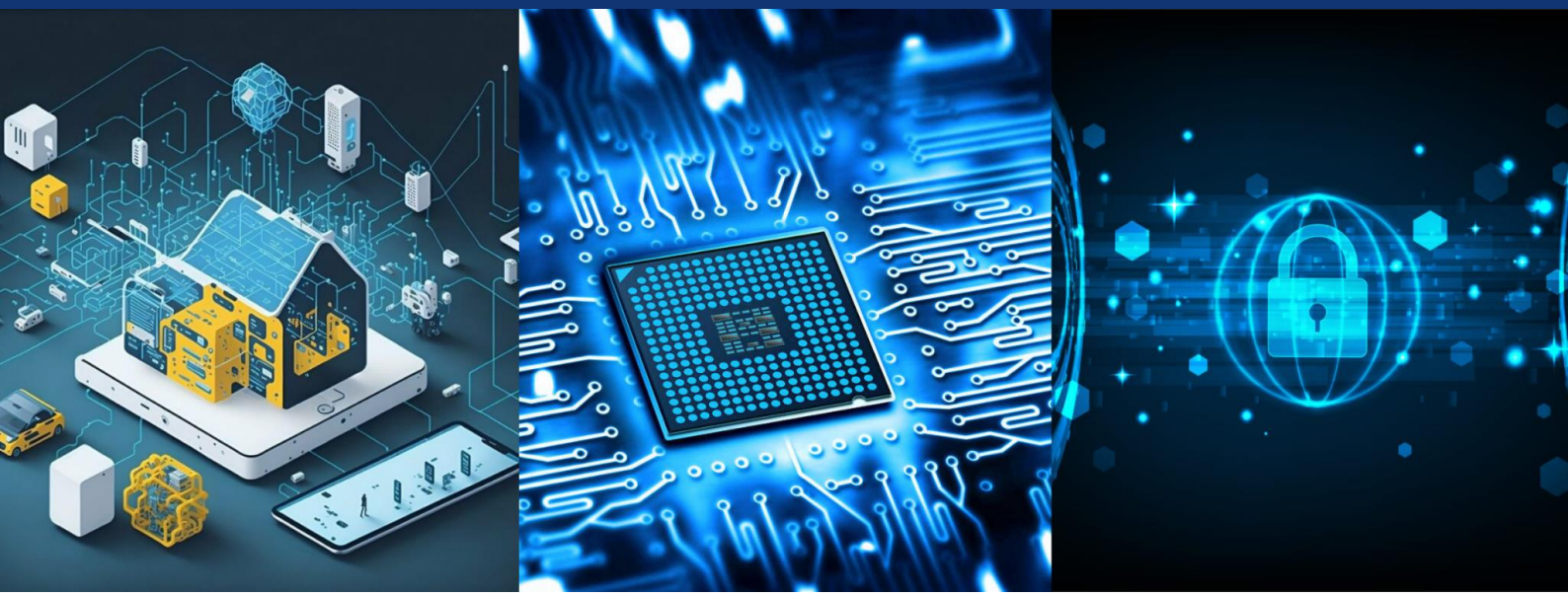
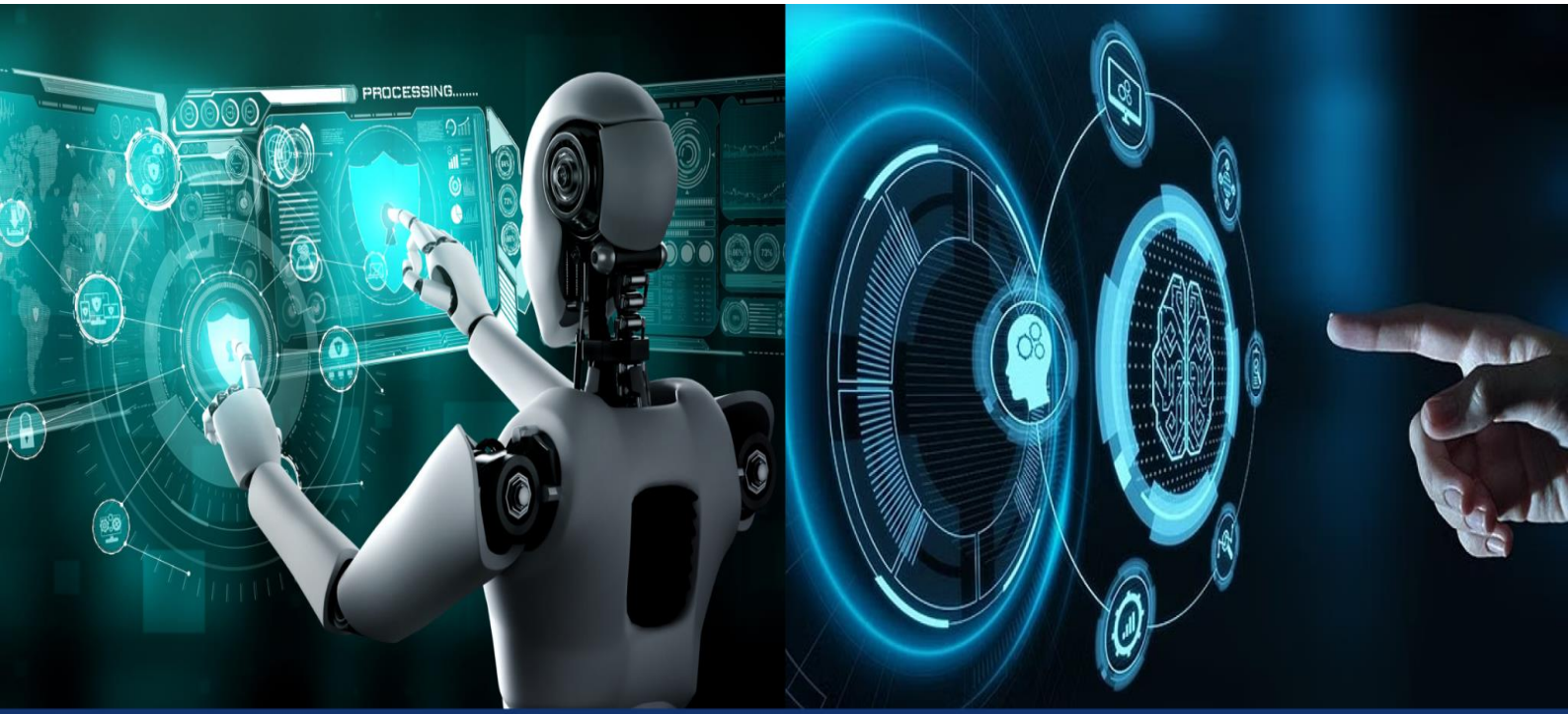
ISSN(O): 2320-9801
ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771 **Volume 13, Issue 4, April 2025**

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304133

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Secure Screen Lock and Voice-Based Mobile Access Application for Android Smartphones

Dr. K. Chaitanya[1], Dimmiti Rakesh[2], Yaraguntala Swathi Priya[2], Chitturi Sindhu Madhuri[2], Munnangi Lakshmi Narasimha[2]

Associate Professor, Department of Computer Science and Engineering, SRK Institute of Technology, Vijayawada, Andhra Pradesh, India [1]

Students, Department of Computer Science and Engineering, SRK Institute of Technology, Vijayawada, Andhra Pradesh, India[2]

ABSTRACT: This paper presents the design and implementation of a voice-controlled mobile access application for Android smartphones. The application provides a secure and convenient alternative to traditional screen lock methods by enabling users to unlock their devices using voice commands, PIN, or biometric authentication. Furthermore, it allows users to access mobile apps and files via voice commands, enhancing accessibility and usability. The system aims to improve security, convenience, and accessibility for smartphone users.

KEYWORDS: Voice Recognition, Android, Biometrics, Screen Lock, Mobile Access, Security.

I. INTRODUCTION

Smartphones are central to modern life, used for everything from communication to banking. Traditional unlocking methods such as PINs and passwords pose challenges including memorability, input errors, and security threats like shoulder surfing or brute-force attacks. Biometric authentication improves security but remains vulnerable to spoofing and hardware limitations.

Voice interfaces provide a natural and hands-free method of device interaction. With advancements in speech recognition and biometric processing, combining these with traditional methods can create a more secure and accessible mobile access solution. This paper proposes a system that integrates voice authentication, PIN entry, and biometric verification for robust, user-friendly smartphone access.

II. LITERATURE REVIEW

Voice recognition has evolved significantly over the past decades. Early work in this field focused on statistical models like Hidden Markov Models (HMMs), as described by Rabiner [1], which effectively captured the probabilistic nature of speech sequences.

The introduction of deep learning, particularly recurrent neural networks (RNNs) and long short-term memory (LSTM) architectures, marked a breakthrough in speech recognition. Hannun et al. [2] presented DeepSpeech, an end-to-end deep learning model that demonstrated superior performance in large vocabulary continuous speech recognition (LVCSR). Similarly, Graves et al. [3] utilized deep recurrent architectures for improved recognition accuracy in noisy and spontaneous speech environments.

Wu et al. [4] conducted comprehensive evaluations of spoofing attacks in speaker verification systems and highlighted the need for advanced countermeasures such as voice liveness detection, anti-spoofing datasets, and anomaly detection techniques.

Yang et al. [5] proposed an enhanced MFA framework for mobile devices that strengthens authentication through redundancy and reduces the likelihood of unauthorized access.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304133

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

In summary, while significant progress has been made in voice recognition, biometric verification, and PIN-based security, most systems treat these mechanisms in isolation. There remains a gap in the literature and in commercial deployment for a unified, multi-factor, voice-controlled mobile access system that provides strong security guarantees and enhances accessibility.

III. EXISTING SYSTEM

Most smartphones use one or a combination of the following:
• **PIN/Password/Pattern Locks:** Widely adopted but easily guessable or forgettable.
• **Biometric Authentication:** Common on newer devices; includes fingerprint and facial recognition.
• **Voice Commands:** Used primarily for virtual assistants, not security.
These methods lack seamless integration and flexible access control. Voice-based unlocking remains limited, with few applications addressing accessibility or multi-factor fallback.

IV. SYSTEM

We propose a secure mobile access application that combines:
• **Voice-Based Unlocking:** Customized voice commands for unlocking and access.
• **Fallback PIN Authentication:** User-defined numeric code.
• **Biometric Authentication:** Fingerprint or facial recognition as an additional layer.
• **Voice Navigation:** Users can open apps and files by voice commands after unlocking the device.
The system fills the gap by combining speech recognition, PIN verification, and biometric authentication with a secure voice-command interface. This multi-modal approach increases accessibility, especially for differently abled users, while enhancing security and usability.

V. WORKFLOW and ARCHITECTURE

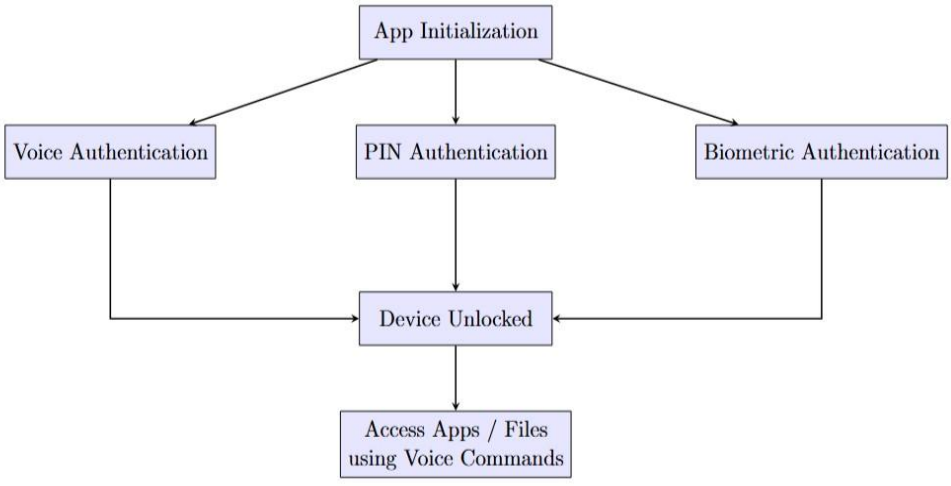


Figure 1: Workflow Diagram of the Voice-Controlled Mobile Access System

In the figure 1, the app is initialized, then the user uses voice, PIN, or biometric authentication to unlock the device. After authentication, the user can access apps or files using voice commands.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304133

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. METHODOLOGY

The methodology adopted for the development of the secure voice-controlled mobile access application consists of the following phases: requirements analysis, system design, module implementation, integration, and testing. The system is divided into modular components to enable extensibility and maintainability.

1.Requirements Analysis

Functional and non-functional requirements were identified to ensure security, usability, and accessibility. Key functional requirements include multi-factor authentication (voice, PIN, biometrics), secure voice command processing, and voice-based app/file access. Nonfunctional requirements focus on real-time performance, privacy, and user-friendly interface design.

2.System Design

The system architecture consists of five major modules:

- **Voice Recognition Module:** Captures and transcribes voice commands using Android's SpeechRecognizer API.
- **Authentication Module:** Implements voice, PIN, and biometric-based authentication.
- **Application/File Access Module:** Maps recognized voice commands to mobile application or file access actions.
- **User Interface Module:** Enables users to set up credentials and receive interactive prompts.

3.Voice Command Processing

1. The user initiates the system through a wake command or tap.
2. Audio input is captured via the device microphone.
3. Speech is transcribed using Android's SpeechRecognizer API.
4. Commands are matched against a predefined set of custom commands using string similarity or keyword mapping.
5. Results are passed to the Access Module for execution.

4.Multi-Factor Authentication Flow

The system supports the following authentication workflow:

- Primary: Voice authentication using voiceprint comparison.
- Secondary: Fallback to PIN if voice verification fails.
- Tertiary: Biometric authentication using fingerprint via BiometricPrompt API.

5.Implementation Environment

The application was developed using:

- Platform: Android Studio
- Language: Java, Kotlin
- APIs: SpeechRecognizer API, BiometricPrompt API
- Testing: Emulators and physical devices running Android 10 and above

6.Testing and Evaluation

Unit and integration testing were conducted to verify the reliability and performance of each module. Usability testing involved real users to assess accessibility, authentication success rates, and voice recognition accuracy in various environments.

IMPLEMENTATION

The application is developed in Java using Android SDK. It uses:

- SpeechRecognizer API for voice recognition.
- BiometricPrompt API for fingerprint and facial authentication.

VII. RESULTS

The outcomes include:

- Secure and user-friendly mobile access.
- Reduced dependency on physical interaction.
- Support for visually or physically impaired users.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304133

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Real-time voice command execution.

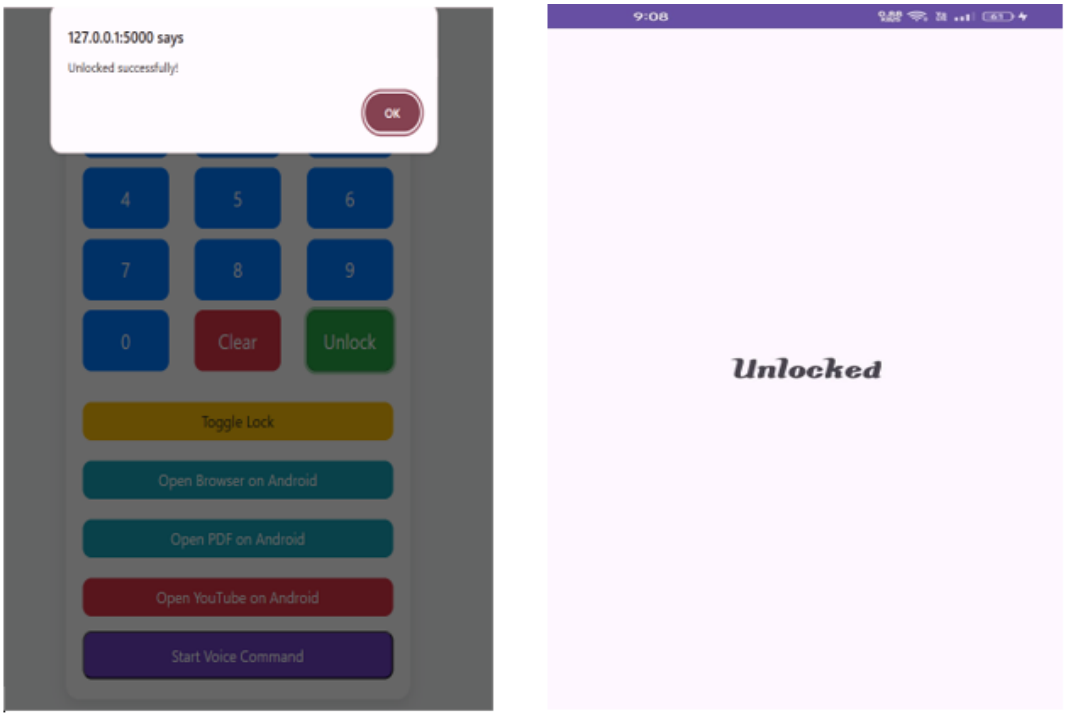


Figure 2: App unlocked by PIN

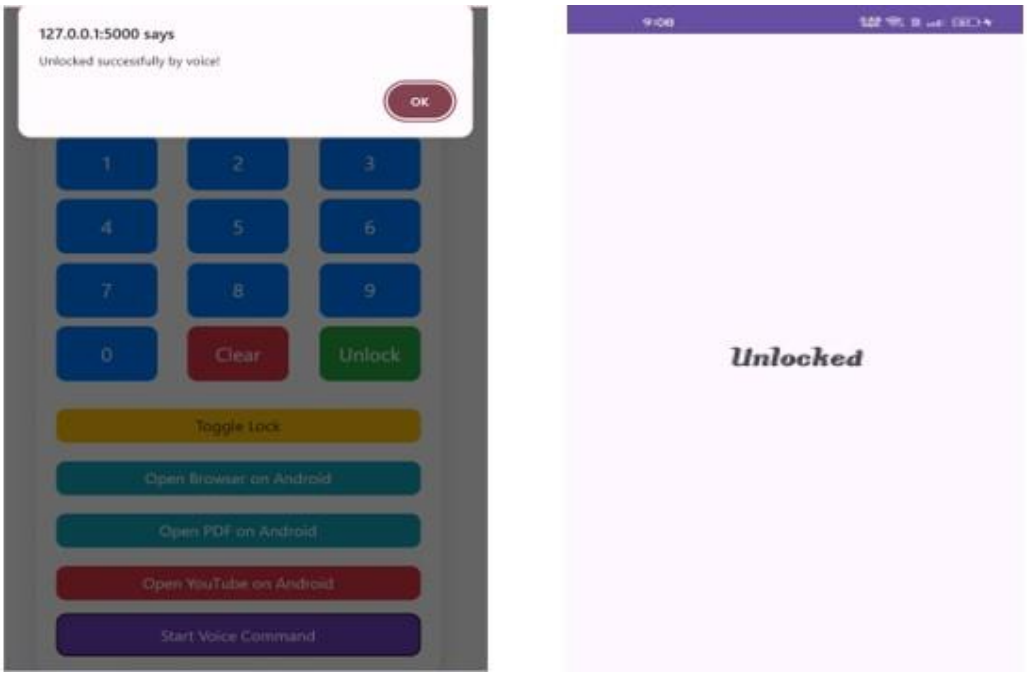


Figure 3: App unlocked by voice

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304133

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

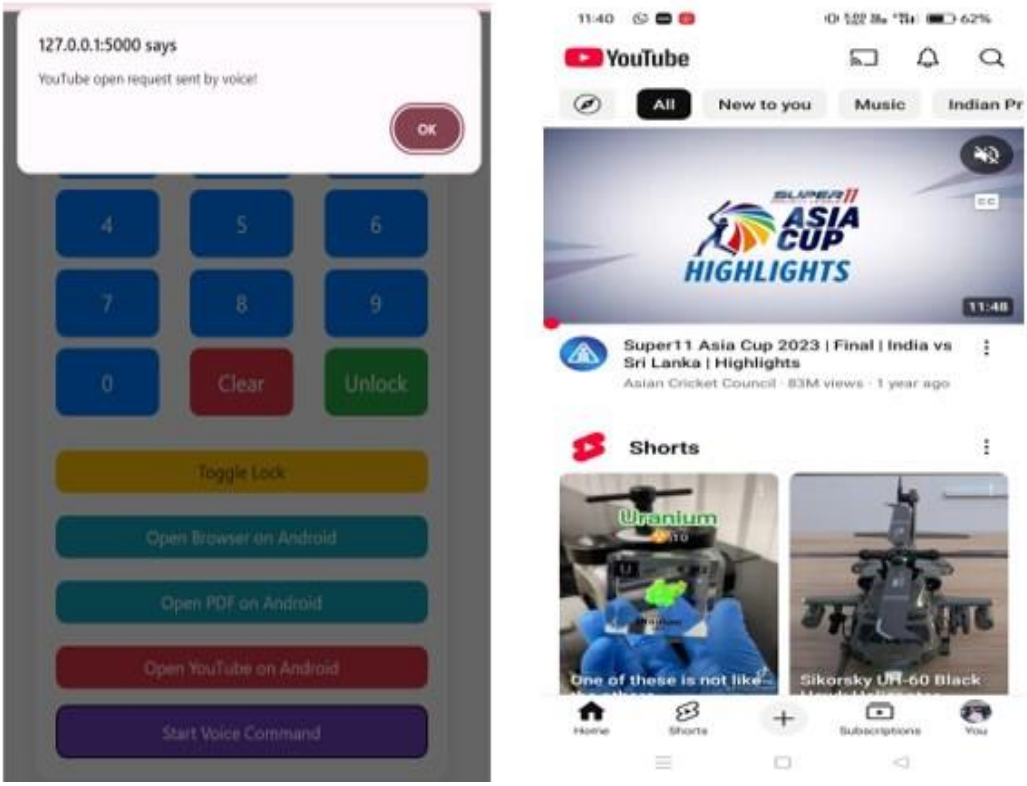


Figure 4: App accessed by voice

VIII. CONCLUSION

This work introduces a novel mobile access control system that integrates voice recognition with PIN and biometric authentication for enhanced security and usability.

FUTURE SCOPE

- Integrate cloud-based speech recognition for improved accuracy.
- Extend support to multiple languages and dialects.
- Conduct real-world testing on diverse user groups.
- Implement continuous authentication for sensitive apps.

REFERENCES

[1] L. R. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," Proceedings of the IEEE, vol. 77, no. 2, pp. 257–286, 1989.
[2] A. Hannun et al., "Deep Speech: Scaling up end-to-end speech recognition," arXiv:1412.5567, 2014.
[3] A. Graves, N. Jaitly, and G. Hinton, "Speech recognition with deep recurrent neural networks," in ICASSP, 2013.
[4] Z. Wu et al., "ASVspoof: The Automatic Speaker Verification Spoofing and Countermeasures Challenge," IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 24, no. 10, pp. 1686–1702, 2015.
[5] S. J. Yang, C. M. Kuo, and Y. L. Chen, "An enhanced multi-factor authentication mechanism for mobile devices," in ICMAN, 2011.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details