possess the capability to manage user accounts, allowing them to add, modify, and delete accounts while defining user roles and access privileges. Routine data backups and recovery procedures safeguard data integrity and availability in case of data loss or system failures. The system supports regular maintenance tasks, including updates, patches, and performance optimization. Integration capabilities are a key feature, enabling the system to connect with other applications and services through APIs. Comprehensive technical documentation assists administrators and users in effectively utilizing the system. Furthermore, user support is available through helpdesk services, including email and phone support during business hours. The initial release of the system is labeled Version 1.0, with plans for future updates and enhancements to continually enhance functionality and security.

9. Database Development Tool

The database development tool chosen for the system is Microsoft SQL Server Management Studio (SSMS). SSMS is a robust and widely used database development and management tool designed specifically for Microsoft SQL Server, making it an ideal choice for the envisioned database security system. SSMS offers a unified and integrated environment that simplifies various tasks related to database design, implementation, and maintenance.

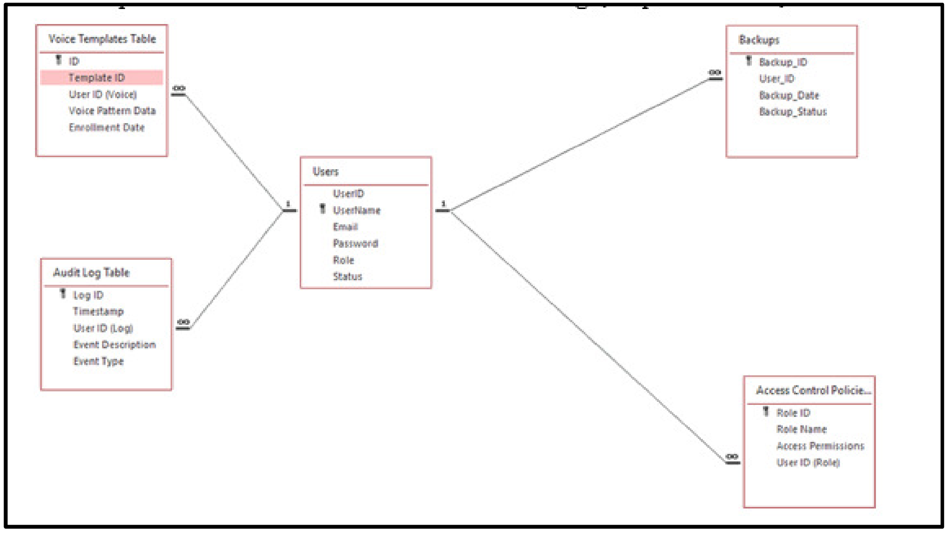


Fig 2: Entity Relationship Diagram

10: Algorithm

Dynamic Time Warping (DTW) is a commonly used algorithm for voice recognition. DTW is a dynamic programming technique that measures the similarity between two sequences while allowing for some degree of time warping or stretching to align them. The algorithm for voice recognition using DTW:

Step 1: Data Preprocessing:

a. Record and digitize the input voice signal.
b. Divide the voice signal into frames (typically 10-30 milliseconds).
c. Extract features from each frame (e.g., MFCC coefficients, energy, pitch).
d. Create a feature matrix where each row represents the features of a frame.

Step 2: Training:

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

b. Extract features from the training samples.
c. For each training sample, compute a distance matrix using DTW against all frames of the training sample.

Step 3: Voice Recognition:

a. Record and digitize the input voice signal to be recognized.
b. Divide the input voice signal into frames and extract features, as in step 1.
c. For each test frame, compute a distance matrix using DTW against all frames of the training samples.

Step 4: DTW Algorithm:

a. 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.
b. 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.
c. For each cell in the matrix (excluding the first row and column):
d. 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.
e. Update the cell with the minimum accumulated cost from the three neighboring cells above, left, and upper-left, plus the local cost.
f. 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.
g. Compute the cumulative distance as the sum of the minimum path costs.

Step 5: Recognition Decision:

a. Calculate a recognition score for the input voice signal based on the cumulative distances for each test frame.
b. 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 a recognition (known speaker).

Step 6: Output:

a. Return the recognized speaker's identity or a rejection result.

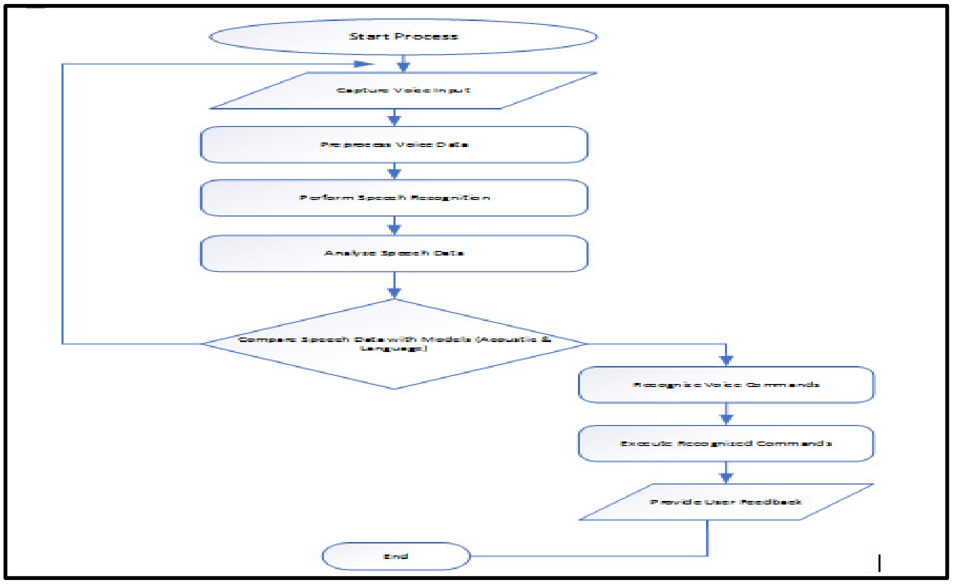


Fig 3: System Flowchart

11: System Implementation

The System Implementation phase marks the transformation of the conceptual design and specifications into a tangible and functional Examination Verification System. Several critical components and steps are involved in this phase.

The User Management Module is developed to facilitate user registration, login, profile management, and access control. The Data Processing Module takes center stage in processing acquired biometric data and comparing it with stored data. This step includes the implementation of biometric matching algorithms and the establishment of matching thresholds to verify user identity accurately.

The Voice and Verification Module is responsible for the final steps of identity verification based on the matching of biometric data. This module is a crucial security point and should be fortified against potential threats and breaches.To interact with users effectively, a User Interface (UI) is developed, encompassing login screens, registration forms, and user dashboards. The UI's design focuses on user-friendliness and accessibility to provide a seamless user experience.

11.1: Hardware Requirements

i. Microphone and Audio Input Devices: Users need access to microphones or audio input devices to capture voice patterns during authentication.

ii. User Devices: End-users and administrators should have access to devices, such as computers, smartphones, or tablets, with internet connectivity for accessing the system's user interfaces.

11.2: Software Requirements

i. Operating System: The system should be compatible with specific operating systems, such as Windows Server for server infrastructure and various operating systems for user devices.

ii. Database Management System: A robust database management system (DBMS) is required for creating and maintaining the database, and it should support SQL queries and database security features.

iii. Speech Recognition Engine: The system relies on a speech recognition engine, typically provided through software libraries or APIs. Compatibility with the chosen engine is essential.

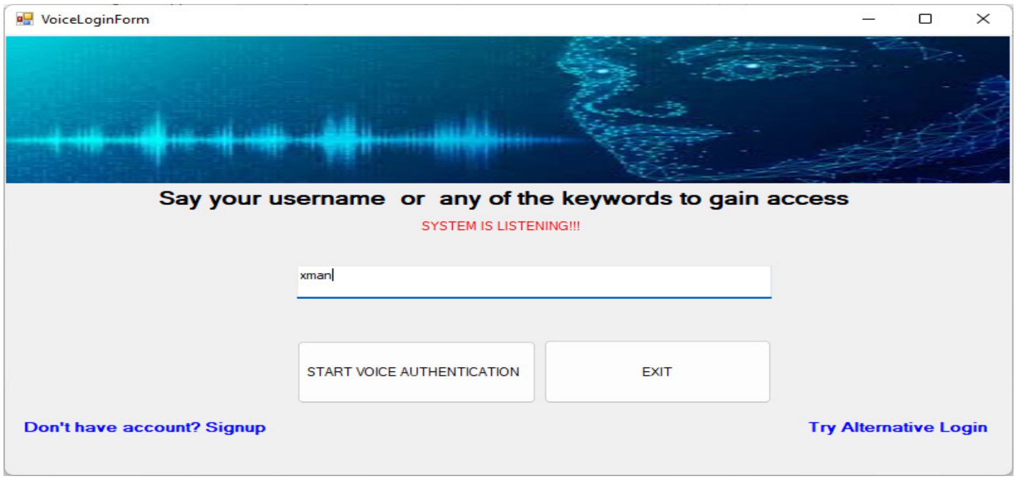
iv. Speech Synthesis Engine: For providing feedback and voice prompts, a speech synthesis engine is required, often provided as part of the speech recognition library.

v. Development Tools: Software development tools, including Microsoft Visual Studio or other compatible IDEs, are necessary for creating and maintaining the software components.

12: Choice of Programming Environment

The choice of a programming environment for the system is a critical decision that significantly influences the system's development and functionality. In this regard, Microsoft Visual Studio 2022 emerges as the chosen integrated development environment (IDE). Its seamless integration with the .NET framework, a core component of the system, streamlines development processes and ensures compatibility. The presence of speech recognition and synthesis tools within Visual Studio is particularly noteworthy for the voice recognition functionality of the system. These tools facilitate precise processing of voice patterns and their secure storage, contributing to the system's effectiveness and reliability.

13: System Design Interface Result



Say your username or any of the keywords to gain access

SYSTEM IS LISTENING!!!

xman

Fig 4: Voice Login Interface

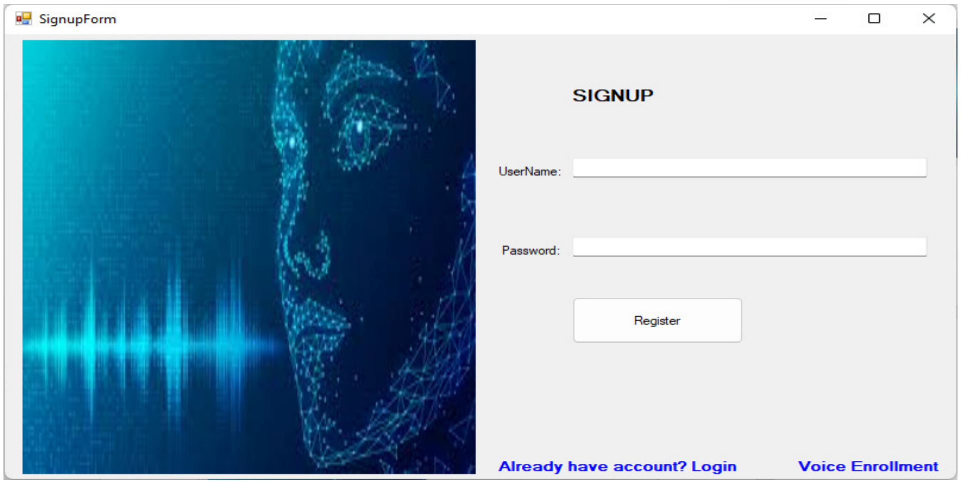


Fig 5: User Account Registration Interface

14: Discussion of Result

The results of the performance evaluation metrics provide valuable insights into the effectiveness of the system, Database Security System Using Dynamic Time-Warping Voice Recognition 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.

Overall, the results suggest that the system, Database Security System Using Dynamic Time-Warping Voice Recognition Authenticationexhibits 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.

15: Summary

This work aims to address the critical 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 susceptible to security risks. To counter these challenges, the project integrates voice recognition as an additional layer of authentication, promoting multi-factor authentication, data privacy, and seamless integration with existing login processes. It leverages the Object-Oriented Analysis and Design Methodology (OOADM) with prototyping and utilizes C-Sharp (C#) and SQL Management Server on the .NET framework, along with Microsoft's Speech Recognition engine for voice recognition. The research methodology draws from a wide range of secondary sources, including papers, internet websites, and articles, to provide an extensive overview of the subject matter. The system analysis reveals 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 enhance security. Additionally, the project introduces a mathematical model for dynamic time-warping (DTW) voice recognition to match captured voices with enrolled voice templates.

16: Conclusion

Conclusively, this study introduces an effective remedy for the enduring obstacles in database security. It proposes a sturdy database security framework incorporating dynamic time-warping voice recognition. Conventional methods of authentication, such as username and password, have demonstrated susceptibility to security threats, underscoring the necessity for inventive solutions. The incorporation of dynamic time-warping voice recognition presents a multi-faceted authentication mechanism that notably bolsters security measures, upholds data integrity, and enhances user interaction when accessing confidential data.

17: References

1. Mubina, A., and Trisha, M. (2016). Enhancing Database Security with Voice Recognition. International Journal of Information Security, 6(3), 231-245.
2. Okpako, A. E. and Anazia, E. K. (2022). Web Based Daily Operational E-Ticketing System for Road Transporters in Nigeria International Journal of Scientific Development and Research (IJSDR) www.ijsdr.org.
3. Sweety, P. R., and Dhande, M. K. (2020). Data Protection and Privacy in the Digital Age. Wiley.
4. Sakshi, K., Anderson, R., and Moore, T. (2017). Information Security: The Complete Reference. McGraw-Hill Education.
5. 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
6. Singh, S. R. (2019). A Novel Approach to Database Security. In Proceedings of the International Conference on Cybersecurity (pp. 45-56). IEEE.
7. Singh, M., Singh, R. and Ross, A. (2019) A Comprehensive Overview of Biometric Fusion. Information Fusion, 52, pp.187-205.

8. Velásquez, Q., Anderson, R., and Moore, T. (2018). Database Security and Auditing: Protecting Data Integrity and Accessibility. Cengage Learning.
9. Gupta, S., Rodriguez, M., and Lee, Y. (2019). Enhancing Mobile Voice Authentication Using Dynamic Time-Warping. International Conference on Cybersecurity and Privacy, 45-58.
10. 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.
11. Rafiq, M. (2014). Database Security Threats & Its Techniques. International Journal of Advanced Research In Computer Science & Software Engineering. 183-185
12. Rihanat B. A., Zaharaddeen S.I., Jamilu A. and Ibrahim N.S. (2022). Database Security Framework Design Using Tokenization, Dutse Journal of Pure and Applied Sciences. 8(1), 16-26.
13. Rose, D. Maltoni, D., Cappelli, R., Wayman, J. L., and Jain, A. K. (2018). Fusion of Multiple Biometric Systemsin Proc. Int. Conf. Pattern Recognition (ICPR), Quebec City, QC, Canada, pp. 744-747.
14. Poornima, N. Abdullahi, A.A., Lame, S.A. and Maikudi, F.A. (2017). Biometric Approach as a Means of Preventing Identity: Fusion-based multimodal biometric system (face and voice). African Scholars Journal of Science Innovation & Tech. Research (JSITR-9), 24(9), 149-164.
15. Chokhani, K. Y. (2017). Enhancing Information Security through Access Control-Based Solutions. Journal of Information Technology Management, 17(2), 123-136
16. Anter, B., Israa M. and Alsaadi, B. (2019). Multimodal biometric scheme combining voice and face recognition: A Review, International Journal of Scientific & Technology Research, VOL 1, ISSUE 1.
17. Zhang, L., Tan, C. and Yu, F. (2017). An Improved Rainbow Table Attack for Long Passwords. Procedia Computer Science, 107, pp.47-52.
18. Erez G., Mubina M., Trisha P., (2014). "Database encryption architectures" International Journal of Scientific & Engineering Research, Volume 7, Issue 12, 313 ISSN 2229-5518.
19. Harba L. (2015). Multi-Tier Web Server System with a Focus on Security, International Journal of Computer Science and Information Technologies, page 374.
20. Kuppuswamy, B., & 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.
21. Karim, A. et al. (2019). Full Encryption Model for Database Security Based on Encryption Classes. A Review, International Journal of Scientific & Technology Research, VOL 1, ISSUE 1
22. 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
23. Lastdrager, E. (2011). Securing Patient Information in Medical Databases with Encryption and Signature Schemes. In: Bulletin of the Transilvania University of Brasov. Engineering Sciences. Series I 2. p. 17
24. 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
25. Mezai Meng; Wong, D.S.; Furnell, S.; Jianying Zhou, (2021) "Fusion of face and voice biometrics using Dempster-Shafer theory," in Communications Surveys & Tutorials, IEEE, vol.17(3) pp.1268-1293.
26. Chen, Y. and Liginlal, D. (2017) Bayesian Networks for Knowledge-Based Authentication. IEEE Transactions on Knowledge and Data Engineering, 19 (5), pp.695-710.