INTRODUCTION OF BIOMETRIC AUTHENTICATION IN BANKING DOMAIN

[1]Himanshu Joshi, [1]Prasanna Desale, [3]Janhavi Danage

[1]BE Third Year ,[1]Information Technology,
[2]BE Second Year ,[1]Computer Science ,
[3]BE Second Year ,[1]Computer Science,

[1]International Institute of Information Technology (Affiliated to SPPU), Pune, Maharashtra India
[2]International Institute of Information Technology (Affiliated to SPPU), Pune, Maharashtra India
[3]International Institute of Information Technology (Affiliated to SPPU), Pune, Maharashtra India

Abstract: The biometric systems are increasingly used in our society. In this paper, we will address on one of these system: the biometric authentication using voice. Starting from the general background of the existing biometric systems we will proceed to analyze each step of a voice authentication system. We will describe the principles of application and at the same time the main problems related to this system, like security and reliability of this kind of system. Like every other authentication system, this one can be target of threats and attacks to its security and we will try to explain the main ones. Therefore we will give an overview about how the system is used in practice

KEY WORD : AUTHENTICATION

I.INTRODUCTION

Information security is concerned with the assurance of confidentiality, integrity and availability of information in all forms. There are many tools and techniques that can support the management of information security. But system based on biometric has evolved to support some aspects of information security. Biometric authentication supports the facet of identification, authentication and non-repudiation in information security. Biometric authentication has grown in popularity as a way to provide personal identification. Person's identification is crucially significant in many application and the hike in credit card fraud and identity theft in recent years indicate that this is an issue of major concern in wider society. Individual passwords, pin identification or even token based arrangement all have deficiencies that restrict their applicability in a widely-networked society. Biometric is used to identify the identity of an input sample when compared to a template, used in cases to identify specific people by certain characteristics. Possession based: using one specific "token" such as a security tag or a card and knowledge-based: the use of a code or password. Standard validation systems often use multiple inputs of samples for sufficient validation, such as particular characteristics of the sample. This intends to enhance security as multiple different samples are required such as security tags and codes and sample dimensions. So, the advantage claimed by biometric authentication is that they can establish an unbreakable one-to-one correspondence between an individual and a piece of data. It is possible to verify a user through three different approaches: something that he knows, like a password or a PIN, something that he has, like a key, or something that he is, biometric characteristics. The biometric systems are more simple because since the user does not have to remember the password or to be afraid of losing it, "but they are not secret. You leave your fingerprints on everything you touch, and your iris patterns can be observed anywhere you look." The development of the biometric systems is tightly coupled to the IT technologies, and this is the reason why today they are very used. There is a large number of biometric methods: fingerprint, iris, signature, gait, hand geometry, voice, retinal pattern, etc.. It is possible to distinguish these characteristics into main fields: - physiological: fingerprint, iris, hand, face; - behavioral: voice, signature, gait. According to their dissimilar quality they can be used in different environments. In this paper, we will examine the biometric authentication using voice, specifying first of all how it works, the problems connected to its usage (like legal and privacy issues) and ultimately, the attack risks that such a system may suffer. After we will give an overview of how a system is used in practice work.

- **EXPERIMENTAL STUDY**

A. SYSTEM PARTS

THE SMART-LOCK-SYSTEM CONSISTS MAINLY OF THREE MAJOR PARTS.

- Sensor : The sensor collects biometric data from the subject to be recognized.

- Matcher : It compares presented data to reference data in order to make a recognition decision.
- Reference Database: Here previously enrolled subjects' biometric data are held.
- Action: Here the system recognition decision is revealed and actions are undertaken based of that decision.

1.2 System Operations

The system should be connected to the home network (LAN) via a UTP cable or Wireless Connection via Router . Also, the user must be Connected to same network in order to control the system. A brief system

architecture is shown in the Figure 1.

Sample operation of a general biometric system. The two basic operations performed by a general biometric system are the capture and storage of enrollment (reference) biometric samples and the capture of new biometric samples and their comparison with corresponding reference samples (matching). This figure depicts the operation of a generic biometric system although some systems will differ in their particulars.

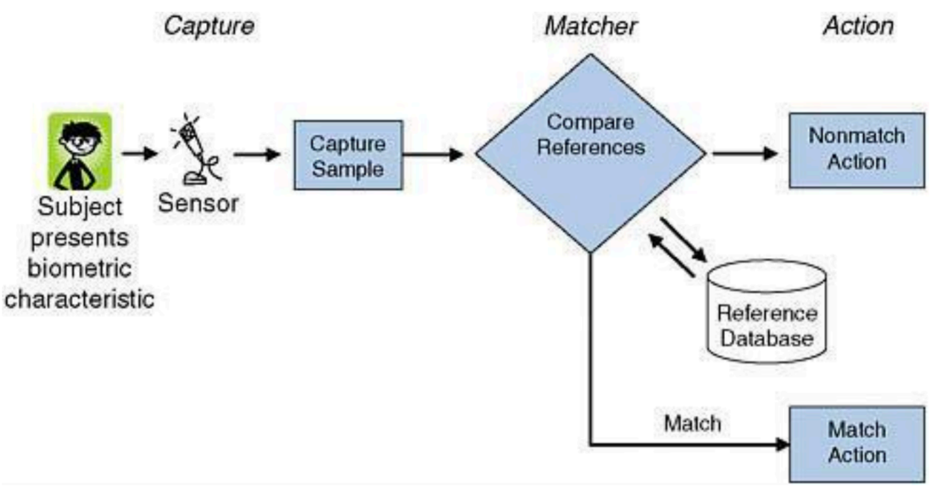


Figure 1. Voice Authentication Architecture

Requirements For Operation

Voice activity detection (VAD), also known as speech activity detection or speechdetection, is a technique used in speech processing in which the presence or absence of human speech is detected. The main uses of VAD are in speech coding and speech recognition.

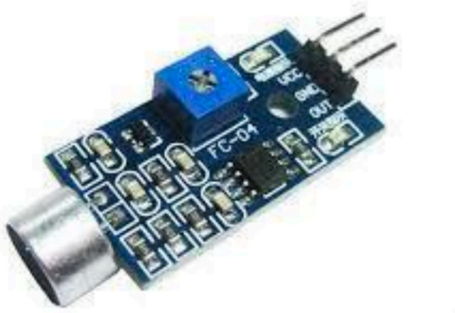


Figure 2. Voice Sensor Module

This Sound Sensor Module can detect the size of the voice. With holes for easy installing and connecting to Arduino.

2.1Microphone and Mic

A microphone, sometimes denoted to as a mic or mike, is a sensor or transducer which is used to convert the sound into an electrical signal. The applications of microphone mainly involve tape recorders, radios, broadcasting of TVs, telephones. In a capacitor microphone also known as condenser microphone, the diaphragm acts as one terminal of the capacitor, and the vibration changes in the distance between the two terminals. To extract an audio o/p from the transducer, there are two methods known as DC biased and HF or RF condenser microphones.

2.2 Principle

The basic principle of voice recognition involves the fact that speech or words spoken by any human being cause vibrations in air, known as sound waves. These continuous or analog waves are digitized and processed and then decoded to appropriate words and then appropriate sentences.

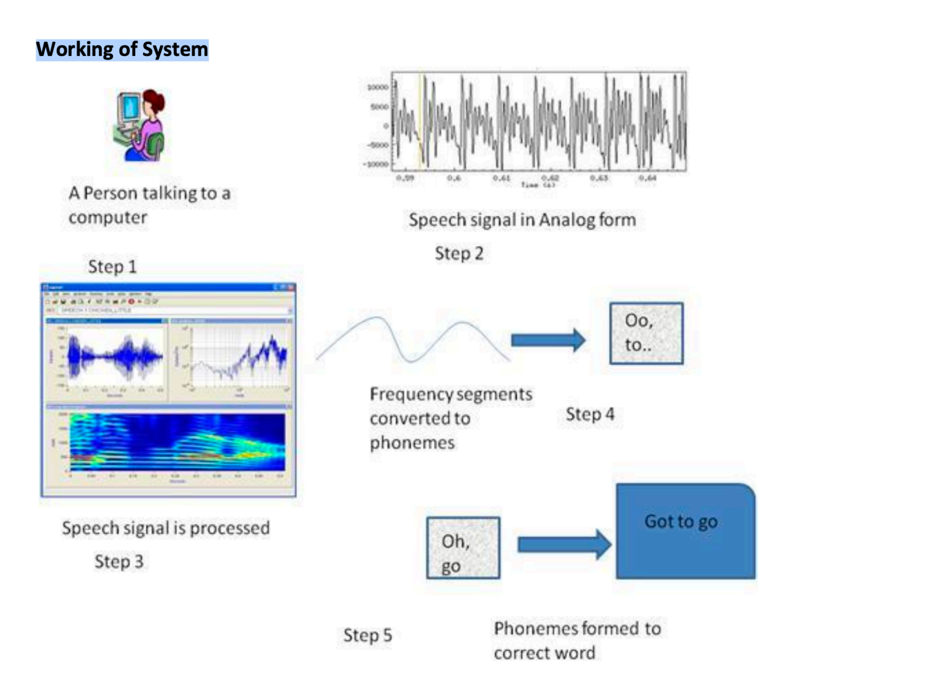

Working of System
A Person talking to a computer
Step 1
Speech signal in Analog form
Step 2
Speech signal is processed
Step 3
Frequency segments converted to phonemes
Oo, to..
Step 4
Oh, go
Got to go
Step 5
Phonemes formed to correct word

Fig 3. Working of System

2.3 Working System

- A speech can be seen as an acoustic waveform, i.e. signal carrying message information. A normal human being with the limited rate of motion of his/her articulators (speech organs) can produce speech at a average rate of 10 sounds per second. The average information rate is about 50-60 bits/second. It means actually only 50 bits/second of information is required in the speech signal. This acoustic waveform is converted to analog electrical signals by the microphone. The Analog to Digital converter converts this analog signal to digital samples by taking precise measurements of the wave at discrete intervals.

- The digitized signal consists of a stream of periodic signals sampled at 16000 times per second and is not suitable to carry out actual speech recognition process as the pattern cannot be easily located. To extract the actual information, the signal in time domain is converted to signal in frequency domain. This is done by the Digital Signal Processor using FFT technique. In the digital signal, the component after every 1/100th of a second is analyzed and the frequency spectrum for each such component is computed. In other words the digitized signal is segmented into small parts of frequency amplitudes.

- Each segment or the frequency graph represents the different sounds made by human beings. The computer performs the matching of the unknown segments with the stored phonetics of the particular language. This pattern matching is done in 3 ways:

I. Methodologies

- Using a Acoustic phonetic approach: In the Acoustic phonetic approach, generally the Hidden Markov Model is used. This model develops a non deterministic probability model for the speech recognition. This model consists of two variables – the hidden states of the phonemes stored in the computer memory and the visible frequency segment of the digital signal. Each phoneme has its own probability and the segment is matched with the phoneme according to the probability and the matched phonemes are then collected together to form the correct words according to the stored grammar rules of the language.

- Using a pattern recognition approach: In the pattern recognition approach, the system is trained with a particular speech pattern for any language and the unknown speech pattern is compared with the reference speech pattern by determining the distance between the signals using time warping technique.

- Using Artificial intelligence: The Artificial Intelligence approach is based on the utilization of basic knowledge sources such as the knowledge of sounds spoken on basis of spectral measurements, knowledge of proper meaningful and syntactical words.

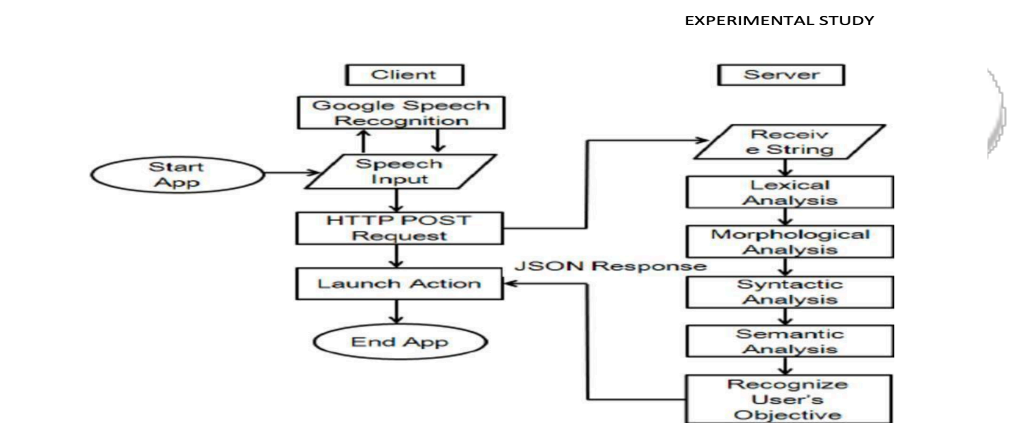


Figure 4. Flowchart of VRT

3.1 Database and Tool for speech Recognition

- **SpeechRecognition**
  There are many speech databases are available to carry out research in automatic speech recognition in American and European languages. Some of the commonly used databases are TIMIT, GlobalPhone, Aurora, Wall Street Journal, AN4, TI Digits, TI46, NTIMIT, RM1, RM2, Switch Board etc. The TIMIT corpus of read speech is designed to provide speech data for acoustic-phonetic studies and for the development and evaluation of automatic speech recognition systems. The DARPA TIMIT acoustic-phonetic continuous speech corpus (TIMIT - Texas Instruments and Massachusetts Institute of Technology), contains recordings of phonetically-balanced prompted English speech. It was recorded using a Sennheiser close-talking microphone at 16 kHz rate with 16 bit sample resolution [22-23]. TIMIT contains a total of 6300 sentences, consisting of 10 sentences spoken by each of 630 speakers from 8 major dialect regions of the United States. All sentences were manually segmented at the phone level. Global Phone, a multilingual database of high-quality read speech with corresponding transcriptions and pronunciation dictionaries in 20 languages. Global Phone [24] was designed to be uniform across languages with respect to the amount of data, speech quality, the collection scenario, the transcription and phone set conventions. With more than 400 hours of transcribed audio data from more than 2000 native speakers Global Phone supplies an excellent basis for research in the areas of multilingual speech recognition, rapid deployment of speech processing systems to yet unsupported languages, language

identification tasks, speaker recognition in multiple languages, multilingual speech synthesis, as well as monolingual speech recognition in a large variety of languages.

3.2 Algorithm

Speech Recognition System on Windows 7

- I would like to recommend the following steps for any person using Windows 7 for the speech Recognition system Open Control Panel from the start menu or by clicking on the icon.

- Select Ease of Access and then click Speech Recognition.

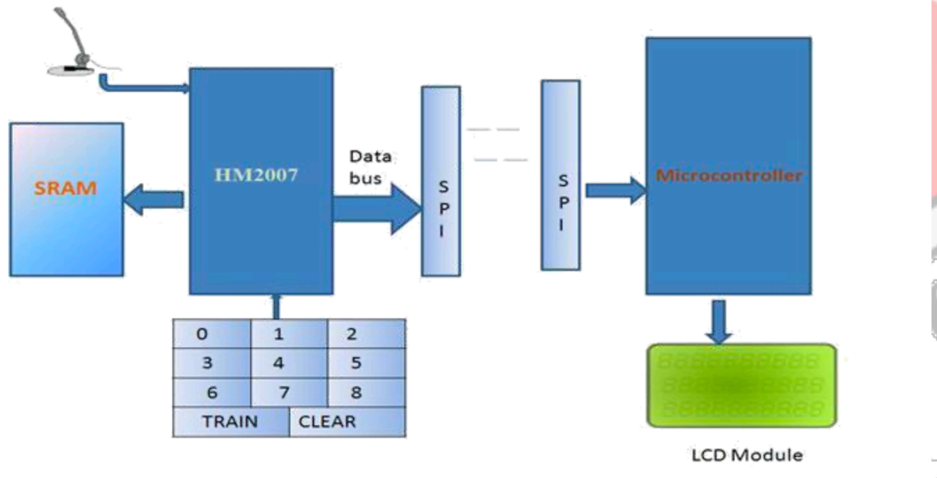
- Next click set up microphone and select desktop microphone from the available options. Next take the speech tutorial and follow the given instructions.

- After that, train your computer for better options so that the computer stores a definite pattern of your speech signal. This is done by clicking on 'train your computer to better understand you' option and then follows the instructions.

- Now start the speech recognition icon and start dictating your speech to the computer. You can also add your own words to the computer dictionary.

3.3 Practical Speech Recognition Systems: Using HM2007

A practical speech recognition System can be constructed using Speech Recognition IC HM2007. The HM2007 is a 48 pin IC which provides speech recognition function. It works in two modes: Manual mode or CPU mode. In both modes, the IC is first trained to recognize words by the user saying each word for corresponding number pressed on the key. The IC stores each word signal in the memory location corresponding to the word. The data output from the IC is interfaced to the Microcontroller from where it is displayed on the LCD.



HM2007 Structure

•Normally we use manual mode for HM2007 operation.

- The HM2007 consists of a RDY pin which is an active low pin indicating the IC is ready for training purpose. The Voice input will be given through a microphone connected to the MICIN pin of the IC.

- The IC is interfaced with a keypad which is used to provide number input corresponding to each word. The IC works in two functions – Clear and Train. When Train key is pressed on the keyboard, the IC begins its training process.

- The user presses a number key before pressing the 'Train' function key and says the required word to the microphone.

- The IC sends a high signal to ME (Memory Enable) pin which is connected to corresponding ME pin of SRAM. The 8 bit data signal corresponding to the number pressed is stored in the SRAM (external RAM) through the external bus.

- After the voice input is detected, RDY pin is at logic high and the IC comes to the recognition state, where it starts the recognition process.

- The result of the process is given through the data bus with the DEN (Data Enable) pin high.

- The 8 bit data can be then given to the Microcontroller through a series Interface processor or first latched using latch IC 74HC573.

- The Microcontroller is interfaced with an LCD and is programmed such that the corresponding word is displayed on the display.

The only precaution that needs to be taken is to not use homonyms (words with similar sound) and also to take care of the excitation in voice.

4 Security

How does VAUB perform against hacks and the latest security bypassing techniques?

- The recognition data is stored internally by the bank, and in order to ensure that recorded voice clips cannot be used to gain unauthorized access, the system uses a string of diffrant questions that are difficult to “spoof”. More Privacy by Appropriate Security Measures

- Creation of Voice Authentication Technique which Resistant to Voice Imitation Attacks

- Strong Electromagnetic Sensor Should Prevent VIA

- Alternate Authentication.

- **Talking About Risk**

  While more people are readily introducing these devices into both home and business settings, experts warn of the risks and challenges associated with voice technology. “The addition of voice absolutely increases the risk level for technology users,” said Nathan Wenzler, chief security strategist at AsTech Consulting, a cyberrisk management firm. “When you add more features to a device, you are also adding complexity and more code and, as a result, you are introducing more avenues for people to hack into the device. It’s a major risk component.”

  “The minute you have microphones in people’s offices, you are creating a situation where other people will want to listen in.”

  Most devices that employ voice-response technology are internet of things devices and, like many data-collecting devices in this nascent category, manufacturers often do not embed adequate security measures into them. “It can be very easy to break into voice-enabled IoT devices and compromise them, and that opens up a lot of problems,” he said.

  One such concern is the vulnerability of any device that uses voice as a biometric identification factor. “I can trick the device into thinking I am you or I can intercept your voice and then use your voice print for other purposes,” Wenzler said. Your voice is essentially a password, but since you cannot change or alter it easily, once compromised, its effectiveness for security disappears.

  Just as the quality of voice recognition and verification technology has improved, so has the ability to spoof or mimic someone else’s voice for nefarious purposes, according to Dr.

  Alexander Rudnicky, professor in the Language Technologies Institute at Carnegie Mellon University’s School of Computer Science. This can result in serious misuse and fraud in the form of “replay attacks,” where a voice is replicated and then replayed to allow access to financial accounts, work facilities or virtual assistants.

Voice-enabled technology also raises serious privacy concerns. “Many voice-enabled technologies have always-on microphones and are listening to pretty much everything you say,” said Matthew D. Green, an assistant professor of computer science at John Hopkins University’s Information Security Institute. Although these devices are usually waiting to hear a “wake word” that activates them to listen and respond to a voice command, there is still a possibility that voice data can be exposed. “This definitely creates a privacy risk in corporate environments where your phone may be activated in error and what you thought was a private conversation is sent to Google in the cloud,” he said.

Should hackers then break into the devices or the cloud systems where the data is stored, they could access these private conversations. “The minute you have microphones in people’s offices, you are creating a situation where other people will want to listen in,” Green said. Businesses with voice data that must be protected from competitors’ prying ears should especially be thinking about these types of risks.

Many companies are sensitive to these concerns and offer customers the option to disable voice data collection or delete such data. “Customers can turn any data capture off, in which case we toss the data,” said Michael Picheny, senior manager at the IBM TJ Watson Research Center, of IBM’s policy. In the case of the Amazon Echo device, customers have the option to go through the Amazon website to delete the questions they have asked Alexa, though the company advises that doing so may inhibit the quality of service.

Earlier this year, these privacy issues came to light when prosecutors in Arkansas sought voice recordings collected by an Echo device as part of a murder investigation. Amazon initially turned down the request for the data, saying in a statement, “Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course.” Amazon eventually released the data when the defendant expressed a willingness to do so, but the case is likely only the first of many such conflicts to come between individuals, providers of voice- enabled technology and the courts over privacy rights.

5 **Advantage**

1. INCREASED SECURITY, DECREASED FRAUD

The growing number of fraud attacks across industries has increased the need for strong, multi- factor authentication. Unlike PINs and security questions, which can be more easily compromised, voice biometrics ensures that the person calling is indeed who they say they are. Research has found that 10-25% of users – almost all of whom are legitimate – fail to answer security questions correctly when calling in. By reducing the risk of social engineering that often occurs with agents, voice biometrics is also much less susceptible to fraud, making it an ideal method for validating callers in your contact center.

2. IMPROVED CUSTOMER EXPERIENCE

A more commonly overlooked benefit of voice authentication solutions is that they actually hold the potential to significantly improve customer experiences. With voice biometrics products, callers no longer need to provide passcodes or PINs or provide answers to challenge questions in order to verify their identity. This makes voice biometrics ideal for various omnichannel and multichannel deployments, because once a customer is enrolled, his or her voiceprint can be leveraged across all of your company’s support channels. This seamless experience not only makes the process easier and more efficient for your customer, but it also leads to improved CSAT, NPS, and Customer Effort Scores, as highlighted by recent Forrester research. In fact, it has been found that voice biometrics can reduce the time it takes to verify a caller’s identity from anywhere from 10 seconds to several minutes, depending on the reason for the call. This offers the ability to dramatically improve not only call personalization, but also customer experiences.

3. REDUCED COSTS

Research has found that voice biometrics solutions can save millions of dollars in agent time by reducing the steps and time involved in the verification process by as much as 70-80%. In addition, companies are – on average – able to reduce Average Handle Time by 30+ seconds per call when using voice biometrics for authentication. This translates not only to increased efficiency in your security process, but also tremendous cost savings associated with the decreased time your agents need to spend authenticating customers.

6 **Disadvantage**

- Environment and usage can affect measurements Systems are not 100% accurate.
- Require integration and/or additional hardware Cannot be reset once compromised
- Biometric devices are costly.
- Educational Factor .
- External factor affection.
- Too much hype and misconception .
- Data Security Measures.

7 **Conclusion**

Currently the biometric seems to be the natural evolution of the traditional systems resulting from technologies improvement. Certainly the voice is one of the more studied technologies. The traditional access techniques have a series of problems, they can be lost, stolen or lent in an unauthorized way. Moreover they do not control the effective identity of the customer and need that the user remembers codes or password. The biometric key is generated from the personal characteristics of the individual, therefore is not subject to the problems listed before. However there are others problems. For example the decision is probabilistic, it does not indicates an absolute certainty, it expresses only likeness: a malfunctioning microphone or a cold could distort the result. Another difficulty is that a voice can be imitated. We believe that a reliable system should be able to understand which part of the voice signal is not possible to imitate in order to use it as a key point during the authentication phase, but we don’t know how it is possible in realistic applications. The voice recognition is a field in which numerous researches and studies are possible, and it has all presuppositions needed to be an important component in the future security systems.

8 **Reference**

- [1] "Biometric and Banking ". Retrieved 2014, website : http://www.biometricupdate.com/wp-content/uploads/2014/12/Biometrics-and-Banking- Special-Report-2014.pdf
- [2] M.Manzutti,C.Nardini, “Biometric Using Voice ”, TDD03 projects , 2006
- [3] X. Lv and L. Xu, "Biometric Authentication A Review ," International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009
- [4] Chih-Chung Lu and Shau-Yin Tseng, " VocalPasswordTM : voice biometrics authentication.," NUAN–CS–2340–01–B, May 12 2014