A Survey on Cloud Security: Select Your Security Mechanism

[1]Mr. Kati Anil, [2]Mr. K. Santhosh Kumar, [3]Mr. P. Srinivas Rao
[1,2]Assistant Professor, [3]Associate Professor.
Department of Computer Science & Engineering.
Jayamukhi Institute of Technological Sciences, Narsampet, Warangal, Telangana, India

Abstract:

Security refers to all the measures that are taken to protect a place, or to ensure that only people with permission enter it or leave it and limiting access to key network resources by keeping the resources behind a locked door and protected from natural and human-made disasters. Here we have different types of security techniques in that you can select, and then you can proceed through that network communication. We have different type's security techniques to protect the information and also our credentials. In this paper we will discuss some of the select security techniques. There are different types of select security techniques are existed, such as Human Authentication Techniques and Computer Authentication Techniques. The Human Authentication Techniques are Knowledge Base, Token Based, Biometrics and Recognition Based. The Computer Authentication Techniques Textual Passwords Graphical Passwords Biometric schemes.

Keywords: Select Security, Authentication, Biometrics, Text and Graphics, Poroscopy, Ear lobe, Nose tip, Recognition System, OTP, Recognition.

I. Introduction

Select Your Security is a new mechanism for securing our data from unauthorized objects. Here we have different techniques are existing, by using this simply select your option go through that your platform. If any hacker wants to attack our network it is not easy task to do. Moreover hacker doesn't know about which type technique they are used by user. So we can protect our credentials from unknown persons.

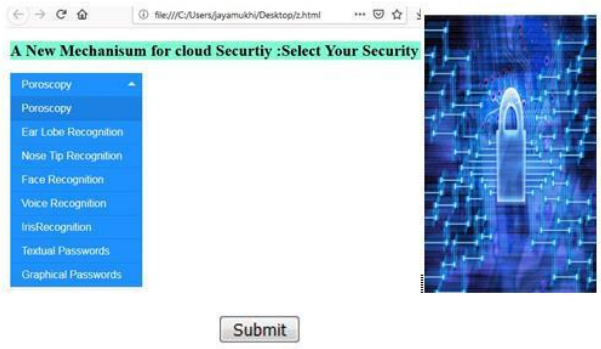

Figure 1: selection security technique

Authentication is a process of validating who you are to whom you claimed to be, or in other words a process of identifying an individual, usually based on a username and password. Currently what we have in the field, are the following set of techniques:

Human Authentication Techniques are as follows:

1. Knowledge Base.
2. Token Based.
3. Biometrics.

A. Poroscopy.
B. Ear lobe Recognition.
C. Nose tip Recognition.

Computer Authentication Techniques are as follows:

1. Textual Passwords
2. Graphical Password

I. Human Authentication Techniques

1. Knowledge Base Technique: In this knowledge base technique, we have the remember the password and some other security credentials. It means that consumer or the person have the memory power to know about his details. And also don't share the details to unauthorized person

2. Token Based Technique: Token based technique is like communication process between client and server or between knowing persons. In this Technique each and every step in process generated tokens and also applies on that area like where we authenticate our information to others.

Token-based authentication is a security technique that authenticates the users who attempt to log in to a server, a network, or some other secure system, using a security

Token provided by the server. An authentication is successful if a user can prove to a server that he or she is a valid user by passing a security token. The service validates the security token and processes the user request. After the token is validated by the service, it is used to establish security context for the client, so the service can make authorization decisions or audit activity for successive user request.

3. Biometrics Based Technique:

In this recognition based technique we have different types of recognition techniques are there that are Poroscopy, Ear lobe, Nose tip Recognition face recognition, voice recognition, and Iris recognition.

A. Poroscopy: Poroscopy is a method of

Personal identification through the comparison of the impressions of sweat pores (present on friction ridges of palmer and plantar surfaces). The method was discovered and developed by Edmond Locard in 1912.

1. Number of Pores

Less than 50x magnification, average length of a ridge under view was found to be about 0.5 cm. Pores were counted on the ridges at random and average number of pores per centimeter of ridge was calculated

2. Distance between Pores (Interspacing) The spacing between the pores was calculated on the basis of number of pores in per unit area and their configuration, they were classified as:

a) Pores with close interspacing: Where pores were lying very close to each other and more than twelve pores were present on 1 cm. ridge length.
b) Pores in groups with close interspacing: The pores lying in the groups of two or more than two number of pores on 1 cm. Ridge length were classified as pores in groups.
c) Pores with distant interspacing: The number of pores present on one centimeter ridge length ranged from 8 to 11 and the space between the pores was comparatively more.
d) Pores with chain like formation: In this type of configuration, the pores were connected with each other making a chain like appearance and there was no interspacing present between the two pores.

3. Size of Pores

Size of the pores was determined by comparing the pores with the largest pore in the print and divided as:{a} minute {b} medium and {c} large.

4. Shape of Pores

Pores on the same ridge were found to be of different shape as following: [I] Rounded

[ii] Rhomboid [iii] Elliptical [iv] Square [v] Rectangular. In each area, the frequency of all these type of pores was determined by counting the number of pores of a particular shape.

5. Position of the Pores on the ridge Position of the pores on a ridge was determined by noting whether the pore as situated in the center of the ridge or on the periphery of the ridge. If lying on the periphery, the pore could either be an open type, i.e. with an open mouth towards furrow or just lying on the periphery with closed, well defined boundary, i.e. closed type.

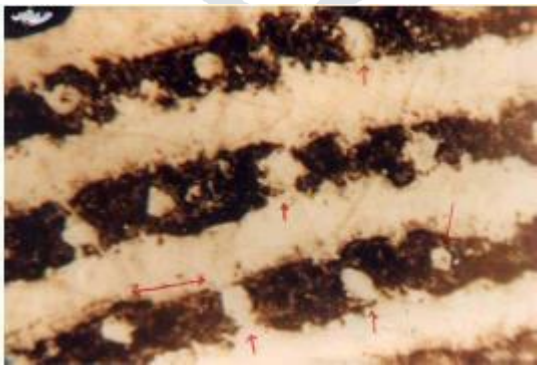

Figure 2 Pores of rhomboid and rectangular shape with open mouth and of distant type.

B. Ear lobe Recognition:

The ear lobes of study participants were assessed using 3D-reconstructed volumetric brain MRI scans. We used the MRIcroGL software to create a 3D model of the head. We confirmed the accuracy and excellent quality of reconstructed images by comparing them with actual participants' photographs in clinic .The typical DELC was defined as wrinkle-like line extending diagonally from the tragus across the lobule to the rear edge of the auricle of the ear. We visually checked for the presence of a distinct crease on each earlobe.

WMH visual rating scale:

We used a modified Fazekas scale for visual rating of WMH31, 32. On this scale, per ventricular WMH were classified as P1 (cap or band < 5 mm), P2 (5 mm ≤ cap or band < 10 mm), and P3 (cap or band ≥ 10 mm); deep WMH were classified into D1 (maximum diameter of deep white matter lesion < 10 mm), D2 (10 mm ≤ lesion < 25 mm), and D3 (≥25 mm). The intra-class correlation coefficients for inter-rater reliability of the WMH visual rating scale were excellent (Cohen's kappa=0.73–0.91)35. The WMH visual rating scale also correlated well with automated measurements of WMH volume36. WMH ratings were combined to give a final classification of minimal (combinations of D1 with P1 [D1P1] and D1 with P2 [D1P2]), moderate (D2P1, D3P1, D2P2, D3P2, D1P3, and D2P3) or severe (D3P3).

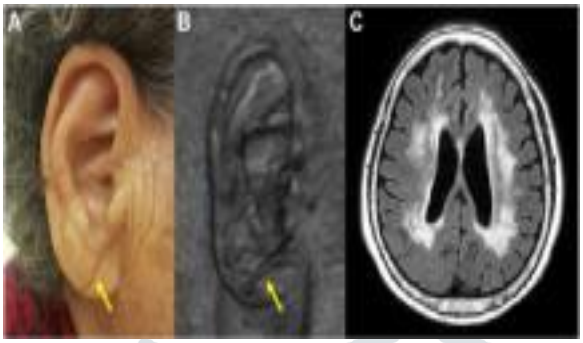

Figure 3: DELC**(**arrows) on photograph (**A**) and 3D-reconstructed MRI (**B**) in a cognitively impaired patient. The patient's brain MRI shows severe WMH on FLAIR imaging (**C**). DELC = diagonal earlobe crease; MRI = magnetic resonance imaging; WMH = white matter hyper intensities; FLAIR = fluid-attenuated inversion recovery.

C. Nose tip Recognition:

Nose detection is an important part of a 3D face recognition process. Knowledge of the nose location will enable us to align an unknown 3D face with those in a face database.

Besides that, the head pose can be deduced from information obtained from the nose. An important face feature point is the nose tip. This is because the nose is the highest protruding point from the face. Besides that, it is not affected by facial expressions. Another important function of the nose is that it is able to indicate the head pose. Using 2D images, past works have included using luminance values to locate the nose tip

This was achieved because the nose tip has a lower luminance value compared to other parts of the face. Besides that, the nostrils are considered as valley regions in a curvature map. However, this method would only work if the face was at a frontal position and looking straight into the camera. Tilted heads and non-frontal faces may cause error in nose detection since the nose tip luminance value might change or the nostrils.

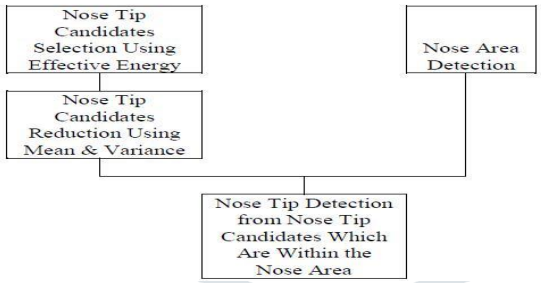

Figure 4: Detection Process

1. Nose tip candidate's detection:

Potential nose tip candidates are detected based on the position of their neighboring pixels. Since the nose tip is a protruding area, this means that all its neighbors should be at a lower height in the protruding direction. the effective energy of each neighboring pixels of each pixel is calculated.

$$Effective\ Energy = ||Pi - P|| \cos \theta$$

Where P is the pixel being investigated and Pi is the neighboring pixel.

From (1), ||Pi – P|| is the distance between the pixel and its neighbor while θ will be the angle between the normal vectors of the investigated pixel and the (Pi – P) vector.

2. Nose area detection:

The nose area is always between the eyes and mouth area. Therefore, the next step in this proposed method is to locate the eyes and mouth.

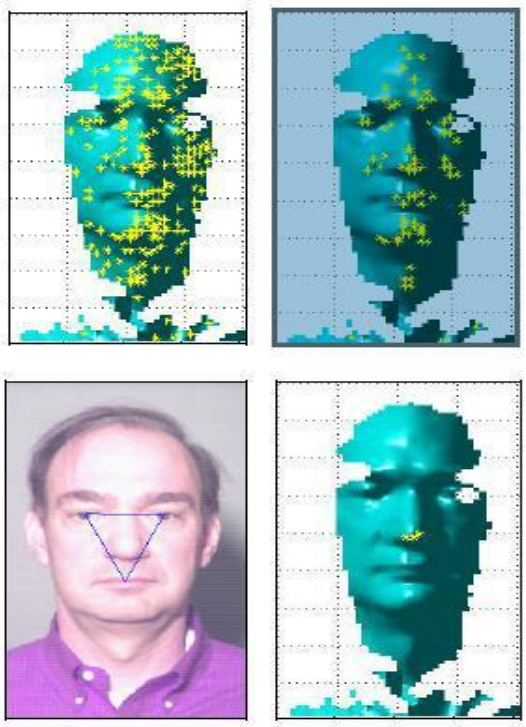

Fig5: Nose tip detection process.

II. Computer Authentication Techniques:

1. Textual and Graphical Passwords :

It can be further divided into two categories: recognition-based and recall-based graphical techniques.

Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage.

Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Main flaw was that password space was small since, the numbers of images were limited to 30.

2. 3D PASSWORD:

Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks.

Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. Many biometric authentications have been proposed. However, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked. The 3Dpassword is a multi factor authentication scheme. The design of the 3D virtual environment and the type of objects selected determine the 3D password key space. Moreover, user have freedom to select whether the 3D password will be solely recall, recognition, or token based, or combination of two schemes or more and given the large number of objects and items in the environment, the number of possible 3D passwords will increase. Thus, it becomes much more difficult for the attacker to guess

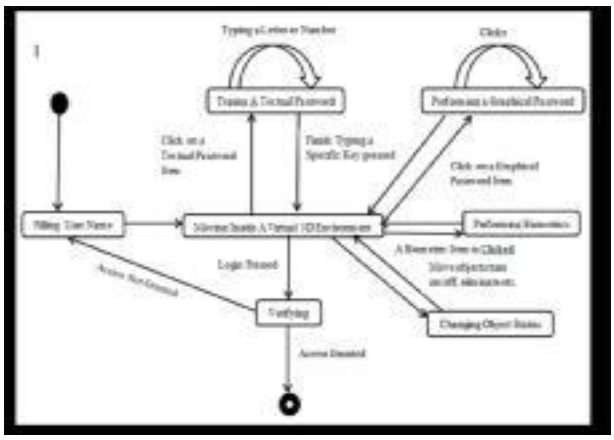

Figure:3 D Password and Diagram of Creating 3D Password.

3. 4DPASSWORD:

As the 3D authentication scheme suffers from many weaknesses such as shoulder surfing attack, timing attack etc., there is the possibility of hacking the 3D password. The 4-D Password scheme is an attempt to make the existing scheme even more robust and powerful [2]. We propose to add another key to the current scheme, and this will lend more stability and make the attacks on user privacy even more difficult to succeed in. This key, what we propose to refer to as the 'FOURTH DIMENSION' would be an encrypted string that encapsulates a gesture that the user is supposed to make with his hands, in front of a webcam, apart from his password.

Consider a web-based repository of research work for scientists, wherein each scientist has his own account which stores his files and folders. This repository employs the 4-D password scheme.

As a new user, I will sign up as follows:

1. Choose a username.
2. I will be redirected to the password generation page.
3. I will enter the 3-D environment. Inside the environment, I will perform certain actions, as have been discussed before.
4. I will exit out of the environment and submit my actions.
5. I will then be asked to perform a gesture in front of the webcam. This gesture, once successfully captured, will be saved. I will be notified of the time that I had taken to perform this gesture this time.
6. I will need to remember it for subsequent attempts at login Sign up process is complete.

IV. Application Areas

1. **Critical Servers:** Many organizations are using critical servers which are protected by a textual password. 4D Password authentication scheme proposes sound re-placement for these textual passwords.
2. **Banking:** Almost all the Indian banks started 3-D password service for security of buyer who wants to buy online or pay online.
3. **Nuclear and military Facilities:** 4D password has a very large password space And since it combines RECOGNITION+RECALL+TOKENS+BI O-METRIC in one authentication system, it can be used for providing security to nuclear and military facilities.
4. **Airplanes and Jet Fighters:** Since airplanes and Jet planes can be misused for religion and political agendas, they should be protected by a powerful Authentication scheme.
5. **ATMs, Desktop and Laptop Logins, Web Authentication.**

V. Conclusion and Future work

In this survey paper we are discussed about different types of security techniques and area applications. In those days most of persons are suffered by the hacker and unauthorized persons. So by knowing this mechanism and these techniques such as Human based, Computer based techniques, 3D, and 4DPASSWORD. We will easily save our credential data and any other hacker also couldn't find our information. We are currently evaluating different ways techniques individually and as part of our future work, we plan to implement this framework as a security system. We believe in prevention over cure, as cure may or may not be achieved.

References:

[1] Ahamed, B. B., & Hariharan, S. (2012). Integration of Sound Signature Authentication System. International Journal of Security and Its Applications, 6(4), 77-86.

[2] Grover Aman and Narang Winnie, "4D Authentication: Strengthening the Authentication Scene", in International Journal of Scientific and Engineering Research (IJSER).

[3] Farnaz Towhidi and Maslin Masrom, "A Survey on Recognition-Based Graphical User Authentication Algorithms", in International Journal of Computer Science And Information Security (IJCSIS).

[4] Ahamed, B. B., & Ramkumar, T. (2016). An intelligent web search framework for performing efficient retrieval of data. Computers & Electrical Engineering, 56, 289-299

[5] Wei Jen Chew, Kah Phooi Seng, and Li- Minn Ang," Nose Tip Detection on a Three-Dimensional Face Range Image Invariant to Head Pose" in IMECS March 2019.

[6] Bindra, B, Jasuja, OP and Singla AK. Poroscopy: "A method of personal identification revisited." in May 16, 2000.

[7] Yuvaraj,D., Sivaram, M., & Porkodi.,V.(2018).Detection and Removal Of Black Hole Attack In Mobile Ad Hoc Networks Using Grp Protocol. International Journal of Advanced Research in Computer Science, V9, no. 6, PP1-6