FILE ENCRYPTION USING AUDIO KEYS FROM SPEAKER RECOGNITION MODE

1. 21BCE5081 - Diya Das
2. 21BCE5115 - Armaan Saini

Project guide: Dr. Trilok Nath Pandey

PROBLEM STATEMENT

- Traditional file encryption methods, while effective, often rely on static keys such as passwords or cryptographic keys that can be vulnerable to theft, misuse, or brute-force attacks. These methods do not provide sufficient protection against unauthorized access, especially in environments where security breaches can have severe consequences.
- The challenge lies in creating a more secure and user-friendly encryption mechanism that leverages biometric data, specifically voice, to generate encryption keys. The existing speaker recognition technologies have not been widely integrated with encryption processes, leaving a gap in the application of voice biometrics for data security.
- This project addresses the need for a novel encryption approach by utilizing audio keys generated through a Speaker Recognition Model. By linking the encryption and decryption processes to the unique voice patterns of an authorized user, the project aims to mitigate the risks associated with traditional encryption methods and enhance the overall security of sensitive data.

RESEARCH OBJECTIVES

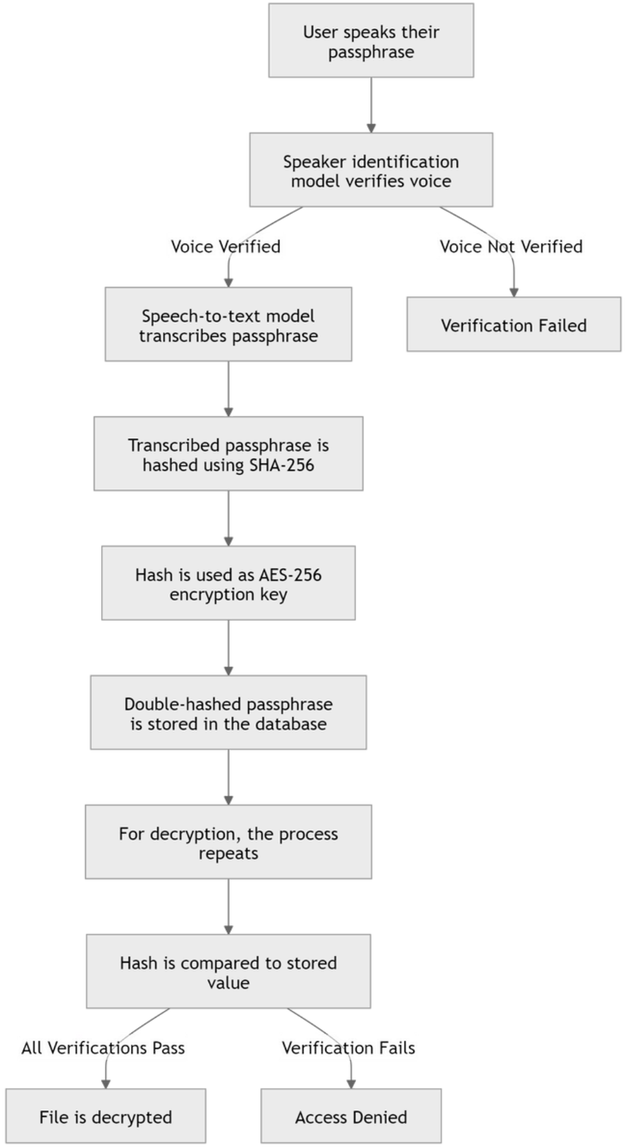
The primary objectives of this research are:

1. Develop a Secure File Encryption System
2. To design and implement a robust system that integrates speaker identification, speech-to-text conversion, and advanced cryptographic techniques (SHA-256 and AES-256) to securely encrypt and decrypt files.
3. Verify User Identity through Voice Biometrics
4. To leverage speaker identification models that can accurately recognize individual users based on their voice, ensuring only authorized individuals can access sensitive data.
5. Integrate Passphrase-Based Authentication
6. To employ a unique passphrase system that users speak, which is securely hashed and used as the key for file encryption. This passphrase also provides an additional layer of security by ensuring that users' spoken phrases must match precisely.
7. Enhance Security Using Cryptographic Hashing
8. To explore the effectiveness of cryptographic hashing (SHA-256) in generating strong, irreversible encryption keys and securely storing user credentials in a database.
9. Develop a Multi-Layer Authentication Mechanism
10. To create a multi-step process for authenticating both the user's voice and their passphrase, ensuring that both identity and passphrase match are required for file access.

PROPOSED MODEL INTRODUCTION

- User Authentication: Verifies user identity through voice recognition and a specific passphrase.
- Integration of Techniques: Combines speaker identification, speech-to-text conversion, and cryptography for secure access.
- Secure File Decryption: Only the correct user with the right passphrase can decrypt sensitive files.
- Enhanced Security & Accessibility: Improves security by preventing unauthorized access while maintaining ease of use.

PROPOSED SYSTEM DIAGRAM



1. SPEAKER IDENTIFICATION MODEL

- User Identity Verification: A pre-trained speaker identification model checks the user's voice against stored samples.
- Matching Process: The input voice is compared to stored data, and if the match score exceeds 0.7, the user is authenticated as legitimate.

2. SPEECH-TO-TEXT CONVERSION MODEL

- Speech-to-Text Conversion: After speaker verification, the spoken passphrase is converted into text using a speech-to-text model, ensuring precise transcription for cryptographic operations.
- Noise Reduction and Accuracy: The system processes the speech to remove background noise and enhance clarity. Accurate transcription is critical—any mismatch in the passphrase would lead to decryption failure, making precision essential.

3. PASSCODE HASHING FOR ENCRYPTION KEY

- Passphrase Hashing: After conversion to text, the passphrase is hashed using the SHA-256 algorithm, generating a secure 256-bit output.
- Encryption Key for AES-256: The SHA-256 hash becomes the encryption key for AES-256, a highly secure standard ensuring data confidentiality and making the key difficult to reverse-engineer.

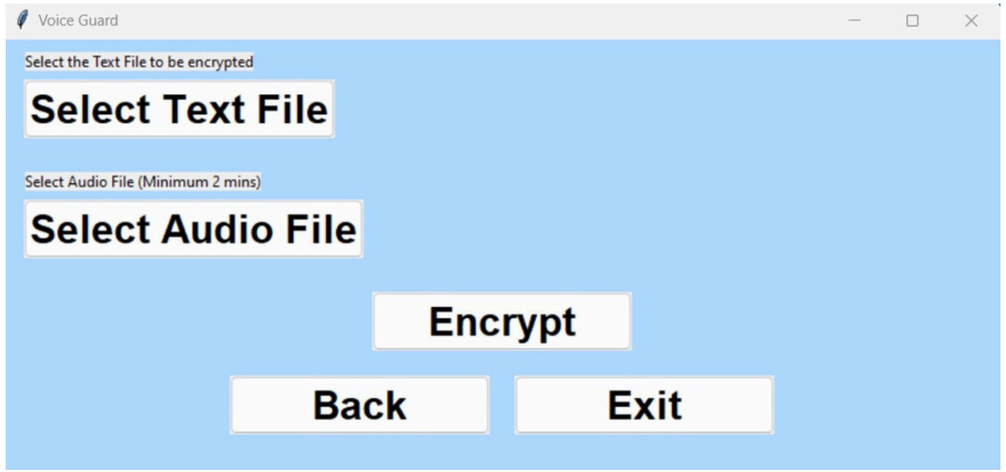
4. STORING HASHED PASSCODE IN DATABASE

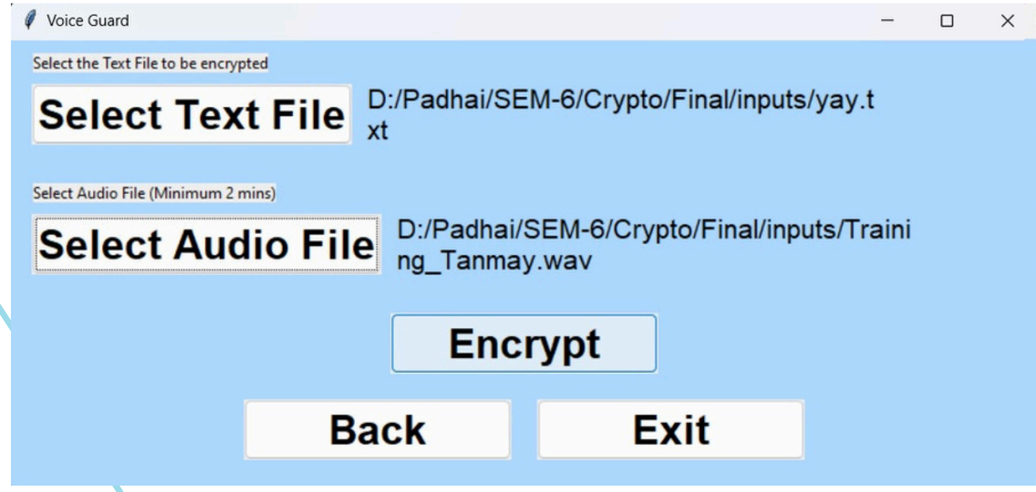
- Double Hashing for Security: The initial SHA-256 hash is hashed again and stored in a secure database, enhancing security even if the database is compromised.
- Protection Against Unauthorized Access: Storing the hashed passcode instead of plain-text prevents unauthorized access to sensitive data, ensuring additional layers of security.

5. DECRYPTION WORKFLOW

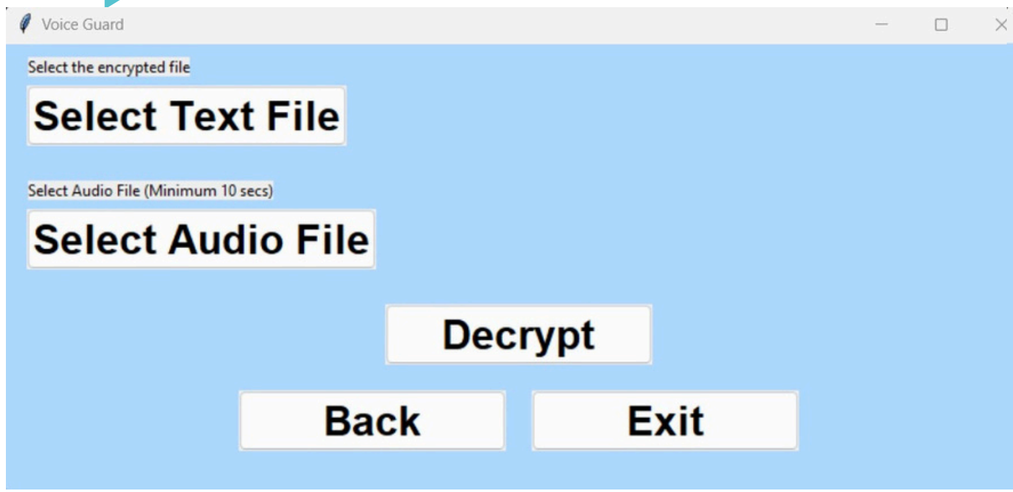
1. File Decryption with AES-256: If both speaker identification and passphrase verification succeed, the AES-256 key is used to decrypt the file.
2. Multi-Step Authentication: Decryption proceeds only if the passphrase matches the double-hashed value stored in the database, ensuring both the voice and passphrase are correct. If either step fails, the file remains encrypted.

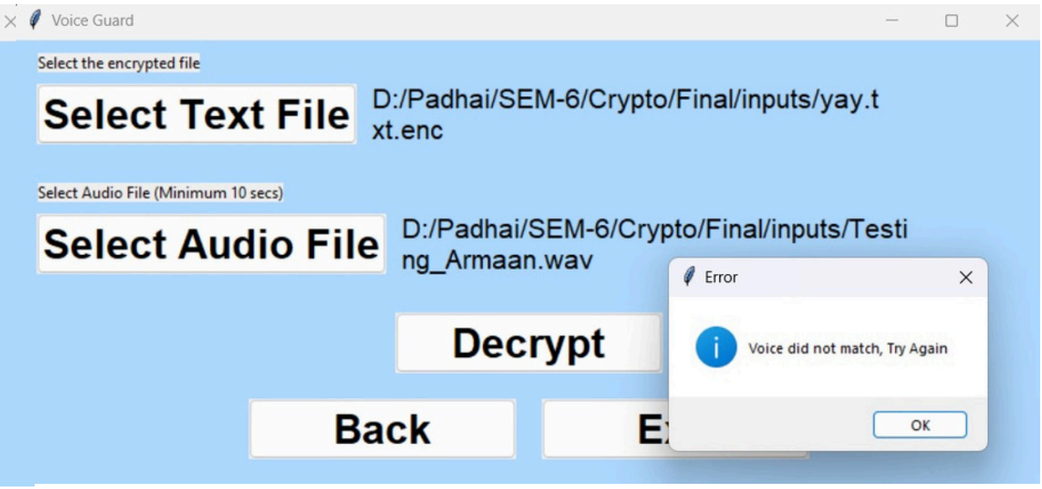
IMPLEMENTATION

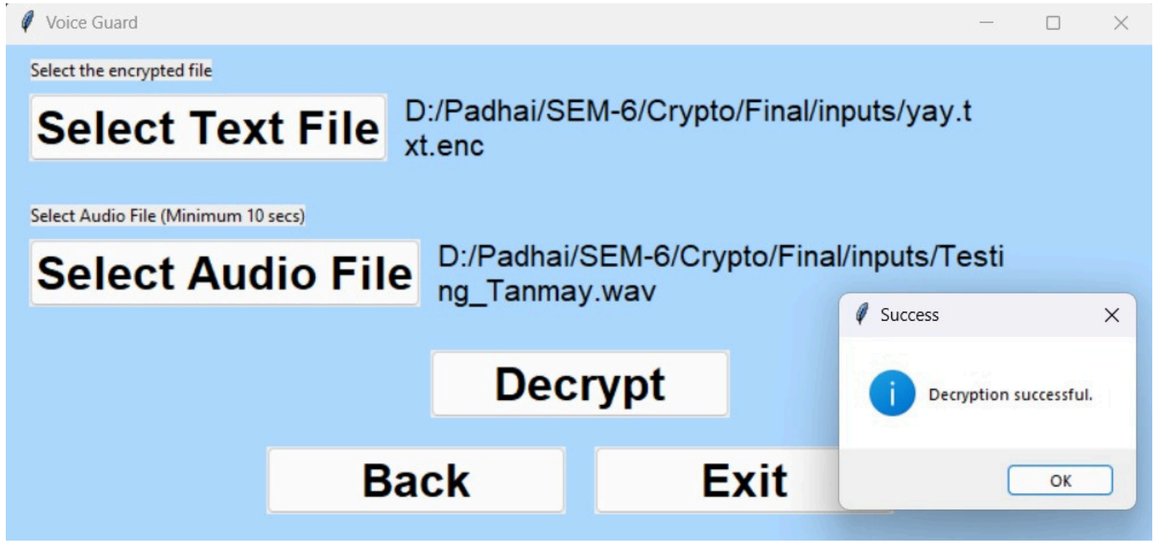




IMPLEMENTATION







WHAT IS TO BE DONE NEXT

I. Implement Speech-to-Text Model:

- Develop or integrate a reliable speech-to-text model to convert the user's spoken passphrase into text, ensuring accuracy for further processing.

II. Add Hashing Functionality:

- Implement the SHA-256 hashing algorithm to securely hash the converted text (passphrase).
- Implement double-hashing to ensure secure storage of passphrases.

III. Integrate Database for Passcode Storage:

- Design and integrate a secure database to store the double-hashed passcodes, ensuring confidentiality and protecting against unauthorized access.

IV. Finalize Decryption Logic:

- Complete the logic for decrypting files based on voice verification and passphrase matching using the hashed keys stored in the database.

V. Testing and Refinement:

- Perform comprehensive testing of the entire system, including speaker identification, encryption, decryption, and security of the hashing process.

REFERENCES

[1] Monrose, F., Reiter, M. K., Li, Q., & Wetzel, S. (2001). Cryptographic key generation from voice. In IEEE Symposium on Security and Privacy (pp. 206-215). IEEE.

[2] Agarwal, A., Singh, P. R., & Katiyar, S. (2019). Secured audio encryption using AES algorithm. International Journal of Computer Applications, 178(22), 31-37.

[3] Monther, A. A., & Azman, A. (2014). Voice-based public key cryptography system for mobile devices. International Journal of Computer Applications, 96(15), 23-28.

[4] Raghavendhar Reddy, B., & Mahender, E. (2013). Speech to text conversion using Android platform. International Journal of Engineering Research and Applications, 3(1), 202-213.

[5] Jain, N., & Rastogi, S. (2019). Speech Recognition Systems - A Comprehensive Study of Concepts and Mechanism. Acta Informatica Malaysia, 3(1), 1-3.

[6] Bai, Z., & Zhang, X.-L. (2021). Speaker recognition based on deep learning: An overview. Neural Networks, 140, 65–99.

[7] Malik, V., Saini, A., & Sangwan, S. (2017). The Design of Secure File Transfer with Speech Recognition. International Journal of Advanced Research in Computer Science, 8(5), 123-126.

THANK YOU