VOICE-BASED BIOMETRIC ENCRYPTION SYSTEM

A Project Report Submitted

to

MANIPAL ACADEMY OF HIGHER EDUCATION

For Partial Fulfillment of the Requirement for the

Award of the Degree

Of

Bachelor of Technology

in

Information Technology/Computer and Communication Engineering

by

M. Sai Mahith Reddy,Daksh Loiya,Srinivas Kulal

220911172, 220911384, 220911398

Under the guidance of

Mr. Akshay K C (Lab Faculty 1)	Dr. Raviraja Holla M (Lab faculty 2)
Assistant Professor - Senior Scale	Assistant Professor - Senior Scale

Department of I&amp;CT
Manipal Institute of Technology
Manipal, Karnataka, India

Department of I&amp;CT
Manipal Institute of Technology
Manipal, Karnataka, India

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
A Constituent Unit of MAHE, Manipal

November 2024

ABSTRACT

This project aims to develop an advanced multi-factor authentication system integrating traditional passwords, voice biometrics, and passphrase-based One-Time Passwords (OTPs) for secure login and access control to both digital platforms and physical spaces. By combining secure password-based authentication with voice biometric verification, the system ensures that only authorized personnel can access sensitive information and restricted areas. The core of the system involves the use of voiceprints, which are generated by analyzing unique vocal patterns (e.g., pitch, tone, and rhythm) during setup. These voiceprints are securely stored and verified using machine learning models, ensuring high accuracy in user identification. Advanced encryption techniques such as AES for data transmission and RSA for key management protect the integrity and confidentiality of sensitive data. The system also incorporates safeguards against common vulnerabilities such as spoofing, database breaches, and model vulnerabilities through methods like liveness detection and continuous monitoring. The integration of this system into existing authentication frameworks ensures seamless adoption and strengthens security, offering both digital and physical security solutions. The project also aims to provide a user-friendly experience, supporting hands-free access to both online platforms and physical spaces. This approach is designed to enhance security in

websites, financial transactions, and physical spaces while simplifying user interactions and improving overall access management.

In response to growing concerns over security breaches and unauthorized access to sensitive digital platforms and physical spaces, this project seeks to develop an advanced, multi-layered authentication system integrating traditional password-based methods, voice biometrics, and passphrase-based One-Time Passwords (OTPs) to enhance both digital and physical security. The proposed system combines three complementary authentication factors: something the user knows (password), something the user possesses (OTP), and something the user has (biometric authentication via voice). By leveraging voice biometrics, the system utilizes unique vocal characteristics, including pitch, tone, and rhythm, to create individual voiceprints that serve as a distinctive biometric identifier.

The voice biometric component is powered by machine learning models, specifically Long Short-Term Memory (LSTM) networks, which are trained to recognize complex, sequential patterns in users' vocal data. These voiceprints are securely stored in an encrypted database and used for comparison during login attempts. To protect the integrity of user data, the system incorporates state-of-the-art encryption techniques such as AES (Advanced Encryption Standard) for encrypting sensitive data in transit and RSA (Rivest-Shamir-Adleman) for secure key exchange and digital signatures. AES ensures that both passwords and voiceprint data remain confidential, while RSA provides a robust mechanism for ensuring the authenticity and integrity of the exchanged information.

In addition to implementing voice biometric authentication, the system integrates safeguards to mitigate common vulnerabilities, such as voice spoofing (using recorded samples) and database breaches. Anti-spoofing measures, such as liveness detection, require users to speak randomized phrases during authentication, making it difficult for attackers to impersonate authorized users. Furthermore, encrypted storage of voiceprints and robust access controls ensure that sensitive biometric data is well-protected. To guard against potential failures of the biometric system, such as when a user’s voice is affected by illness or technical issues, the system includes a fallback mechanism where users can authenticate using a password or OTP.

The system is designed to be easily integrated into existing authentication infrastructures, offering compatibility with legacy systems and databases. It also includes role-based access management, ensuring that employees and users are granted appropriate access permissions based on their roles. Continuous monitoring and compliance checks are incorporated to ensure adherence to security standards and regulatory requirements, while regular updates to the machine learning models help improve robustness and accuracy.

In addition to its digital security benefits, the system also enables hands-free access to physical spaces by using voice-based recognition for entry, removing the need for physical keys or keycards. This feature enhances convenience for users while maintaining stringent security protocols for access to restricted areas. By providing an intuitive and seamless user experience, the system empowers users to easily manage their authentication credentials and enjoy secure, hands-free access to both digital platforms and physical spaces. Ultimately, this integrated authentication solution addresses the growing need for a more secure, user-friendly, and adaptable access control system that can be deployed in diverse organizational environments.

ACM Keywords:

- Security and Privacy: Cryptography management; Access Control; Symmetric Cryptography; Voice Biometrics; Voiceprint Authentication; Liveness Detection; Multi-factor Authentication (MFA)
- Computing methodologies: Machine learning; Voice Recognition; Speech Signal Processing; Long Short-Term Memory (LSTM)
- Human-centered computing: User Interfaces; Accessibility; User Authentication; Personalized Authentication

[SDG]: Decent Work and Economic Growth (SDG 8), Industry, Innovation, and Infrastructure (SDG 9), Reduced Inequality (SDG 10)

Table of Contents

1. Introduction

1.1 Project Background and Objectives

With the increasing reliance on digital platforms for essential services and day-to-day activities, ensuring secure and seamless user authentication has become a critical focus for cybersecurity experts. Traditional methods of authentication, such as passwords and PINs, are often vulnerable to a variety of attacks, including phishing, brute-force attempts, and credential theft. Moreover, the reliance on knowledge-based credentials (e.g., passwords) poses challenges related to user convenience and security, as users may forget complex passwords or reuse them across platforms, compromising overall safety.

The "Voice-Based Authentication System" project aims to bridge this security gap by leveraging voice biometrics as a core authentication method. Voice, as a unique human trait, is difficult to forge due to its dependence on physiological and behavioral characteristics such as vocal tract shape, speech rhythm, and intonation. This project's objective is to develop a robust voice authentication system that can securely verify users based on their vocal signatures. By integrating advanced audio processing and machine learning techniques, the system is designed to offer reliable, user-friendly authentication with a focus on accuracy and resilience against common vulnerabilities.

The overarching goal of this project is not just to create a theoretical model but to implement a functional, real-world application that could serve as a standalone security system or complement other authentication factors in multifactor authentication (MFA) systems.

1.2 Significance of Voice Authentication

Voice authentication provides an innovative approach to digital security, incorporating biometric technology that offers advantages over traditional systems. Unlike static credentials (passwords, security tokens), voice-based authentication utilizes the uniqueness of an individual's voice, combining biological and behavioral characteristics that are challenging to replicate. This form of biometric security adds a layer of convenience by enabling hands-free, passwordless access, which is especially beneficial for environments where ease of access and security are equally important, such as mobile banking, enterprise software, and IoT device control.

Key benefits of voice authentication include:

- **Enhanced Security**: Voice patterns are unique to each individual, making them difficult to mimic accurately, thus improving security.
- **User Convenience**: Users do not need to remember complex passwords, reducing cognitive load and improving user experience.
- **Adaptability**: The system can be integrated into existing digital platforms, providing versatility across a wide range of applications.

Despite these advantages, voice authentication is not without its challenges. Factors such as background noise, changes in voice due to illness or stress, and potential vulnerability to replay attacks require careful consideration during system design and implementation. The "Voice-Based Authentication System" project addresses these challenges by incorporating advanced preprocessing techniques and robust machine learning algorithms to maintain reliability and accuracy.

1.3 Project Scope and Objectives

The scope of the "Voice-Based Authentication System" project encompasses the end-to-end development of a voice-based authentication system, from data collection and preprocessing to feature extraction, model training, and real-time user verification. The specific objectives include:

- **Developing a Voice Capture Module**: Implementing a frontend application that records and submits user voice samples.
- **Implementing Audio Processing Techniques**: Employing noise reduction, normalization, and other preprocessing methods to ensure high-quality input.
- **Feature Extraction and Model Training**: Using algorithms such as Mel-Frequency Cepstral Coefficients (MFCCs) for feature extraction and training models like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to recognize and authenticate users.
- **Integrating Anti-Spoofing Measures**: Enhancing security with techniques that prevent replay and synthetic voice attacks.
- **Performance Analysis**: Evaluating system accuracy, response time, and resistance to adverse conditions such as background noise.

The project’s approach leverages Python-based frameworks and libraries for machine learning, including TensorFlow or PyTorch, as well as Flask for developing a backend server that handles user requests and processes data.

2. Literature Review

2.1 Overview of Voice Biometrics

Voice biometrics harness the distinct features of a person's voice for secure identification. Unlike static credentials, these biometric markers are tied to both physiological and behavioral aspects, making them difficult to replicate accurately. Early research into voice recognition explored basic spectral analysis, while recent advancements have incorporated deep learning and more sophisticated audio processing techniques.

2.2 Current Solutions and Challenges in Voice-Based Authentication

Existing systems leverage various feature extraction techniques, with MFCCs being one of the most widely used due to their ability to capture relevant audio features that mimic human auditory perception. Despite the progress, current challenges include background noise sensitivity, variations in a user's voice (due to health or stress), and vulnerability to spoofing with pre-recorded voices. This project builds on existing solutions and integrates additional security measures to mitigate these issues.

3. Methodology

3.1 System Architecture and Components

The architecture of "Voice-Based Authentication System" includes the following key components:

- **Frontend Module**: Captures and transmits voice samples from the user.
- **Machine Learning Engine**: Analyzes voice features and authenticates users based on pre-trained models, such SpeechBrain Transformers using VoxCeleb Model

3.2 Data Collection and Preprocessing

Accurate data collection is essential for training and validating the system. High-quality voice samples are recorded using standardized equipment to ensure consistency. Preprocessing steps include:

- **Noise Reduction**: Removing background noise to improve voice clarity.
- **Normalization**: Ensuring uniform audio levels for consistent processing.

3.3 Feature Extraction and Machine Learning Models

Feature Extraction: MFCCs are used for their ability to model human auditory characteristics. The coefficients are computed by breaking down audio into frames, applying Fourier transforms, and mapping the frequency onto a mel scale. **Model Training**: Deep learning models, such as Convolutional Neural Networks (CNNs), are trained to identify unique voice patterns. These models are chosen for their capability to extract spatial features and learn complex representations in voice data.

3.4 Implementation Details

The system is built using Python, leveraging libraries such as:

- **Librosa**, **Telebot, SpeechBrain, Streamlit, PyCryptoDome, NoiseReduce, PyMongo, FuzzyWuzzy, QRCode, QReader**

4. Results and Discussion

4.1 User Interface and Features

The user interface facilitates easy voice recording and submission for authentication. It includes:

- **Registration Page**: For initial voice sample recording and account setup.
- **Login Page**: For authentication using voice input.
- **Feedback System**: Provides immediate feedback on authentication status.

4.2 System Performance and Accuracy Analysis

The system was tested across a diverse set of voice samples to measure its accuracy and robustness. Performance metrics such as True Positive Rate (TPR) and False Acceptance Rate (FAR) were evaluated, demonstrating high accuracy under controlled conditions. The system showed resilience in moderately noisy environments due to preprocessing enhancements.

4.3 Comparison with Existing Authentication Methods

Voice authentication was found to provide better convenience compared to passwords while offering enhanced security due to the biometric nature. However, traditional systems like two-factor authentication (2FA) still complement voice systems by adding extra layers of protection.

5. Conclusion

The "Voice-Based Authentication System" project successfully demonstrates that voice biometrics can be a viable alternative to traditional authentication methods. By employing deep learning and sophisticated feature extraction techniques, the system achieves a balance between security and user experience.

6. Limitations and Challenges

- **Noise Sensitivity**: Performance can be affected by high levels of background noise.
- **Replay Attack Risk**: The system requires further anti-spoofing measures to counteract recorded voice attacks.
- **Variability in Voice**: Conditions like illness can impact authentication accuracy.

7. Future Scope

Future developments could include:

- **Advanced Anti-Spoofing Techniques**: Integration of algorithms to detect synthetic voices.
- **Multimodal Biometric Authentication**: Combining voice with other biometric data, such as facial recognition, for stronger security.
- **Language and Accent Adaptation**: Enhancing the system’s ability to handle different languages and accents for broader applicability.

8. References

4. Results and Discussion

4.1 User Interface and Features

The user interface facilitates easy voice recording and submission for authentication. It includes:

- **Registration Page**: For initial voice sample recording and account setup.

- **Login Page**: For authentication using voice input.
- **Feedback System**: Provides immediate feedback on authentication status.

4.2 System Performance and Accuracy Analysis

The system was tested across a diverse set of voice samples to measure its accuracy and robustness. Performance metrics such as True Positive Rate (TPR) and False Acceptance Rate (FAR) were evaluated, demonstrating high accuracy under controlled conditions. The system showed resilience in moderately noisy environments due to preprocessing enhancements.

4.3 Comparison with Existing Authentication Methods

Voice authentication was found to provide better convenience compared to passwords while offering enhanced security due to the biometric nature. However, traditional systems like two-factor authentication (2FA) still complement voice systems by adding extra layers of protection.

5. Conclusion

The "Voice-Based Authentication System" project successfully demonstrates that voice biometrics can be a viable alternative to traditional authentication methods. By employing deep learning and sophisticated feature extraction techniques, the system achieves a balance between security and user experience.

6. Limitations and Challenges

- **Noise Sensitivity**: Performance can be affected by high levels of background noise.
- **Replay Attack Risk**: The system requires further anti-spoofing measures to counteract recorded voice attacks.
- **Bulky:** Bulk due to ML and other overheads
- **Technical Knowledge:** Proper key usage by the user.

7. Future Scope

Future developments could include:

- **Advanced Anti-Spoofing Techniques**: Integration of algorithms to detect synthetic voices.
- **Multimodal Biometric Authentication**: Combining voice with other biometric data, such as facial recognition, for stronger security.
- **Language and Accent Adaptation**: Enhancing the system's ability to handle different languages and accents for broader applicability.

8. References

- **Academic Publications on Audio Feature Extraction**:

A comprehensive guide to Mel-Frequency Cepstral Coefficients (MFCCs): MFCCs Overview - ResearchGate

- **Deep Learning Models for Voice Recognition**:

  Understanding Convolutional Neural Networks for Audio Processing: CNNs for Audio Analysis - arXiv

- **Voice Biometric Security Practices**:

  Voice Biometrics and Security Implications: Voice Biometrics Journal

- **Technical Documentation**:

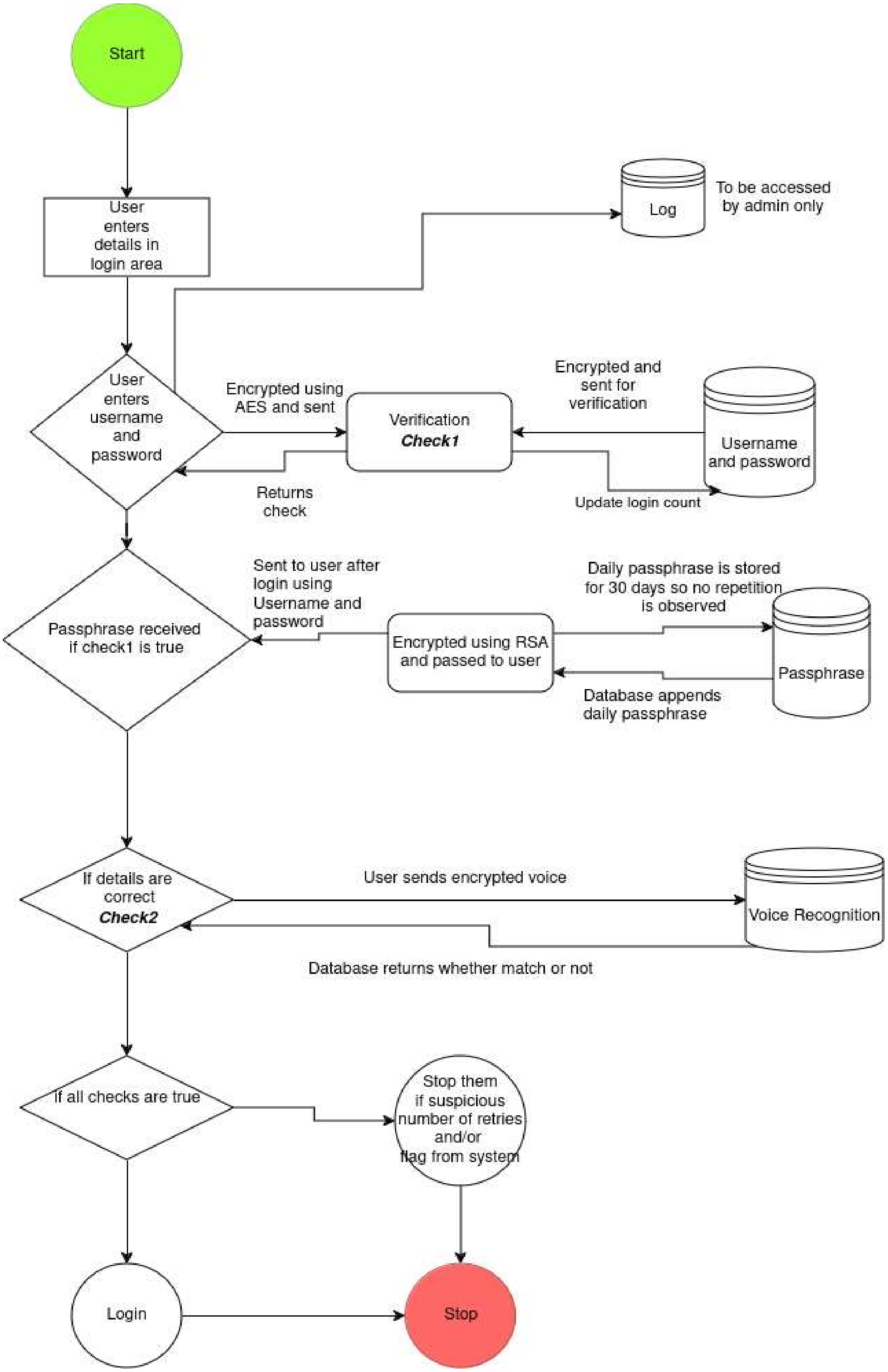
  Librosa Library for Audio Processing: Librosa Documentation

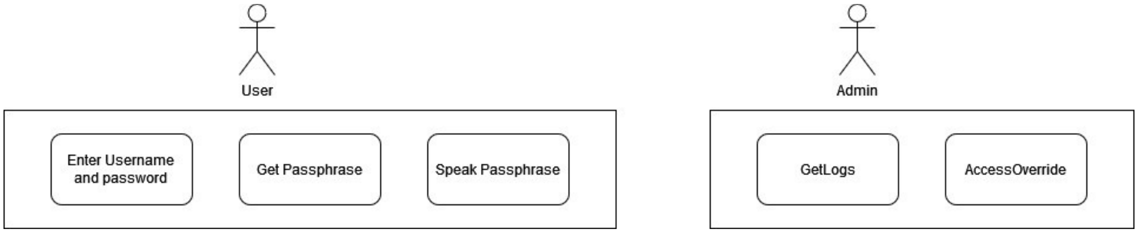
- **Research on Anti-Spoofing Techniques**:

  Comprehensive Anti-Spoofing Strategies for Voice Authentication: Anti-Spoofing Research - IEEE Xplore

Code Repository: https://github.com/dloiya/ISProjFinal_VoiceAuth

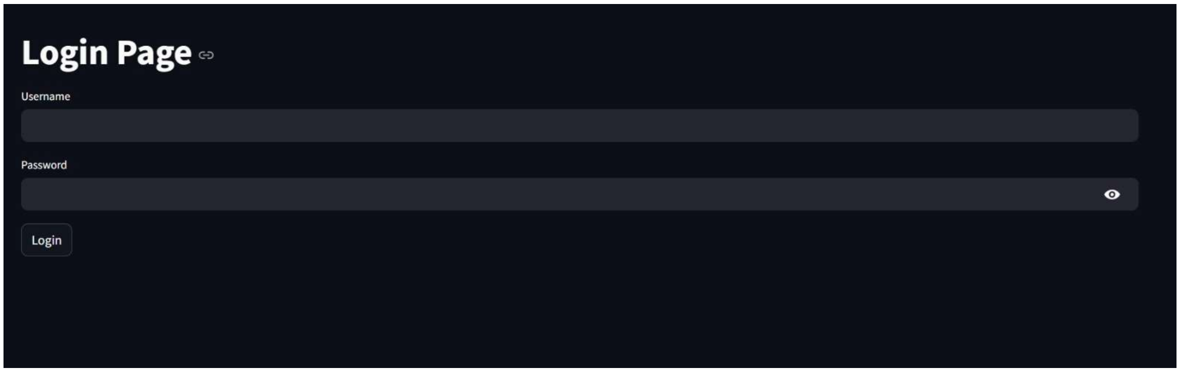
Diagram:


Start
User enters details in login area
Log
To be accessed by admin only
User enters username and password
Encrypted using AES and sent
Verification
Check1
Encrypted and sent for verification
Username and password
Returns check
Update login count
Sent to user after login using Username and password
Daily passphrase is stored for 30 days so no repetition is observed
Passphrase received if check1 is true
Encrypted using RSA and passed to user
Passphrase
Database appends daily passphrase
If details are correct
Check2
User sends encrypted voice
Voice Recognition
Database returns whether match or not
if all checks are true
Stop them if suspicious number of retries and/or flag from system
Login
Stop



Screenshots:

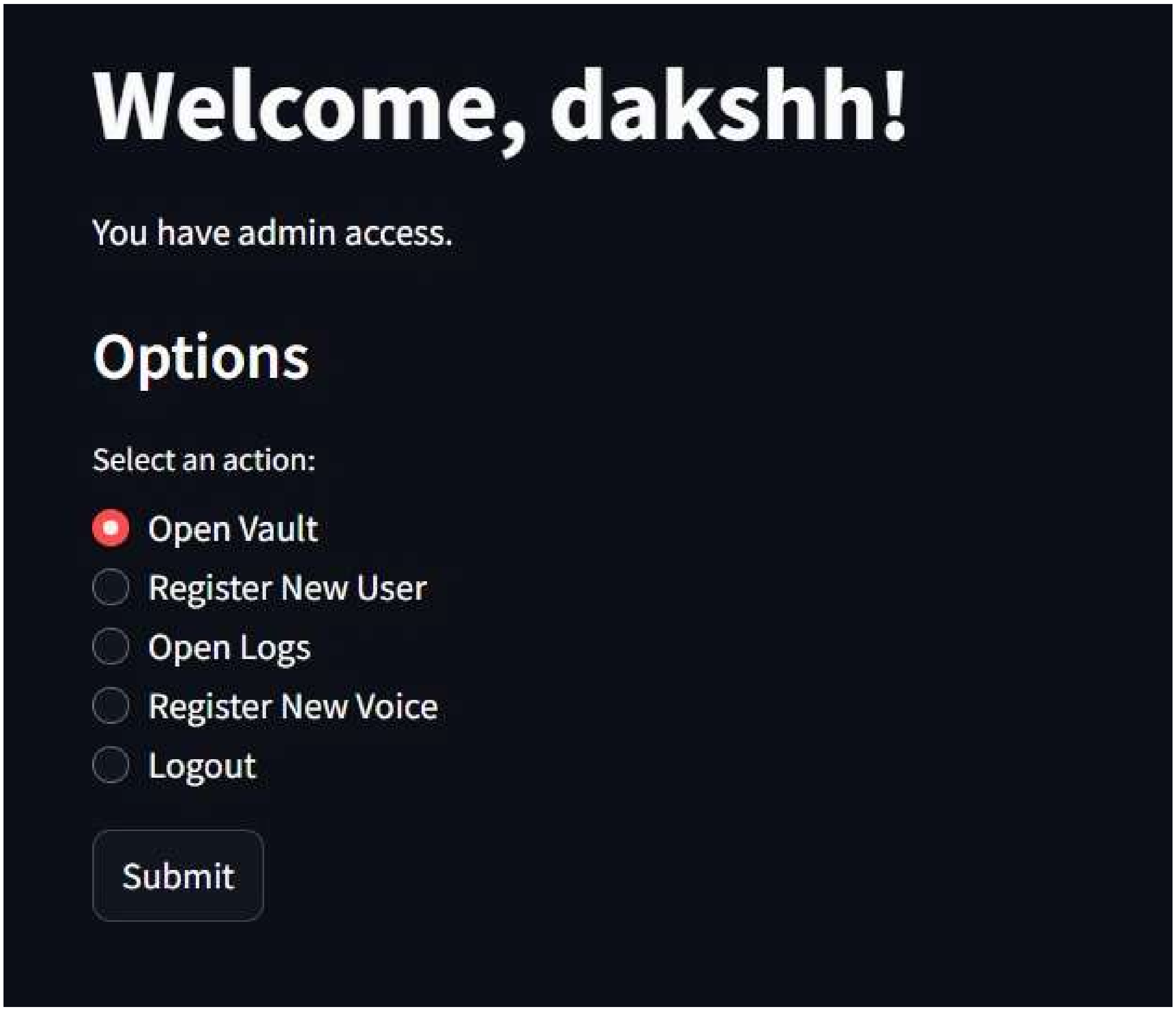
GUI:



Login Page

Username

Password



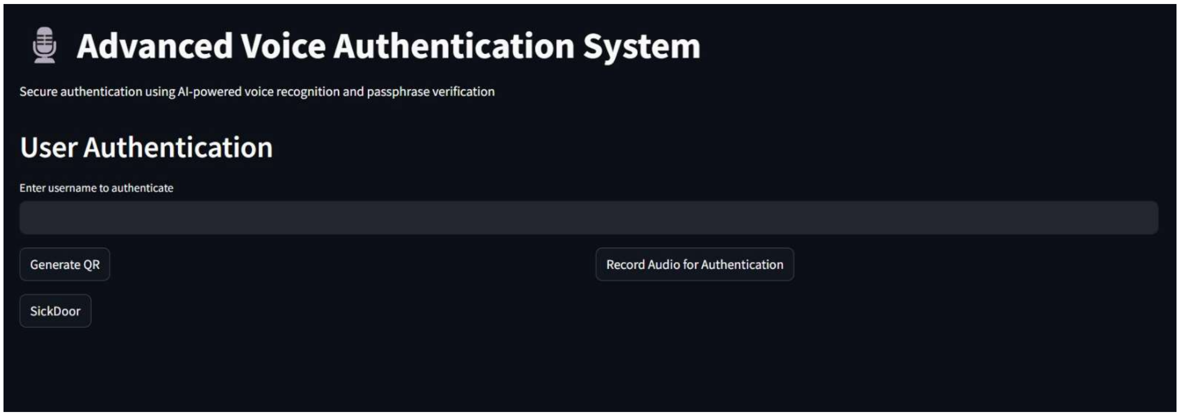
Welcome, dakshh!

You have admin access.

Options

Select an action:

- ● Open Vault
- ○ Register New User
- ○ Open Logs
- ○ Register New Voice
- ○ Logout

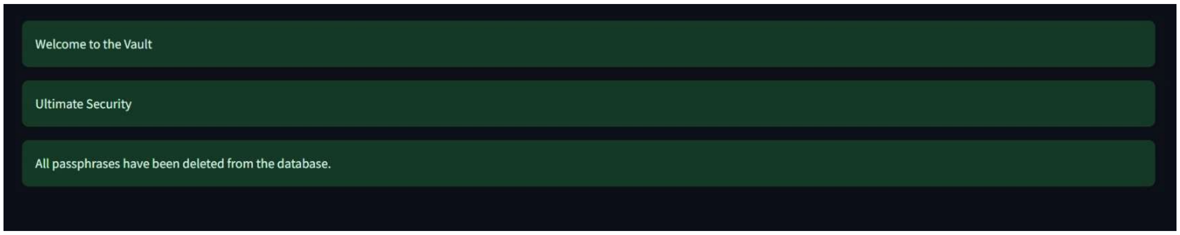


🎙 Advanced Voice Authentication System

Secure authentication using AI-powered voice recognition and passphrase verification

User Authentication

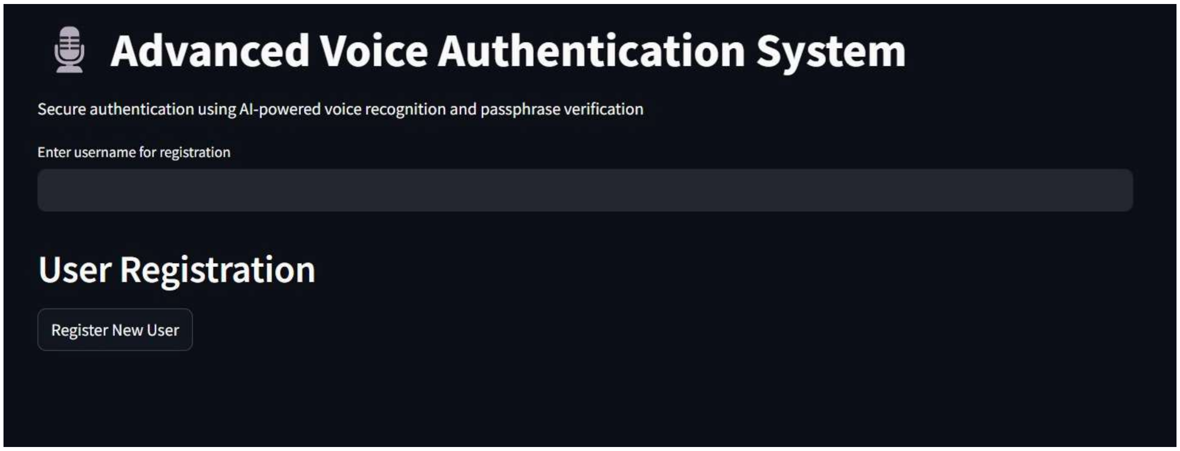
Enter username to authenticate



Welcome to the Vault

Ultimate Security

All passphrases have been deleted from the database.

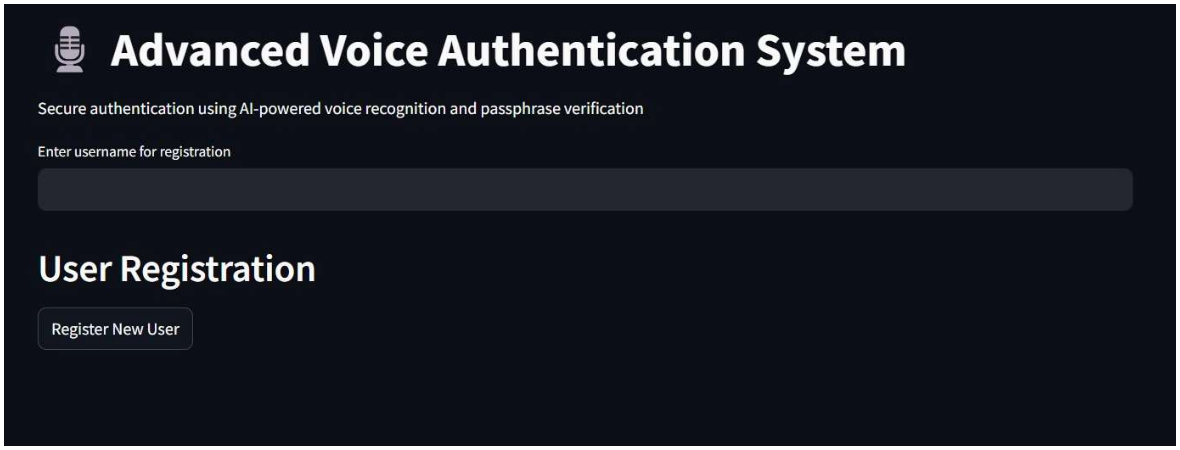


🎙 Advanced Voice Authentication System

Secure authentication using AI-powered voice recognition and passphrase verification

Enter username for registration

User Registration

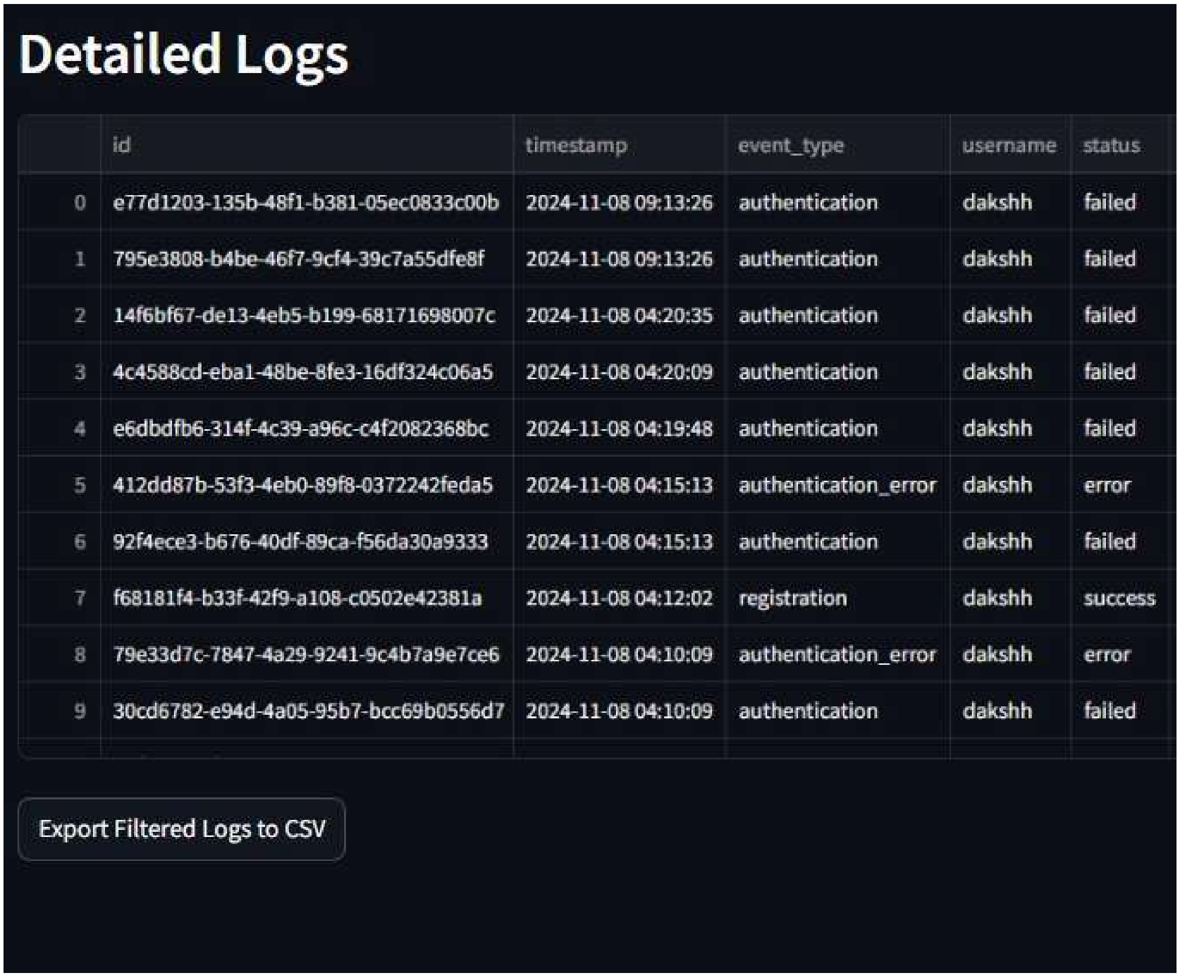


🎙 Advanced Voice Authentication System

Secure authentication using AI-powered voice recognition and passphrase verification

Enter username for registration

User Registration

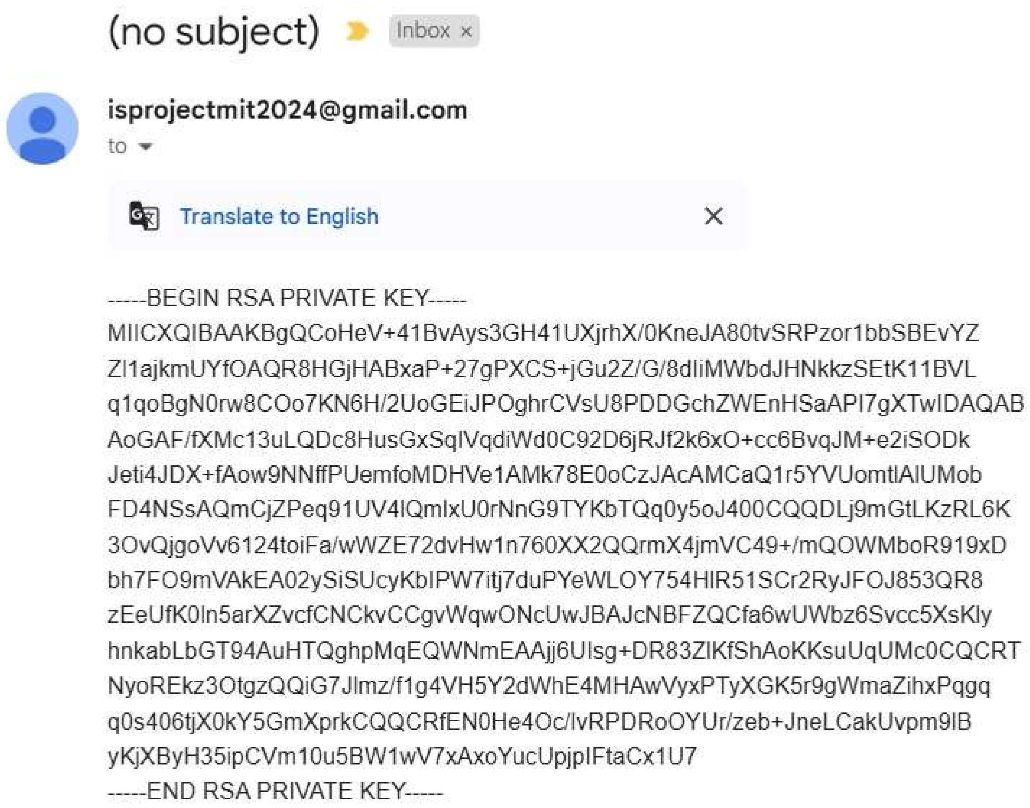


Detailed Logs

	id	timestamp	event_type	username	status
0	e77d1203-135b-48f1-b381-05ec0833c00b	2024-11-08 09:13:26	authentication	dakshh	failed
1	795e3808-b4be-46f7-9cf4-39c7a55dfe8f	2024-11-08 09:13:26	authentication	dakshh	failed
2	14f6bf67-de13-4eb5-b199-68171698007c	2024-11-08 04:20:35	authentication	dakshh	failed
3	4c4588cd-eba1-48be-8fe3-16df324c06a5	2024-11-08 04:20:09	authentication	dakshh	failed
4	e6dbdfb6-314f-4c39-a96c-c4f2082368bc	2024-11-08 04:19:48	authentication	dakshh	failed
5	412dd87b-53f3-4eb0-89f8-0372242feda5	2024-11-08 04:15:13	authentication_error	dakshh	error
6	92f4ece3-b676-40df-89ca-f56da30a9333	2024-11-08 04:15:13	authentication	dakshh	failed
7	f68181f4-b33f-42f9-a108-c0502e42381a	2024-11-08 04:12:02	registration	dakshh	success
8	79e33d7c-7847-4a29-9241-9c4b7a9e7ce6	2024-11-08 04:10:09	authentication_error	dakshh	error
9	30cd6782-e94d-4a05-95b7-bcc69b0556d7	2024-11-08 04:10:09	authentication	dakshh	failed

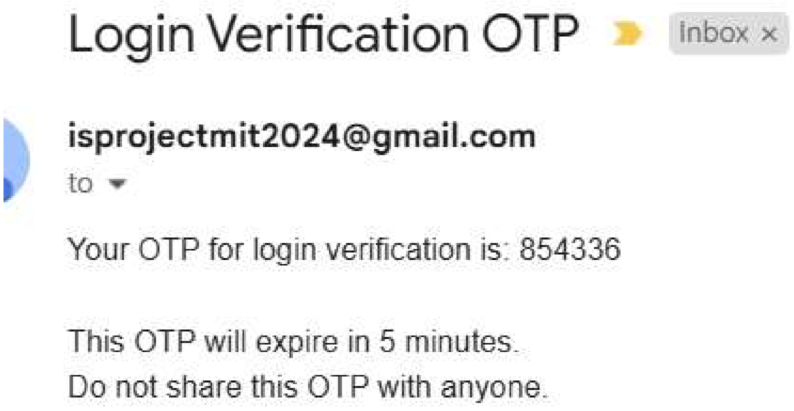
Sample Image

Mail:



isprojectmit2024@gmail.com

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCoHeV+41BvAys3GH41UXjrhX/0KneJA80tvSRPzor1bbSBEvYZ
Zl1ajkmUYfOAQR8HGjHABxaP+27gPXCS+jGu2Z/G/8dIiMWbdJHNkkzSEtK11BVL
q1qoBgN0rw8COo7KN6H/2UoGEiJPOghrCVsU8PDDGchZWEnHSaAPI7gXTwIDAQAB
AoGAF/fXMc13uLQDc8HusGxSqlVqdiWd0C92D6jRJf2k6xO+cc6BvqJM+e2iSODk
Jeti4JDX+fAow9NNffPUemfoMDHVe1AMk78E0oCzJAcAMCaQ1r5YVUomtlAlUMob
FD4NSsAQmCjZPeq91UV4lQmlxU0rNnG9TYKbTQq0y5oJ400CQQDLj9mGtLKzRL6K
3OvQjgoVv6124toiFa/wWZE72dvHw1n760XX2QQrmX4jmVC49+/mQOWMboR919xD
bh7FO9mVAkEA02ySiSUcyKbIPW7itj7duPYeWLOY754HlR51SCr2RyJFOJ853QR8
zEeUfK0In5arXZvcfCNCkvCCgvWqwONcUwJBAJcNBFZQCfa6wUWbz6Svcc5XsKly
hnkabLbGT94AuHTQghpMqEQWNmEAAjj6UIsg+DR83ZlKfShAoKKsuUqUMc0CQCRT
NyoREkz3OtgzQQiG7Jlmz/f1g4VH5Y2dWhE4MHAwVyxPTyXGK5r9gWmaZihxPqgq
q0s406tjX0kY5GmXprkCQQCRfEN0He4Oc/lvRPDRoOYUr/zeb+JneLCakUvpm9lB
yKjXByH35ipCVm10u5BW1wV7xAxoYucUpjpIFtaCx1U7
-----END RSA PRIVATE KEY-----
```

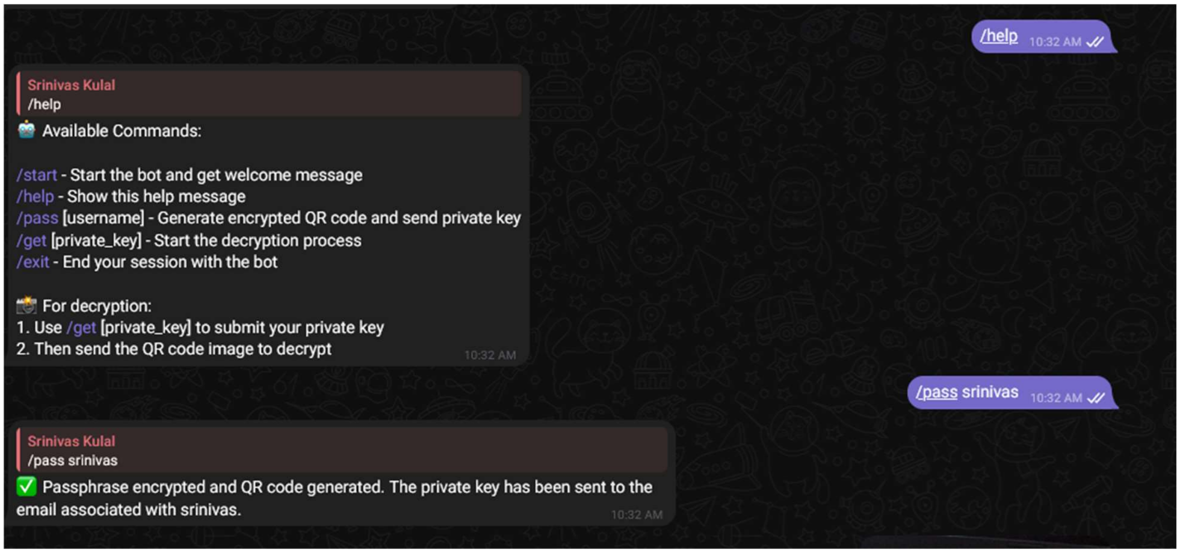


isprojectmit2024@gmail.com

Your OTP for login verification is: 854336

This OTP will expire in 5 minutes.
Do not share this OTP with anyone.

BOT:



/help 10:32 AM

Srinivas Kulal
/help

🤖 Available Commands:

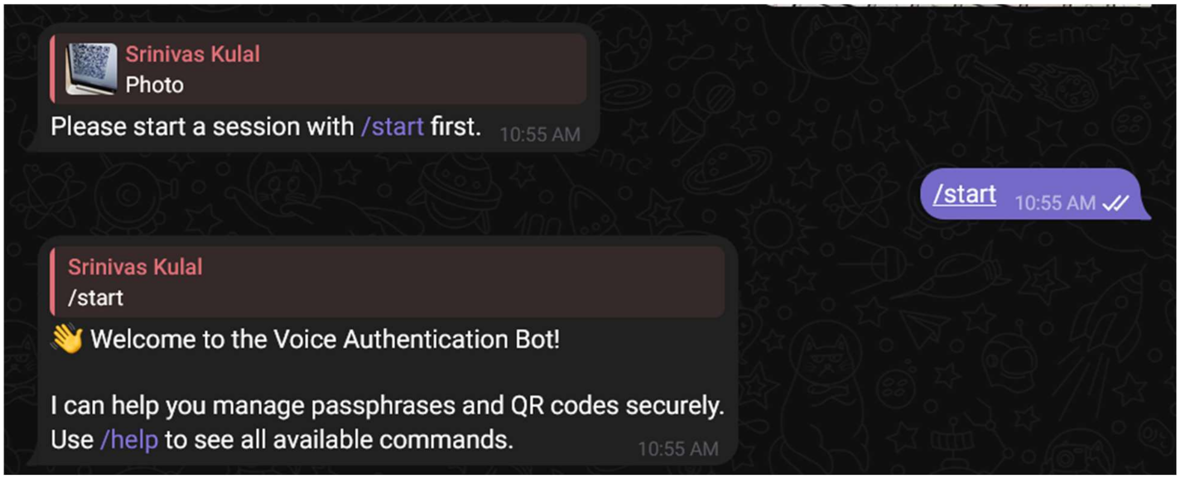
/start - Start the bot and get welcome message
/help - Show this help message
/pass [username] - Generate encrypted QR code and send private key
/get [private_key] - Start the decryption process
/exit - End your session with the bot

📸 For decryption:
1. Use /get [private_key] to submit your private key
2. Then send the QR code image to decrypt
10:32 AM

/pass srinivas 10:32 AM

Srinivas Kulal
/pass srinivas

✅ Passphrase encrypted and QR code generated. The private key has been sent to the email associated with srinivas. 10:32 AM



Srinivas Kulal
Photo

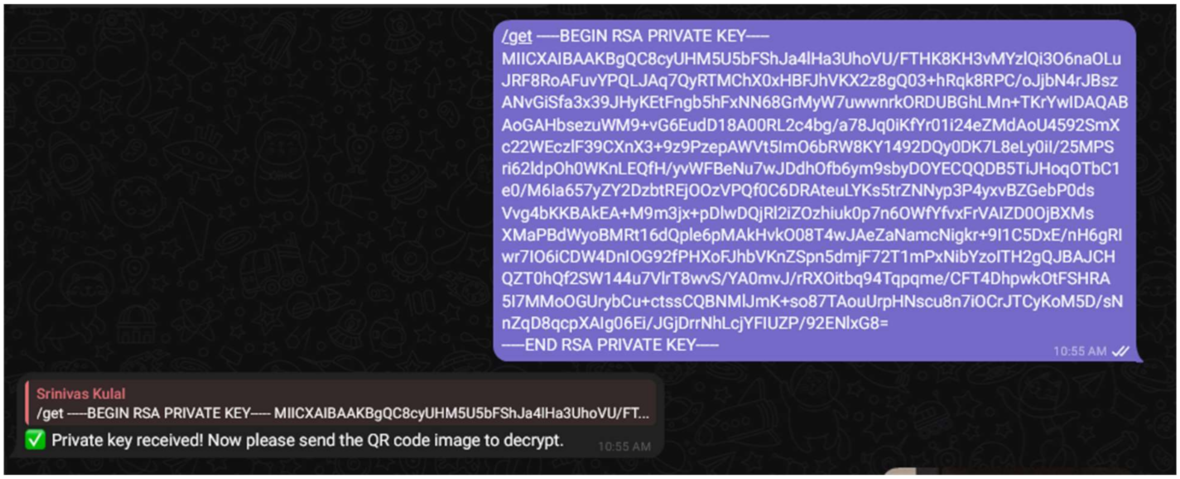
Please start a session with /start first. 10:55 AM

/start 10:55 AM

Srinivas Kulal
/start

👋 Welcome to the Voice Authentication Bot!

I can help you manage passphrases and QR codes securely.
Use /help to see all available commands. 10:55 AM

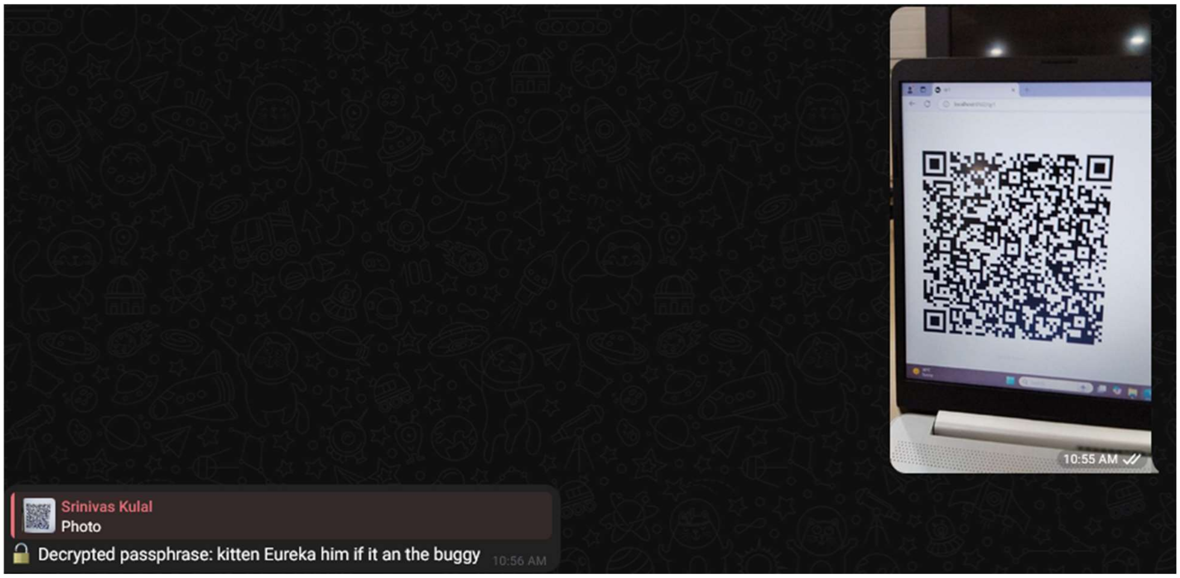


```
/get ——BEGIN RSA PRIVATE KEY——
MIICXAIBAAKBgQC8cyUHM5U5bFShJa4lHa3UhoVU/FTHK8KH3vMYzlQi3O6naOLu
JRF8RoAFuvYPQLJAq7QyRTMChX0xHBFJhVKX2z8gQ03+hRqk8RPC/oJjbN4rJBsz
ANvGiSfa3x39JHyKEtFngb5hFxNN68GrMyW7uwwnrkORDUBGhLMn+TKrYwIDAQAB
AoGAHbsezuWM9+vG6EudD18A00RL2c4bg/a78Jq0iKfYr01i24eZMdAoU4592SmX
c22WEczlF39CXnX3+9z9PzepAWVt5lmO6bRW8KY1492DQy0DK7L8eLy0iI/25MPS
ri62ldpOh0WKnLEQfH/yvWFBeNu7wJDdhOfb6ym9sbyDOYECQQDB5TiJHoqOTbC1
e0/M6la657yZY2DzbtREjOOzVPQf0C6DRAteuLYKs5trZNNyp3P4yxvBZGebP0ds
Vvg4bKKBAkEA+M9m3jx+pDlwDQjRl2iZOzhiuk0p7n6OWfYfvxFrVAIZD0OjBXMs
XMaPBdWyoBMRt16dQple6pMAkHvkO08T4wJAeZaNamcNigkr+9I1C5DxE/nH6gRl
wr7IO6iCDW4DnlOG92fPHXoFJhbVKnZSpn5dmjF72T1mPxNibYzoITH2gQJBAJCH
QZT0hQf2SW144u7VlrT8wvS/YA0mvJ/rRXOitbq94Tqpqme/CFT4DhpwkOtFSHRA
5I7MMoOGUrybCu+ctssCQBNMlJmK+so87TAouUrpHNscu8n7iOCrJTCyKoM5D/sN
nZqD8qcpXAIg06Ei/JGjDrrNhLcjYFIUZP/92ENlxG8=
——END RSA PRIVATE KEY——
```

10:55 AM

Srinivas Kulal
/get ——BEGIN RSA PRIVATE KEY—— MIICXAIBAAKBgQC8cyUHM5U5bFShJa4lHa3UhoVU/FT...

✅ Private key received! Now please send the QR code image to decrypt. 10:55 AM

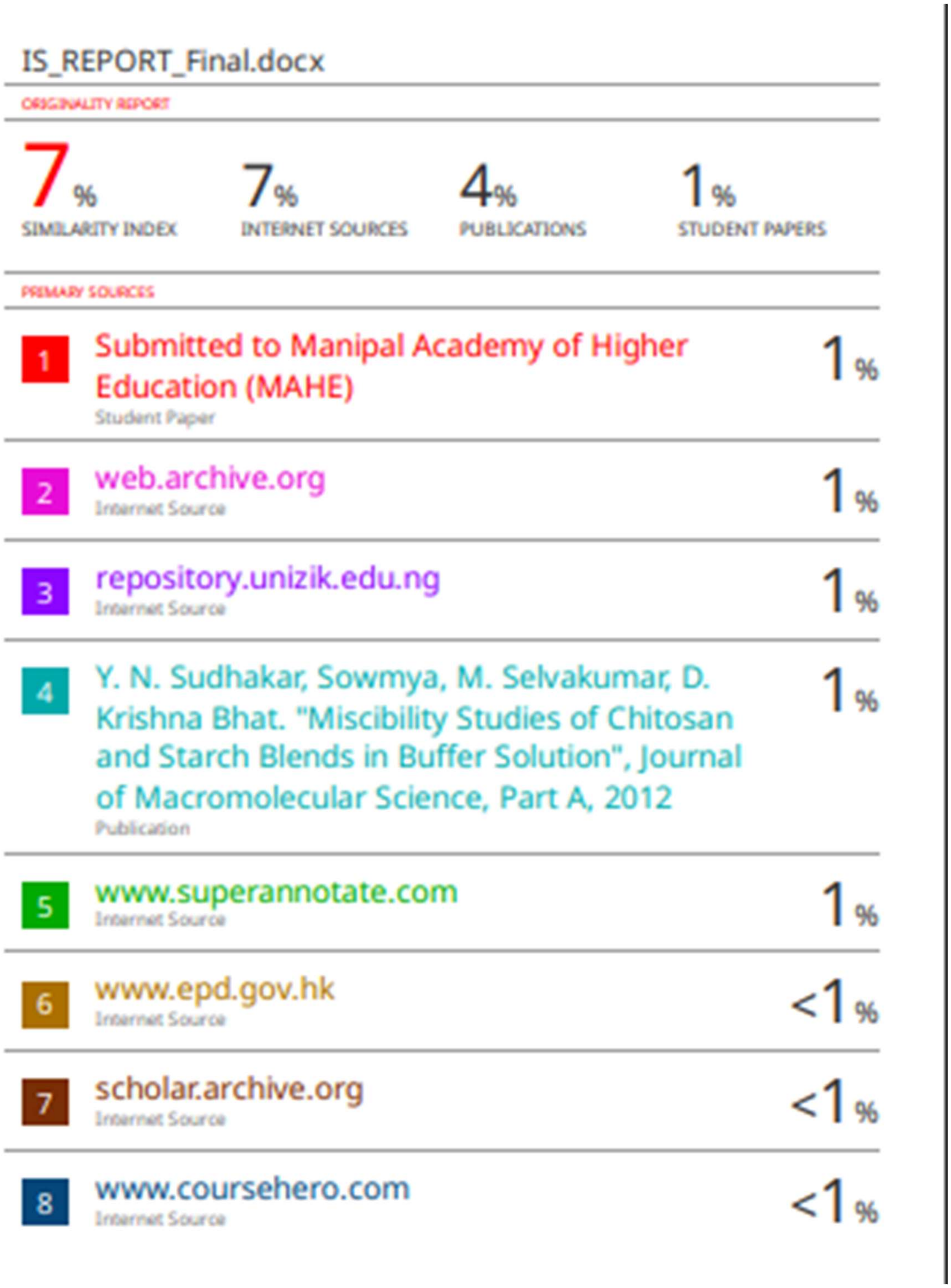


10:55 AM

Srinivas Kulal
Photo

🔒 Decrypted passphrase: kitten Eureka him if it an the buggy 10:56 AM

Plagiarism Report:



IS_REPORT_Final.docx

ORIGINALITY REPORT

7%	7%	4%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Manipal Academy of Higher Education (MAHE) Student Paper	1%
2	web.archive.org Internet Source	1%
3	repository.unizik.edu.ng Internet Source	1%
4	Y. N. Sudhakar, Sowmya, M. Selvakumar, D. Krishna Bhat. "Miscibility Studies of Chitosan and Starch Blends in Buffer Solution", Journal of Macromolecular Science, Part A, 2012 Publication	1%
5	www.superannotate.com Internet Source	1%
6	www.epd.gov.hk Internet Source	<1%
7	scholar.archive.org Internet Source	<1%
8	www.coursehero.com Internet Source	<1%