Smart Phone Based Authentication



Using Speech Recognition

By:

Jarel Ross, Alexia Jackson, Dazhia Celeste

**Introduction/Abstract**

Smart phone-based authentication is verification of a user’s identity through the use of a personal mobile device as well as one or more methods for secure access. Mobile authentication is sometimes used to authorize either the device itself or as a part of a systematic multiprocessing authentication scheme for logging into a website or location. For example, whenever you log into Google using a new device, they send you a code to your phone to verify that it is you logging in, or your Apple iPhone when they use the two-way authentication factor or simply an SMS text. Why? It is because you are your phone and when I say that, I mean that without your phone, you’re naked, you have nothing. In today’s world, 97% of the working class have personal information ranging from credit cards to social security numbers to everything basically implanted into your cellular device. With the rise of technology comes a higher need for security. Two-way factor authentication using voice recognition will lead the way in regards to security and keeping everything safe. That’s my overall statement. Our mobile phones contain most of our sensitive information such as credit/debit card information, home address, and our email which contains emails about credit card accounts, subscriptions, investments, and pretty much our entire lives. We cannot afford to have issues with mobile authentication. Artificial intelligence was one of my many fascinations in computer science because I was always intrigued on how a machine can understand and interact with a human being. Communication with technological devices and gadgets by voice has become so people and normalized to the point where I wonder why many high profile companies are revealing their services to us now. My rationale for smartphone-based authentication using voice/speech recognition is because my mother was a victim of credit card fraud. Since we live in a world full of hackers and thieves, phone companies have come up with multiple methods for users to access their mobile devices under a secure path. Non-text passwords using codes and numbers, face recognition passwords, and fingerprint access, one-time passwords are some of the way’s companies use smartphone-based authentication. Smartphone based authentication is important and needed because our smartphones store a lot of sensitive data and used to access a lot of different cloud data. Smartphones are often stolen, and it would be highly beneficial to have other security options besides the initial login. It is important to reauthenticate those who have continuously failed to authenticate themselves as the primary user. Mobile-based authentication verifies the user of the system/mobile based on their identity which can be Username and password. mobile can be easily stolen so we required protection against unauthorized access it. Mobile is not too much secure when it is connected to any network so there, we need to verify the sender's identity. Mobile-based authentication can save our personal data and information it protects it from data leak. Many companies need extra security beyond a simple ID and password but additional security measures such as facial recognition and voice verification.

### **Motivation**

Artificial intelligence has always been a fascination to computer science students because we are always intrigued on how a machine can understand and interact with a human being. Communication with technological devices and gadgets by voice has become so people and normalized to the point where I wonder why many high profile companies are revealing their services to us now. As students who are learning to program and operate machine learning and AI, we discover a world of possibilities. We are able to see from outside the box the type of inspirational and educational purposes machine learning and AI can produce. But, since computer science students study to actually understand how and why machine learning and AI were created and how they operate is a different type of learning. Not only can we create and design whatever our imaginations can create with machine learning, but we see the background work that machine learning provides. Machine Learning and AI is vastly different and requires deep learning which can result in amazing inventions. AI and Machine Learning can immensely impact different aspects of businesses like the tech world, financial world, healthcare and many more. AI and Machine Learning is used everywhere technology is used, and said to be versatile and the skill of the century to learn and execute.

### **Findings and Observations**

Many banks and establishments are switching to voice recognition on their mobile app as a secure form of logging into your account to view information. Voice recognition, a form of biometric software, is a more secure form of banking protection because our voices are unique. Each voice has a set of around 100 characteristics. Half of those are physical characteristics such as the shape of the mouth and throat as well as behavioral characteristics such as sound and words used. Once an individual’s unique voice print has been captured, further banking calls will be matched against it. The system cannot be cheated by mimicking a voice, and will recognize the voice even if you are quiet,have a cold or are in a loud office. There are many forms of authentication but voice recognition is one of the best forms when perfected. No two voices are the same. Because of the uniqueness of our voice, this gives businesses and corporations a better and more secure way to tend to their customers. It is more time efficient, as well as secure. Many prefer the voice recognition authentication because it can detect your unique voice print even with loud background noise, being sick or any other obstacles. It is impossible to trick the system into thinking you are someone else which provides a very tight lock on the security aspect of this authentication. Overall, businesses and corporations can utilize this authentication to provide better and secure customer service. Some of the best software to use to execute speech recognition are Dragon, Dragon Anywhere, G Suite, Braina Pro and Windows 10.

### **How Authentication Works**

Initially how two-way authentication requires the customer to correctly insert two to three different forms of login and password. The user will first gain access to their terminal, which in our case is a smartphone, and will be asked to insert their login name and password. Ways to determine authentication is speech, finerger print, Face ID and character passwords. If the login name and password is incorrect, the system will notify the user that it is invaild and needs to be inserted again. Once the correct login method is inserted within the terminal, then there is another form of security to go through. Earlier I listed multiple security ways to correctly obtain access within the user’s terminal. You can do Face ID and fingerprint, or fingerprint and speech authentication. Once the machine is not available to send verification codes to the trusted device, the machine will show an error message. Once the machine is able to send verification codes, the user will then be successfully logged into the terminal, or smartphone. The user’s settings are then displayed and once the user logs out, the system will start again. In our paper and project we focus on the speech and voice authentication of a smartphone. A few speech recognition software that is top tier is Siri and Cortna.

### **Future Plans**

We are still some good distance from understanding the genuine capability of speech recognition technology. This applies both to the modern day teachings as well as innovations of technology and to its combination into our lives. The current speech recognition technology can translate and interpret speech very fluently already, yet they are not the conversational interfaces that the A.I. developers need them to be. Additionally, speech recognition remains restricted to a small number of products and features. The pace of progress, contrasted with the soonest attacks into speech recognition along with a.i has exceeded its expectations The future of voice recognition is looking bright. Given its current usage both in the home and on the move, it seems as though this technology will only get bigger over the next few years.

References

<https://searchsecurity.techtarget.com/definition/mobile-authentication>

<https://www.aware.com/voice-authentication/>

<https://voice.mozilla.org/en/datasets>

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.678.5713&rep=rep1&type=pdf>

<https://www.hindawi.com/journals/misy/2018/2649598/>

<https://www.nuance.com/omni-channel-customer-engagement/security/identification-and-verification.html>

<https://medium.com/@Alibaba_Cloud/voiceprint-recognition-system-not-just-a-powerful-authentication-tool-6b3702b5c5a>

<https://www.neurotechnology.com/verispeak.html>

<https://discourse.mozilla.org/c/voice>