Authentication Using Voice Recognition and Timestamp OTP

Neha Nomula, Komareddy Anusha, Neha Panuganti, Niharika Chitumadugula, Satya Sai Charan Pusapati, Srividya Ranganthan.
Advisor: Dr. Shakour Abuzneid
Department of Computer Science & Engineering

Abstract:

This work is related to providing security using authentication. By looking into other research works, we have found many attacks while logging in a system like phishing attack, brute force attack, etc. We came up with a solution which uses voice biometric as a recognition technique and also adding a time stamp one-time password (TOTP) which will help in providing a better authentication during login. Voice recognition technique uses a Bark frequency scale mapped with the input voice signal and made into spectral analysis with cepstral coefficients which is tough to forge, and adding this with TOTP provides stronger security in today's Internet of Things (IOT).

Methodology:

In this project, we have calculated the Bark frequencies, Fourier Transforms, and cepstral coefficients. This algorithm is used for recognition of voice signals. For comparing the voice signals, we have used MATLAB software. For Timestamp OTP, we are using Google Authenticator for TOTP. A random six- digit number is generated when the user tries to log in, which is valid for a time frame of 30 seconds. Once the time frame expires, it automatically generates a new six- digit random number, and it continues until the user authenticates. This process is repeated for 5 minutes. After that, it asks the user to change the trusted device. It computes a one-time password from a shared secret and the current time. It is used in some two-factor authentication systems. It is an example of hash-based message authentication code. It is a combination of secret key with the current time stamp using a cryptographic hash - function to generate a one-time password. A single secret key is used for all authentication sessions must have been shared by server and user device via secure channel ahead of time. Finally, we came up combining both the methodologies, which protects the attacks of phishing, spoofing, forging. If the authentication is not done, then the user could not enter the system.

Figure 1 : Block diagram of Client-server system

Algorithm for TOTP:

$$SHA1(outer\ pad\ +\ SHA1\ (inner\ pad\ +counter))$$

$$new\ number = old\ number\ mod\ 10^6$$

The inner and outer pads are calculated as follows:

$$inner\ pad = seed \oplus 0x36$$

$$outer\ pad = seed \oplus 0x5C$$

Where seed is the input value the system tries to give.

Formula for calculating voice recognition:

$$bark = 13arctan(0.00076f) + 3.5arctan\left(\left(\frac{f}{7500}\right)^2\right)$$

Results:

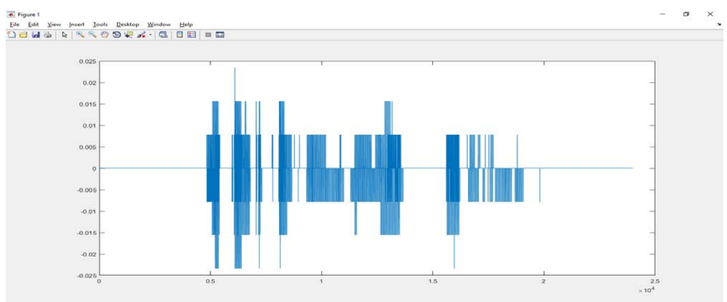

Figure 2: Stored Voice Signal

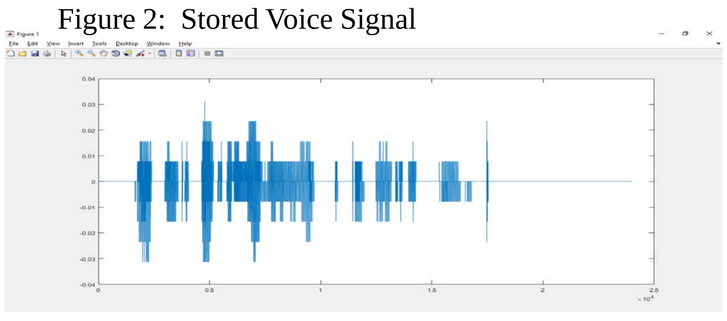

Figure 3. Input Voice Signal

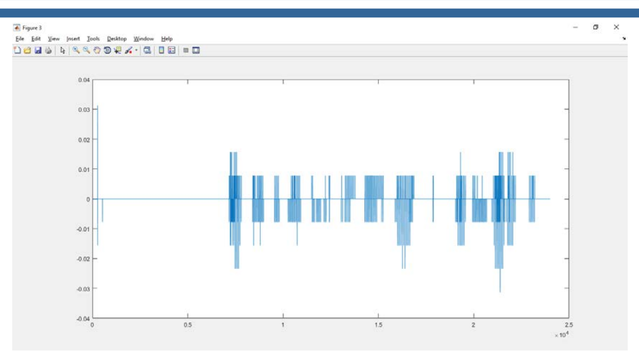

Figure 4. Non- matching Voice Signal

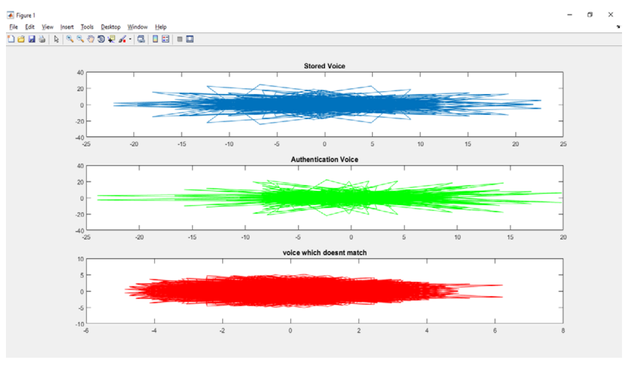

Figure 5:Input Signal Fourier Transform

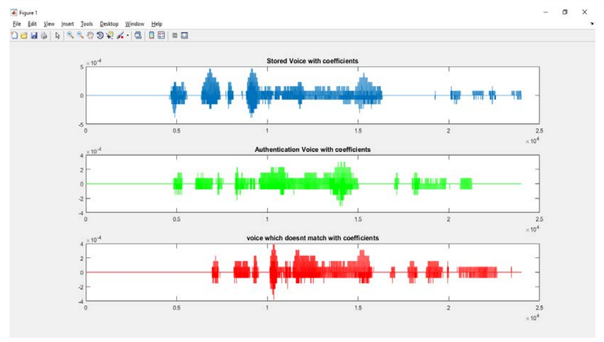

Figure 6. Output Bark Frequency Cepstral Coefficients

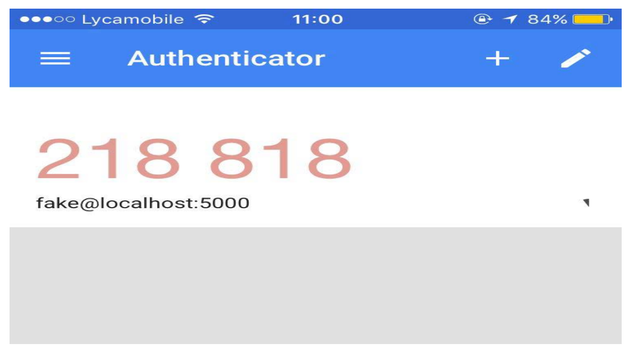

Figure 7. Six-digit token before expiring

Conclusion:

To conclude our project we mainly focused on voice recognition and time stamp OTP. By providing both the authentication techniques, we are trying to provide a more secure login improving the existing technologies. The system can be enhanced with any other biometric technique as sometimes the voice may not match depending on a person's health condition. This method is very much useful for business purposes for getting into the company's personal systems and also can be used for individuals who are handicapped and may not be able to use other biometrics. This project can be implemented for mobile.