WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Smart Door Unlocking System Using Voice Authentication

G. Chandu Preethi[1], B. Syam Sundar[2], K. Thorani Nyshidha[3], K. Krishna[4], Mr. CH. Viswanathasarma[5]

[1,2,3,4] Department of CSE(AL & ML), GMRIT, Rajam, India
[5]Senior Assistant Professor, Department of CSE(AL & ML), GMRIT, Rajam, India
DOI : https://doi.org/10.55248/gengpi.6.0425.14185

ABSTRACT:

Voice authentication, also called speaker verification, is a way to confirm a person's identity using their unique voice patterns. A voice-recognized door lock system is designed to enhance security and convenience by replacing traditional access methods like keys and passwords. The system employs voice authentication technology to identify authorized individuals using their unique vocal patterns. Speech recognition techniques are implemented to capture and process voice commands, while feature extraction and classification ensure robust identification and security. The system uses Mel Frequency Cepstral Coefficients (MFCC) for feature extraction, and a Convolutional Neural Network (CNN) model verifies the voice against a pre-trained directory of authorized users. To strengthen security, an additional mechanism is implemented: if an unauthorized person attempts to access the door, the system will send an email alert to the administrator along with a one-time password (OTP). The system will only grant access if the correct OTP is submitted within a specified time limit of 90 seconds. If the OTP is not entered within this timeframe, access will be automatically denied. This solution is scalable and user-friendly, and it ensures security across various environmental conditions. It holds potential applications in homes, banks, offices, and public spaces, offering a modern approach to secure access control.

Keywords: Voice Authentication, Speaker Verification, Convolutional Neural Network (CNN), Mel Frequency Cepstral Coefficients (MFCC), Email Alert System, Smart Access Control.

1.Introduction

In recent years, advancements in technology have significantly improved security systems, making them more reliable, intelligent, and user-friendly. One such innovation is voice authentication, also known as speaker verification, which confirms a person's identity by analyzing the unique patterns of their voice. Unlike traditional methods such as keys, passwords, or access cards, voice-based systems offer a hands-free and biometric approach to secure access, reducing the risk of unauthorized entry and increasing convenience.

The system uses Mel Frequency Cepstral Coefficients (MFCC) to capture the unique features of a person's voice. A Convolutional Neural Network (CNN) model processes these features and matches them with a stored database of authorized voices. To enhance security further, the system incorporates an alert mechanism: if an unauthorized voice attempt is detected, an email notification is sent to the administrator along with a One-Time Password (OTP). Access is only granted if the correct OTP is entered within 90 seconds; otherwise, the request is denied. For added security, the system sends notifications to administrators when it detects unauthorized attempts to gain access. This feature ensures quick responses and minimizes security risks, making the system suitable for homes, offices, banks, and other secure areas. This paper outlines the development and working of the voice-authenticated door lock system. It describes the system architecture, voice recognition techniques, and security measures in detail. The results demonstrate the effectiveness and practicality of using voice authentication for secure access management.

1.1 Study Objective

The primary objective of this study is to design, develop, and evaluate a voice-authenticated door lock system that leverages biometric voice recognition for secure and convenient access control. The system aims to enhance security by utilizing Mel Frequency Cepstral Coefficients (MFCC) for feature extraction and a Convolutional Neural Network (CNN) for speaker verification. Additionally, the study implements an advanced security mechanism wherein, if an unauthorized person attempts to access the door, the system will send an email notification to the administrator along with a one-time password (OTP). The system will only grant access if the user enters the correct OTP within a 90-second time limit. If the OTP is not submitted within this time, access will be automatically denied. Through this research, the objective is to demonstrate the system's reliability, accuracy, and usability in various environments, including homes, offices, banks, and public facilities.

1.2 Problem Statement

Traditional door locking systems rely on physical keys, passwords, or PINs, which are prone to theft, loss, or unauthorized access. Additionally, managing multiple keys or remembering complex passwords can be inconvenient and insecure. To address these issues, there is a need for a secure, user-friendly, and efficient access control system. This project aims to develop a voice-authenticated door lock system using voice recognition technology. By employing Mel Frequency Cepstral Coefficients (MFCC) for feature extraction and a Convolutional Neural Network (CNN) for voice verification, the system ensures accurate and reliable speaker authentication. Furthermore, the system includes an administrative OTP approval mechanism. In case an unauthorized access attempt is detected, an email alert is sent to the administrator containing an OTP. Access is granted only if the correct OTP is entered within 90 seconds; otherwise, the access request is automatically denied. This additional layer of verification enhances security while maintaining a seamless and intuitive user experience.

2. Literature Review

Saxena, N., & Varshney, D. [1] developed Smart home devices offer convenience but also introduce security risks that can affect user adoption. Researchers emphasize the need for stronger protective measures to ensure reliable security. Advanced deep learning models, such as Deep Siamese Networks and multi-task Convolutional Neural Networks (CNNs), have shown significant improvements in face recognition accuracy. Real-time processing using neural networks enables faster detection and alerts for unauthorized access. Studies suggest further research to enhance recognition capabilities for masked faces and expand applications to public areas like malls and offices. This paper builds upon these findings to implement a robust voice-authenticated door lock system for secure access management.

Palivela, L. H., Dharmalingam, V., & Elangovan, P. [2] proposed Gaussian Mixture Models (GMMs) have been widely used in speaker verification for capturing speech variations, but they often face challenges in noisy environments. Long Short-Term Memory (LSTM) networks offer a better alternative by efficiently handling sequential voice data and maintaining long-term dependencies, leading to improved verification accuracy. Various feature extraction methods like Mel Frequency Cepstral Coefficients (MFCCs), Linear Predictive Coding (LPC), and Perceptual Linear Prediction (PLP) are used to capture voice characteristics, with MFCCs being the most effective. Recent studies show that integrating deep learning models with advanced feature extraction techniques significantly enhances the accuracy and security of voice authentication systems. This paper applies these insights to develop a reliable and secure voice-authenticated door lock system.

Tiwari, M., & Verma, D. K. [3] presented Gaussian Mixture Models (GMMs) are widely used for speaker identification as they effectively capture variations in speech patterns, even in noisy environments. Hidden Markov Models (HMMs) further enhance accuracy by modeling the temporal dynamics of speech, making them suitable for recognizing phoneme and word transitions. Recent advancements with Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have improved feature extraction and classification, reducing reliance on manual feature engineering. Among various feature extraction techniques, Mel Frequency Cepstral Coefficients (MFCCs) are commonly used as they capture frequency components that resemble human auditory perception, ensuring better speaker distinction. This paper utilizes these insights to develop a reliable voice-authenticated door lock system for secure access control.

Çabuk, U. C., Senocak, T., Demir, E., & Çavdar, A. [4] developed Authentication methods have evolved from traditional passwords to Multi-Factor Authentication (MFA), providing enhanced security by combining multiple verification factors. MFA typically involves knowledge-based factors like passwords, possession-based factors such as devices or tokens, and inherence-based factors like biometrics. While SMS-based authentication using One-Time Passwords (OTPs) is commonly used, it is prone to security threats like SIM swapping and man-in-the-middle attacks. To address these vulnerabilities, researchers are exploring AI-powered security systems, behavioral biometrics, and blockchain-based authentication for stronger protection. This paper applies biometric voice authentication to offer a secure and convenient alternative for door lock systems, ensuring reliable access management.

Zhang, R., Yan, Z., Wang, X., & Deng, R. H. [5] presents Traditional voice authentication systems face security challenges like voiceprint leakage, replay attacks, and adversarial threats, increasing the risk of identity theft. To mitigate these risks, VOLERE's innovative voiceprint synthesis uses the Log Magnitude Approximate (LMA) vocal tract model to generate anonymous voiceprints, making impersonation more difficult. Additionally, security can be further improved by using User Agents, Relying Parties, and Authentication Providers to create random personal voice challenges, eliminating the need for passwords. Researchers emphasize enhancing user interfaces, security mechanisms, and system adaptability to improve the overall usability and effectiveness of biometric authentication. This paper applies these concepts to build a secure voice-authenticated door lock system with real-time monitoring and notifications.

Wankhede, N., & Wagh, S. [6] evaluates Mel Frequency Cepstral Coefficients (MFCC) play a key role in speaker recognition by extracting unique voice features. To further enhance data integrity and noise resistance, polar coding has been introduced, leading to improved accuracy in voice authentication systems. Studies have shown that polar coding can boost recognition accuracy from 90% to 95.2%, while reducing bit error rates. Performance metrics such as Recognition Ratio (RR), False Acceptance Ratio (FAR: 0.09), and False Rejection Ratio (FRR: 0.19) demonstrate the reliability of this approach. Future research aims to reduce the computational complexity of polar coding and integrate voice biometrics into multi-factor authentication systems. This paper applies these advancements to develop a secure and efficient voice-authenticated door lock system.

Perdana, N. J., Herwindiati, D. E., & Sarmin, N. H. [7] presents Gaussian Mixture Models (GMM) are extensively used in voice recognition for their ability to model complex speech data distributions. However, the accuracy of GMM models is influenced by recording conditions, with performance

typically around 82%, but it can reach 100% when using earphones to minimize background noise. Feature extraction techniques like Linear Predictive Coding (LPC) further enhance GMM performance by capturing essential speech features, improving classification efficiency. The combination of GMM and LPC ensures reliable voice authentication, making it a practical choice for biometric security applications. This paper builds on these findings to develop a secure and efficient voice-authenticated door lock system.

Zhang, X., Cheng, D., Jia, P., Dai, Y., & Xu, X. [8] developed Multimodal biometric systems combining face and voice recognition offer enhanced security by reducing spoofing risks and improving authentication reliability. Techniques like Haar cascades, Local Binary Patterns (LBP), Mel Frequency Cepstral Coefficients (MFCC), and Gaussian Mixture Models (GMM) are commonly used to achieve greater accuracy and resilience against challenges like lighting changes, noise, and aging. Adaptive fusion methods that integrate face and voice data significantly increase the True Accept Rate (TAR) while minimizing False Reject Rate (FRR) and False Accept Rate (FAR). Future research suggests incorporating additional biometrics, such as iris scanning and gait recognition, alongside advanced matching algorithms to further strengthen system security. This paper adopts the concept of biometric authentication using voice recognition to ensure reliable access control in smart door lock systems.

Sanghavi, M. R., Sancheti, S., Patel, B., Shinde, S., & Lunkad, N. [9] explores Biometric authentication methods like face and voice recognition are increasingly being adopted as secure alternatives to traditional key-based home security systems. These technologies offer added convenience, particularly for elderly individuals who may face difficulties using physical locks. However, environmental factors present challenges, as lighting variations can affect face recognition and background noise can reduce voice recognition accuracy. Researchers emphasize the need to balance security, usability, and cost to promote wider adoption of these systems. This paper builds upon these advancements to develop an efficient and user-friendly voice-authenticated door lock system that ensures reliable access control.

Aiswarya, I. P. [10] utilizes Real-time data processing using ARM microcontrollers, motion sensors, and cameras has significantly enhanced biometric authentication systems by enabling quick detection of unauthorized activity. The integration of Internet of Things (IoT) technology allows users to remotely monitor, lock, and unlock doors, as well as receive instant notifications. Multi-layer security mechanisms, such as One-Time Password (OTP) verification, provide an additional layer of protection during user registration and authentication. Moreover, these systems offer scalability and customizable designs, making them adaptable to different environments. This paper applies these concepts to develop a secure and efficient voice-authenticated door lock system with real-time monitoring capabilities.

Nasution, T., & Andesa, K. [11] explores Radio Frequency Identification (RFID) technology is extensively used in automated access control systems due to its speed, accuracy, and affordability, making it a reliable choice for modern security applications. To further enhance security, integrating RFID with voice recognition provides a dual-layer authentication system, ensuring only authorized individuals gain access. Recent advancements suggest the incorporation of additional biometric features to improve security, scalability, and adaptability for larger user bases. However, challenges remain in maintaining voice recognition accuracy across various environmental conditions and developing cost-effective RFID alternatives.

Arifin, R. D. H., & Sarno, R. [12] developed Bluetooth-based security systems face challenges due to limited connectivity, as obstacles like walls and doors reduce the range from 14 meters to 8 meters, affecting usability. Additionally, Android applications used for speech-to-text authentication often experience performance degradation over time. Signal fading and scattering in environments with numerous obstacles further lead to communication disruptions. Noise sensitivity remains a significant issue, as background noise reduces the accuracy and reliability of voice authentication systems. This paper addresses these challenges by implementing a voice-authenticated door lock system using robust speech recognition techniques and reliable IoT components to ensure secure and accurate access management.

Samuel, F. A., Titilayo, A. O., Abiodun, A. O., Modupe, A. O., Oyeladun, M. B., Mayowa, I. R., & Samuel, A. M. [13] evaluates the Internet of Things (IoT) has significantly advanced home automation by reducing human intervention, lowering risks, and improving system efficiency. IoT-driven solutions also optimize energy consumption, contributing to sustainable living through intelligent management. Recent research has introduced innovative methods to enhance energy efficiency, ensuring better protection and control of energy systems. Additionally, the integration of smart assistants like Google Assistant and various sensors has differentiated modern systems, providing enhanced automation and effective power management. This paper leverages these advancements to develop a voice-authenticated door lock system, combining security and convenience through seamless IoT integration.

Sayeduzzaman, M., Hasan, T., Nasser, A. A., & Negi, A. [14] presents the integration of Internet of Things (IoT) technology in smart door systems has significantly improved security and user convenience. However, connectivity challenges often arise, and researchers suggest using LTE technology to ensure reliable network performance. Advanced authentication methods, supported by adaptive machine learning algorithms, further strengthen system security by accurately identifying authorized users. Additionally, efficient data integration and improved communication mechanisms enhance the overall performance and responsiveness of smart door systems. This paper builds on these advancements to develop a secure and efficient voice-authenticated door lock system with reliable connectivity and robust authentication.

Qasim, N. H., Rahim, F., & Bodnar, N. [15] developed an access control systems have evolved from traditional key-lock mechanisms to advanced computer-based solutions that use various credentials like keys, keycards, and biometrics. Among these, speaker recognition technology has gained attention for its ability to identify individuals based on their unique voice patterns, while speech recognition focuses on understanding spoken words. Speaker authentication systems involve both enrollments, where voice data is registered, and verification, which confirms the identity during access attempts. This dual-layer approach enhances security by ensuring only authorized individuals gain entry.

3.Methodology

The voice-authenticated door lock system follows a step-by-step process to ensure secure and convenient access. It starts by capturing the user's voice using a microphone.

3.1 Feature Extraction Process

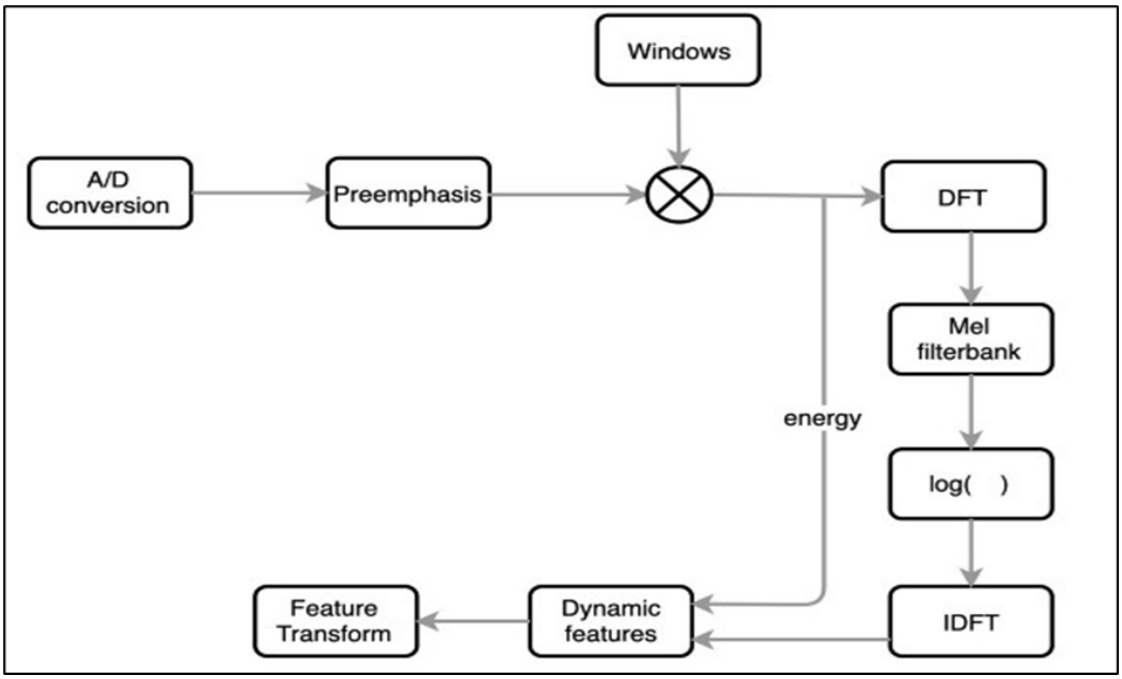

Fig 3.1. Flowchart of MFCC system methodology phases

The analog voice signal is then converted into a digital format using an Analog-to-Digital (A/D) converter. To improve accuracy, a pre-emphasis filter is applied, which enhances the high-frequency components of the voice.

Next, the system extracts unique voice features using Mel Frequency Cepstral Coefficients (MFCC). This involves processes like windowing to minimize data loss, Discrete Fourier Transform (DFT) to convert the signal into the frequency domain, and applying a Mel filter bank to mimic human hearing. These extracted features are essential for distinguishing different voices.

The extracted voice features are then processed using a Convolutional Neural Network (CNN). The CNN compares the input voice with a pre-stored dataset of authorized voice patterns to verify the speaker's identity. This machine learning-based approach ensures accurate and reliable recognition, even under different environmental conditions. Once the voice is verified, the system sends a command to a Node MCU, which controls the solenoid lock to unlock the door. If the system detects an unauthorized voice or multiple failed attempts, it immediately triggers an alert notification to the administrator. This additional security layer ensures quick action against potential threats. This overall process combines voice authentication, real-time processing, and secure access management, making it an efficient solution for enhancing security in homes, offices, and other restricted areas. (Uday Kiran. (14 Aug, 2023) MFCC Technique for Speech Recognition.

https://www.analyticsvidhya.com/blog/2021/06/mfcc-technique-for-speech-recognition/

3.2 Voice recognition model

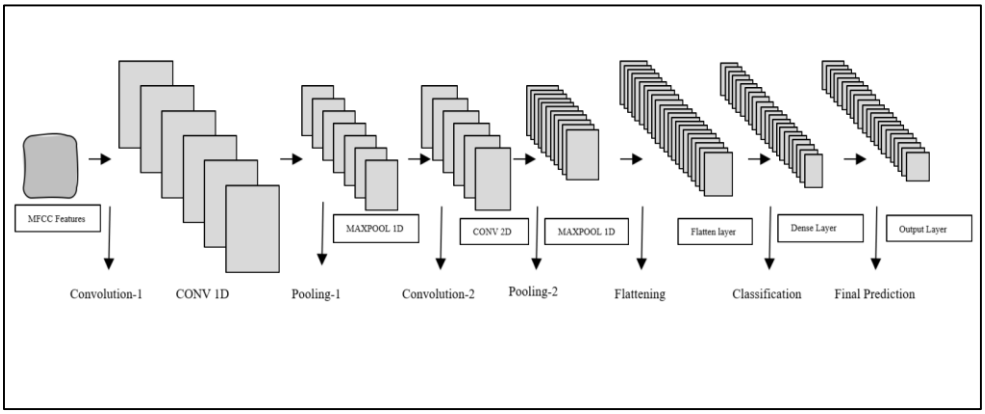

Fig 3.2. Flowchart of Voice Recognition Model

The voice authentication process using a CNN starts with preparing voice data by converting it into numerical features that can be analyzed. A CNN model is designed with layers that extract patterns from these features, such as tones or frequencies unique to each speaker. The model is trained using labeled voice samples, where it learns to associate patterns with specific speakers. After training, it is tested on new voice samples to measure accuracy. If the model performs well, it is saved along with additional tools like a label encoder (to match predictions with speaker names) and a scaler (to preprocess input data for consistency). These saved components allow the system to be deployed for real-world voice authentication tasks, enabling it to identify speakers based on their voice accurately and efficiently.

Flow Chart:

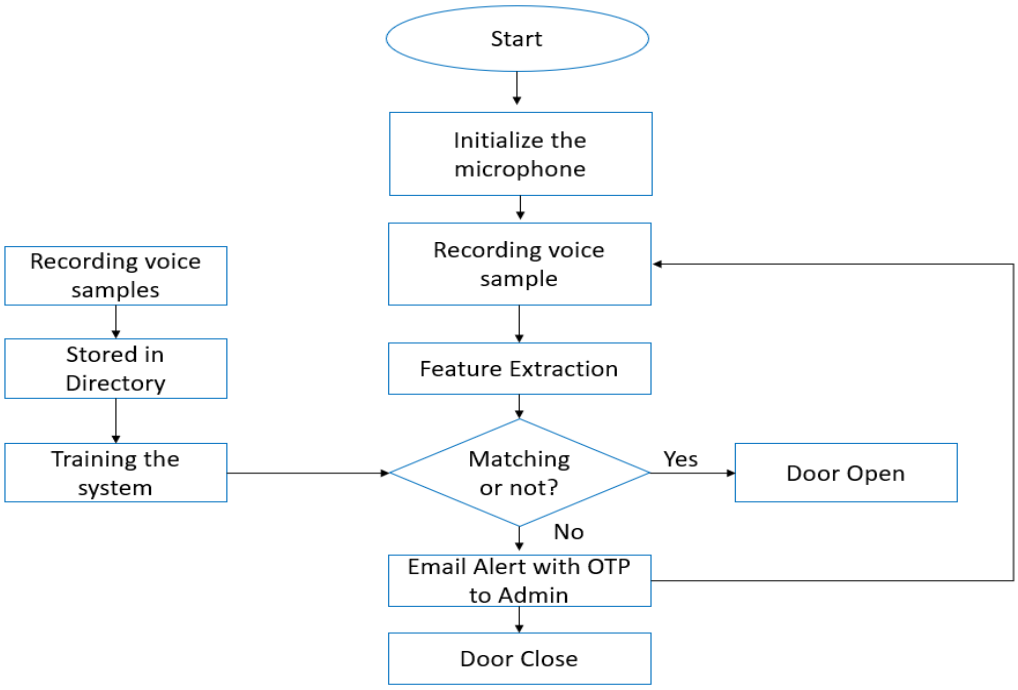

Fig 3.3: Flow Chart

This flowchart illustrates the working of a voice-authenticated door lock system. Initially, users register by recording voice samples, which are stored and used to train a CNN model using MFCC features. During access, the system records the user's voice, extracts features, and checks for a match. If matched, the door opens. If not, an email with an OTP is sent to the admin. The user must enter the correct OTP within 90 seconds to gain access; otherwise, the door remains closed, ensuring an additional layer of security against unauthorized access.

4. RESULTS

A Prototype of our Proposed System is

This figure 4.1 displays the user interface of the Smart Door Unlocking System. It features a “Record & Authenticate” button for voice-based access and confirms successful authentication

With a “User Verified” message.

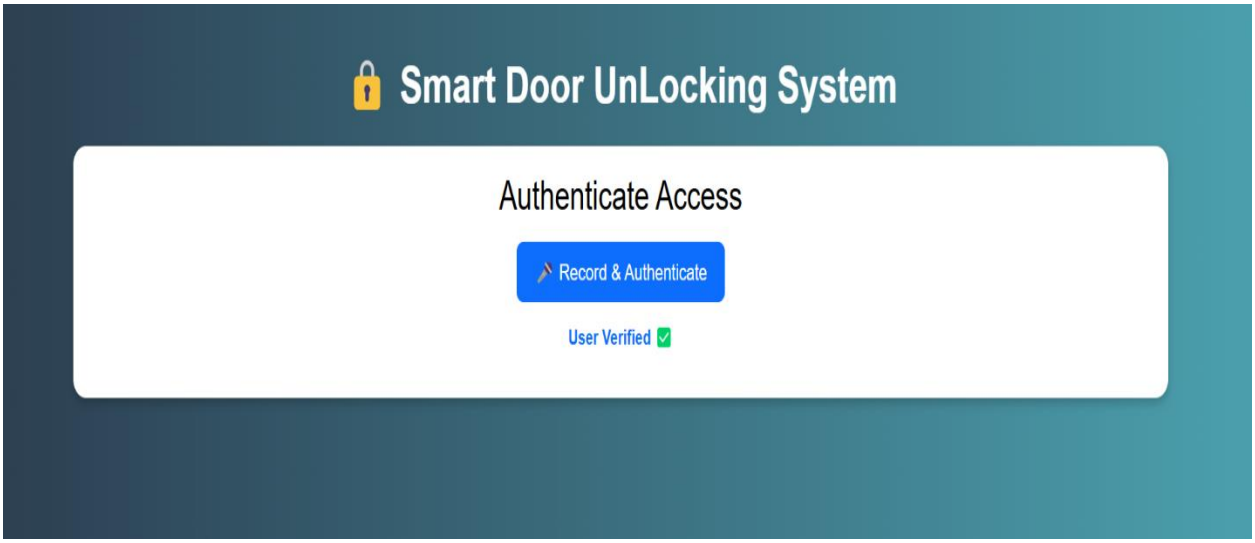

Fig 4.1: “User Verified” message on successful verification

This figure 4.2 shows the OTP verification interface triggered after an unauthorized user attempts access. An OTP is sent to the admin, and the user must enter the correct OTP within the countdown period to gain access.

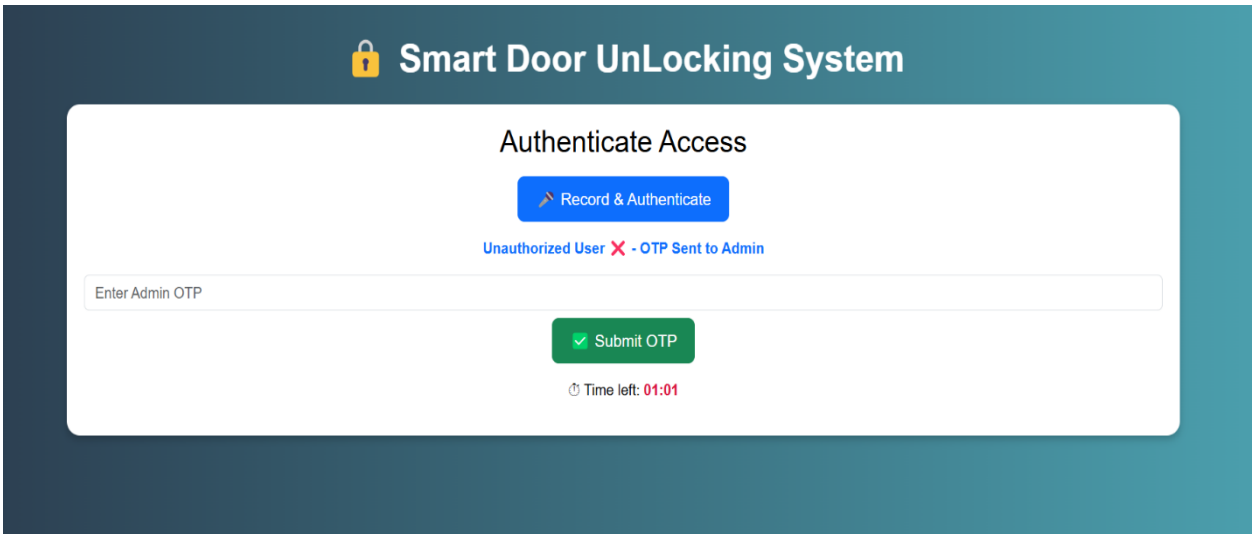

Fig 4.2: OTP Verification for Unauthorized Access

This figure 4.3 shows an email alert titled "Unauthorized Access – OTP Required", indicating an attempted unauthorized login. An OTP (243985) valid for 90 seconds is sent to the recipient for verification.

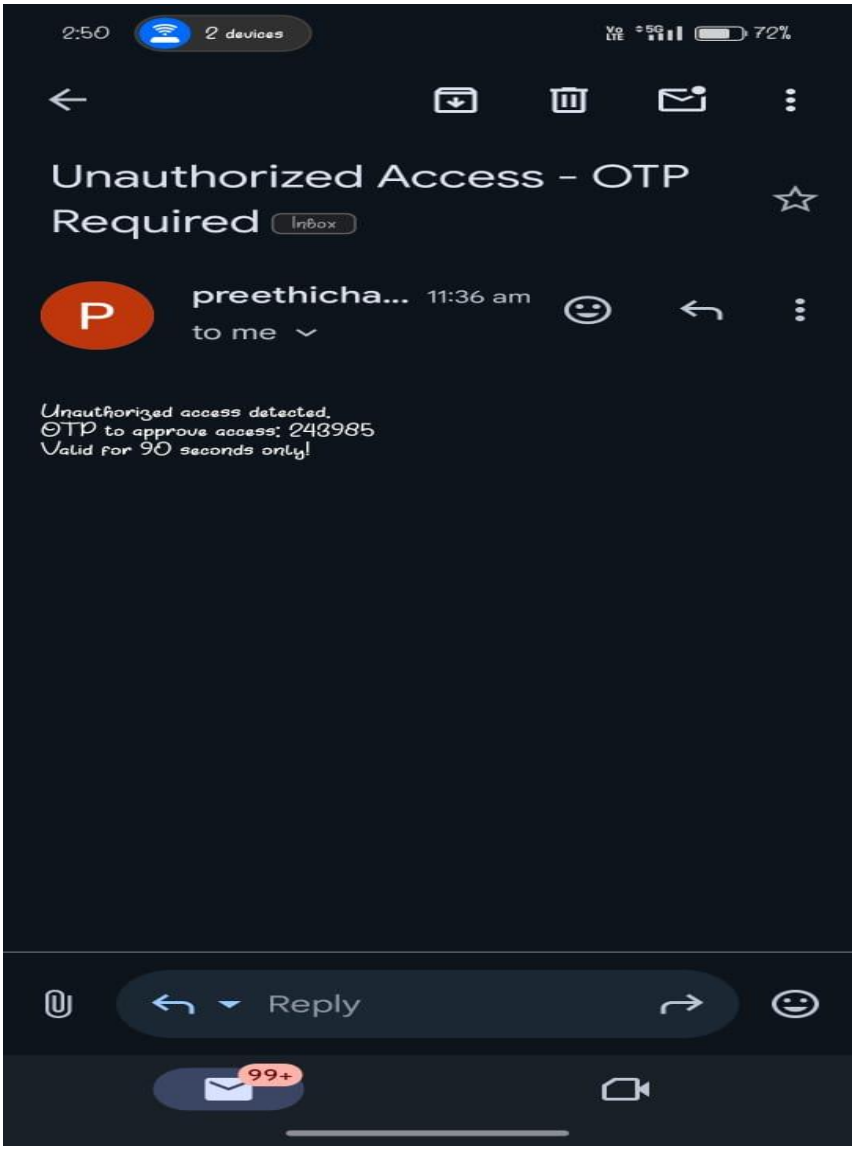

Fig 4.3: Email OTP Notification sent to Admin

This figure 4.4 displays a web interface for a Smart Door Unlocking System, where an unauthorized user is prompted to enter an admin OTP. The system shows an "OTP Expired! Access Denied ✕" message, indicating the OTP verification failed due to time expiration.

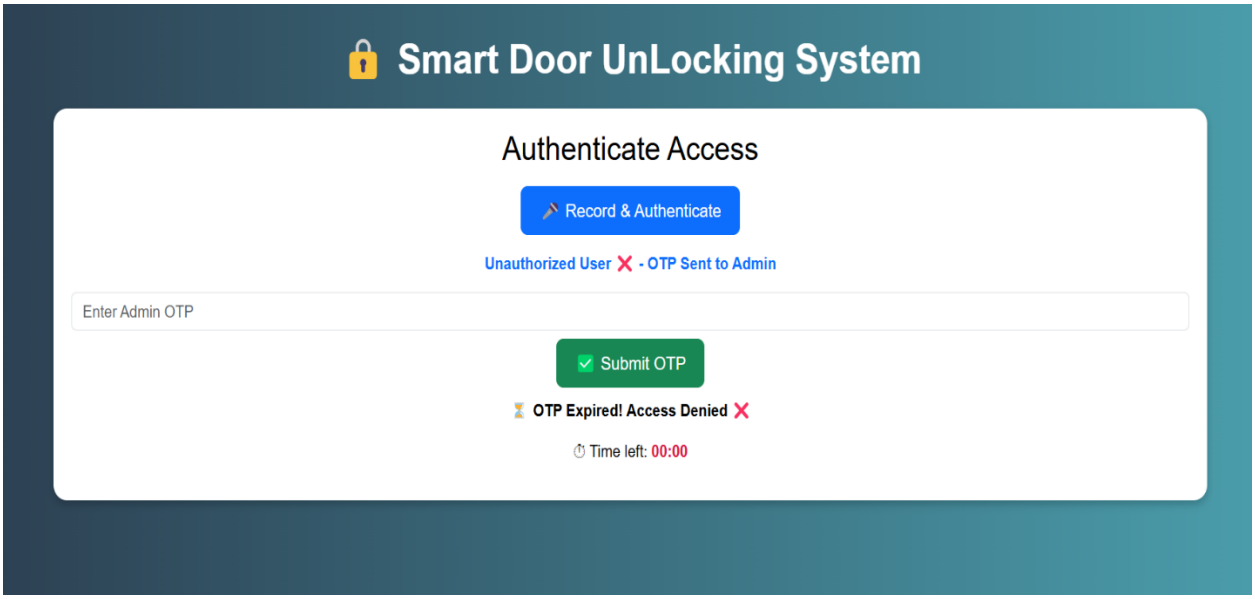

Fig 4.4: OTP Verification Failure and Access Denied

4. CONCLUSION

The proposed Smart Door Unlocking System using Voice Authentication offers a secure and intelligent solution for controlling access to sensitive areas by leveraging the distinctiveness of human voice patterns. By employing MFCC for feature extraction and a Convolutional Neural Network (CNN) for speaker recognition, the system achieves an accuracy of approximately 85%, demonstrating its effectiveness in correctly identifying users. To further enhance security, the system integrates an OTP-based verification mechanism via email for unrecognized users, adding a second layer of authentication. This combination of biometric and token-based security ensures both robustness and reliability. The developed system holds great promise for real-world applications such as smart homes, offices, and secure facilities, delivering a user-friendly, cost-effective, and technologically advanced access control solution.

REFERENCES

[1] Saxena, N., & Varshney, D. (2021). Smart home security solutions using facial authentication and speaker recognition through artificial neural networks. International Journal of Cognitive Computing in Engineering, 2, 154-164.

[2] Palivela, L. H., Dharmalingam, V., & Elangovan, P. (2023, December). Voice Authentication System. In 2023 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) (pp. 1-6). IEEE.

[3] Tiwari, M., & Verma, D. K. Real Voice Recognition and Authentication System: A Comprehensive Review.

[4] Cabuk, U. C., Senocak, T., Demir, E., & Çavdar, A. (2017).A Proposal on initial remote user enrollment for IVR-based voice authentication systems. Int. J. of Advanced Research in Computer and Communication Engineering, 6, 118-123.

[5] A. Duth, A. A. Nambiar, C. B. Teja, and S. Yadav: 'Smart Door System with COVID-19 Risk Factor Evaluation, Contactless Data Acquisition and Sanitization', in Editor (Ed.)^(Eds.): 'Book Smart Door System with COVID-19 Risk Factor Evaluation, Contactless Data Acquisition and Sanitization' (2021, edn.), pp. 1504-11

[6] Wankhede, N., & Wagh, S. (2023). Enhancing Biometric Speaker Recognition Through MFCC Feature Extraction and Polar Codes for Remote Application. IEEE Access, 11, 133921-133930.

[7] Perdana, N. J., Herwindiati, D. E., & Sarmin, N. H. (2022, September). Voicerecognition system for user authentication using gaussian mixture model. In 2022 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET) (pp. 1-5). IEEE.

[8] Zhang, X., Cheng, D., Jia, P., Dai, Y., & Xu, X. (2020). An efficient android-based multimodal biometric authentication system with face and voice. Ieee Access, 8, 102757-102772.

[9] Sanghavi, M. R., Sancheti, S., Patel, B., Shinde, S., & Lunkad, N. (2020). Smart door unlock system using face recognition and voice commands. International Research Journal of Engineering and Technology, 7(06), 3304-3307.

[10] Aiswarya, I. P. (2020). Real Time Smart Door Lock System Using Image Detection and Voice Recognition. International Research Journal of Modernization in Engineering Technology and Science, 2, 393-407.

[11] Nasution, T., & Andesa, K. (2024). RFID and Voice Recognition Based Dual Security System: A Robust Secured Control to Access Through Door Lock Operation: -. Journal of Research and Technology, 10(1), 57-71.

[12] Arifin, R. D. H., & Sarno, R. (2018, March). Door automation system based on speech command and PIN using Android smartphone. In 2018 International Conference on Information and Communications Technology (ICOIACT) (pp. 667-672). IEEE.

[13] Samuel, F. A., Titilayo, A. O., Abiodun, A. O., Modupe, A. O., Oyeladun, M. B., Mayowa, I. R., & Samuel, A. M. (2021). Voice recognition system for door access control using mobile phone. Int. J. Sci. Eng. Appl. [Internet], 10(9), 132-139.

[14] Sayeduzzaman, M., Hasan, T., Nasser, A. A., & Negi, A. (2024). An Internet of Things- Integrated Home Automation with Smart Security System. Automated Secure Computing for Next- Generation Systems, 243-273.

[15] Qasim, N. H., Rahim, F., & Bodnar, N. (2024). A comprehensive investigation of an LTE-enabled smart door system using the Arduino UNO. Edelweiss Applied Science and Technology, 8(4), 697-708.