# Voice-Based Authentication System

Jarpula Bhanu Prasad
AI21BTECH11015

Kola Akshitha
AI21BTECH11017

## 1 Introduction

This project presents a secure and intelligent **Voice-Based Authentication System**, leveraging machine learning and modern cryptographic techniques to ensure robust user authentication. The application integrates a **React-based frontend**, a scalable **FastAPI backend**, and AI models for **anti-spoofing** and **voice feature extraction**. It also employs encryption to protect user data and ensures a seamless and secure user experience.

### 1.1 Objective

The project aims to develop a reliable authentication system based on voice biometrics, addressing the increasing need for secure, user-friendly identity verification methods.

### 1.2 Background

Traditional authentication methods, such as passwords, are prone to theft and misuse. Voice biometrics offers a convenient and secure alternative, ensuring authentication through unique vocal characteristics.

### 1.3 Target Audience

- Businesses requiring secure user authentication.
- Applications in banking, healthcare, and enterprise-level security systems.

### 1.4 Scope

The system supports:

1. User registration and login using voice data.
2. Detection of spoofing attempts using a trained AI model.
3. End-to-end encryption for securing voice data.

# 2 Features and Functionality

## 2.1 Key Features

- **User Registration:** Collects voice samples during registration and extracts features for future authentication.
- **Login via Voice:** Matches the user's voice input against registered samples.
- **Anti-Spoofing Detection:** Identifies fake or synthesized voice attempts.
- **Secure Data Storage:** Encrypts voice data before storage.

## 2.2 User Workflow

1. A user registers by providing their email, password, and a voice sample.
2. The system verifies the sample for authenticity.
3. During login, the user's voice is validated against stored features.
4. Spoofing attempts are flagged and denied access.

# 3 System Design and Architecture

## 3.1 System Overview

The application is divided into three components:

1. **Frontend:** React-based, providing an intuitive user interface.
2. **Backend:** FastAPI-powered server handling requests, database interactions, and encryption.
3. **AI Model:** TensorFlow-based anti-spoofing model ensuring the authenticity of voice inputs.

## 3.2 Technologies Used

- **Frontend:** React, Styled-components, React-icons.
- **Backend:** FastAPI, SQLAlchemy, TenSEAL, Librosa.
- **AI Model:** TensorFlow (Anti-spoofing).
- **Version Control:** Git

### 3.3 Challenges Faced

- Ensuring accurate spoof detection.
- Encrypting and decrypting voice features while maintaining performance.

## 4 Implementation Details

### 4.1 Backend

The backend is built using **FastAPI** for rapid development and scalability. Key functionalities include:

- **User Management:** Handled via SQLAlchemy ORM and bcrypt for password hashing.
- **Voice Data Encryption:** Implemented using TenSEAL's CKKS encryption scheme.

### 4.2 AI Model

The anti-spoofing model uses **MFCC features** to identify real and fake voices. It was trained on synthetic and real voice datasets, achieving high accuracy.

### 4.3 Frontend

A React-based frontend interacts with the backend via RESTful APIs. It ensures seamless user experiences through modern UI design.

## 5 Testing

### 5.1 Test Cases

- User registration with valid and invalid inputs.
- Spoof detection with real and synthetic voices.
- Encryption and decryption accuracy.

### 5.2 Performance Metrics

- **Anti-Spoofing Model:** 95% accuracy on test data.

# 6 Results and Achievements

## 6.1 Key Outcomes

- Successfully implemented voice-based authentication.
- Detected spoofing attempts with high accuracy.
- Ensured secure data storage and transfer using encryption.

# 7 Limitations and Future Work

## 7.1 Known Issues

- Performance may degrade with extremely noisy inputs.
- Limited language support for diverse voice samples.

## 7.2 Future Enhancements

- Enhance the anti-spoofing model for diverse datasets.
- Optimize encryption methods for larger voice data.

# 8 Conclusion

This Voice-Based Authentication System combines AI, cryptography, and web technologies to provide a secure and user-friendly authentication solution. The project demonstrates the potential of voice biometrics as a scalable and effective alternative to traditional authentication methods.