Passwordless Authentication System Using Voice Biometrics

Abstract

Traditional password-based authentication systems are vulnerable to attacks such as password theft, brute-force attacks, and phishing. To overcome these limitations, this project implements a Passwordless Authentication System using voice biometrics. The system authenticates users based on their voice characteristics rather than passwords. A Flask-based backend processes voice input, extracts MFCC features, and verifies them against stored voice patterns. The proposed system improves security, usability, and user experience.

Introduction

Authentication is a critical component of modern digital systems. Password-based authentication suffers from security and usability issues. Biometric authentication provides a secure alternative by using unique biological traits. This project focuses on voice biometrics, which is natural, contactless, and user-friendly.

Problem Statement

To design and implement a secure passwordless authentication system that authenticates users using voice biometrics instead of traditional passwords.

Existing System

1. Username and password-based authentication.
2. Vulnerable to hacking and phishing.
3. Users tend to reuse weak passwords.
4. Poor user experience.

Proposed System

1.Passwordless authentication using voice biometrics.
2.Voice is recorded and processed using MFCC.

3.Authentication based on similarity with stored voice features.
4.Improved security and convenience.

System Architecture

Frontend (HTML, CSS, JavaScript)
→ Sends request to backend
Backend (Flask, Python)
→ Records voice → Extracts features → Matches voice → Sends response

Technology Stack

1. **Frontend**: HTML, CSS, JavaScript.
2. **Backend**: Python, Flask.
3. **Libraries**: Librosa, NumPy, SoundDevice.
4. **Tools**: VS Code, GitHub.

Implementation Details

1. Voice is recorded for a fixed duration.
2. MFCC features are extracted using Librosa.
3. Features are compared using Euclidean distance.
4. Authentication succeeds if similarity is within threshold.

Results

- ☐ System successfully authenticates users using voice.
- ☐ Backend responds with success or failure.
- ☐ Password dependency eliminated.

Advantages

1. Enhanced security
2. No password management
3. User-friendly
4. Contactless authentication

Limitations

- Affected by background noise
- Voice changes due to illness
- Requires microphone access

Future Enhancements

- Multi-factor authentication
- Support for face and fingerprint
- Cloud database integration
- Deep learning-based voice model.

Conclusion

The Passwordless Authentication System using Voice Biometrics provides a secure and user-friendly alternative to traditional authentication methods. The system successfully demonstrates voice-based authentication using Python and Flask.