International Journal of Advance Research and Innovation
Vol. 4(2), Apr-Jun 2017, pp. 49-51
Doi: 10.51976/ijari.421608
www.gla.ac.in/journals/ijari

Article Info
Received: 20 Jan 2016 | Revised Submission: 10 Feb 2016 | Accepted: 28 Feb 2016 | Available Online: 15 Mar 2016

Securing Email Using Voice Recognition

*Imtiyazul Haq**

ABSTRACT

We are living in the age of digitization. Everything is going to be digitized in next few years. Hence we are becoming more dependent on technologies like email, where we keep some necessary information viz; business information, financial information and personal information etc. Thus it becomes necessary to keep this information more and more secure from the intruders that are continuously targeting to our email for collecting confidential information. It is easy to Hackers because of email spoofing, shoulder surfing and man in middle attacks. So in this paper, I proposed a new approach, using two layer authentication i.e. knowledge based (username and password) authentication together with Biometric based (Voice based)authentication to overcome the problem of existing system.

Keywords: *Shoulder Surfing; Email Spoofing; Man in Middle Attack; Biometric Based Authentication*.

1.0 Introduction

As the technology growing day by day the chances of hacking of one's account also rapidly increases. Hackers are trying frequently to collect confidential information that is related to our business or finance. They are trying number of attack like Brute force attack, shoulder surfing [1] etc. Email is currently the most widely used communication system in daily life. The main reason of using email is probably the convenience and speed provided by it with which it can be transmitted. Many important information like bank statements, business secrets, is being exchanged through emails. So the email keeps extra sensitive information.

Authentication is a very important part of any type of communication, it enables only the legitimate user to enter. So it is the first step for securing email system. Currently we are using only knowledge based authentication (user name and password), which is less secure because of one layer authentication. So in our approach we are using two layer authentication i.e. second layer is biometric based authentication (Voice recognition) with knowledge based authentication system.

1.1. Biometric authentication

Biometric is a technique generally used for authentication purpose. Biometric technology uses Biometric recognition algorithm [2].

Biometric technique can be defined in two categories i.e. Physiological based technique in which the physiological characteristics of a person are collected such as facial analysis, fingerprint, hand geometry, retinal analysis and DNA etc. for verification purpose and another technique is Behavior based techniques includes signature, key-stroke, voice analysis and measure behavioral characteristics.

There are two phases of Biometric based recognition system: identification phase and authentication phase. In identification phase the system identifies a person searching from database of enrolled for a match and in authentication phase the system verifies a person's claim identity from his earlier enrolled pattern.

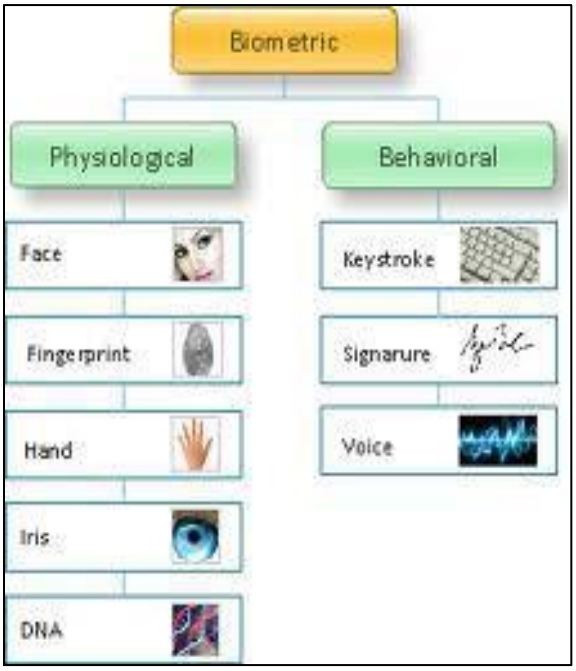
1.2. Drawbacks of existing system

- The current email system is less secure because of shoulder surfing, email spoofing and man in middle attack.

**Department of Computer Science, Invertis University, Bareilly, Uttar Pradesh, India*
(E-mail: idealimtiyaz@gmail.com)

- High vulnerabilities, one way authentication.

Fig 1: A Biometric Based Recognition [3]



2.0 Related Work

The number of works have been completed in the field of biometric based authentication. 'Ahmed obied' proposed a new approach as an email client called SEFR [4]. He used fingerprint together with the knowledge based (username and password) authentication. The idea was to enroll the fingerprint of a user for login purpose. For registration phase the user have to provide the path of his fingerprint. When a user provides his username and password, SEFR attempts to connect via a secure tunnel to Gmail's POP and SMTP servers.

3.0 Proposed Work

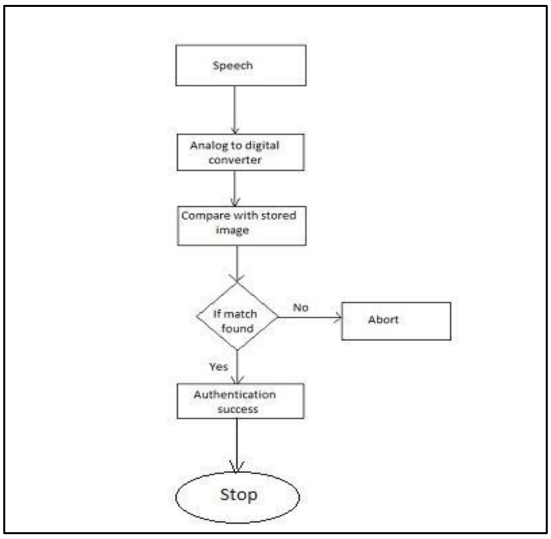
Our approach is implemented using an email client and is designed and implemented on a T2400processor running on Windows XP. Visual Studio is used for IDE (Integrated Development Environment). The main idea is to enroll the voice templates providing by the user. Two test email accounts are created to send and receive email. The user is required to provide the email account information (username and password) together with the path of their voice template, where the voice template is stored. Once the registration phase completed successfully, the user can login.

3.1. Components and design

In this phase, database, voice template and enroller are required. A database is required to store the user's email-account information (username and password), the user's voice template and the hash values of email- sent, so here MYSQL server is used. The user can use mic of laptop or other similar device to record his voice. Enroller play an important role in the registration phase, user have to provide the enroller with their email account information (username and password) and the path of their recorded voice template.

When a user provides his username and password to login to his account, the email client tries to connect via a secure tunnel. The email client ask to provide that path of voice template that has been provided at the time of enrollment. If both the voice templates matches successfully, the user is allowed to send or receive email. In our approach Secure- Hash Algorithm-1 (SHA-1) [5] is used to hash the value of password and voice template. The user want to check if-their email account information and voice template have been already registered or not. In the enrollment phase the enroller takes the username and password and check if a voice template has been already registered if so, then the enroller downloads the voice template and display it to user. If a user want to register using an account that already exists then this email client display an error message.

Fig 2: Voice Based Recognition



3.2. Advantages of proposed approach

- Non-intrusive. High social acceptability.
- Provides two layer enhanced authentication.
- The proposed system is much secure because ones gets the email account information i.e. username and password, it is hard to forge voice template from the user's computer.

4.0 Conclusion

Public key cryptography have been used for many years to protect email system via encryption and digital signature. But due to technical, social and usability issues it becomes less secure. So we presented an approach for enhancement of email security.

In our approach we used two layer of authentication i.e. voice template and knowledge based authentication. This will help from attacks like shoulder surfing, man in middle attack and email spoofing.

References

[1] Viresh Chapte, Yogesh Mali, Grid based authentication system, International Journal of Advance Re-search in Computer Science and Management Studies, 2(10), 2014

[2] Biometric recognition algorithm, https://en.wikipedia.org/wiki/Biometrics.

[3] Smita S. Mudholkar, Pradnya M. Shende, Milind V. Sarode, Biometric authentication technique for Intrusion-detection systems using fingerprint recognition, International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), 2(1), 2012

[4] Secure Email with Fingerprint Recognitionobieda@cpsc.ucalgary.ca and http: //www.cpsc.ucalgary.ca/obieda

[5] Secure Hash Algorithm (SHA-1), William Stallings―Cryptography and Network Security‖, 3rd Edition.