A SURVEY ON SECURE AUTHENTICATION WITH 4-D PASSWORD IN CLOUD COMPUTING

Priyanka C. Talhan, Rupali M. Thakare, Prof. A. D. Patil

Abstract— Cloud computing is an emerging frontier in field of computer technology in which the data and services resides in massively scalable data centers in the cloud and can be accessed from any connected devices over the internet. The advantages offered by cloud computing make it today's most existing technologies which is lower cost associated with computing while increasing flexibility and scalability for computer process, improved performance, increase computer power, unlimited storage capability etc. Cloud-computing is now-a-day one of the fastest growing part of IT industry. But it has bigger concern about its security. It is certainly possible that cloud system can be hacked and cloud-based documents accessed by unauthorized user. Due to this to access those cloud services only by authorized user we need a more secure authentication technique. In cloud computing authentication is done by many ways it could be 3-D password Authentication, Biometrics base authentication. 3-D Password authentication support multifactor authentication .3-D Password combines all those existing authentication schemes into a single 3-D virtual environment. There are several objects or items contained by 3-D virtual environment in which user has to interact with it. This type of interaction performed with many items and it varies from one item to another. The attackers from different backgrounds can break the system using 3-D password so strengthen it by adding a four dimensional password in it. This paper presents a study of the 3-D password and an approach to strengthen it by adding a 4-D password, which contain gesture recognition and time recording, and that would help in strengthen the authentication. Hence here we are using 4-D password using the 3-D password authentication.

Index Terms— Authentication Technique, cloud computing, cloud security, Privacy, 3-D virtual Environment, 3-D password generation, Gesture recognition.

1 INTRODUCTION

From the past few decades there is rapid change is happened in case of computer technology one of them is the cloud computing which portends a major change in how we store data and run applications. So all the IT companies put their data on cloud but it has major concern about its security so to put data securely in cloud database we need a more secure authentication technique.

Authentication is to check the identity of an individual. The job of authentication mechanism is to check whether only valid users are admitted. Basically the human authentication is base on those parameter knowledge base (what you know), token base(what you have) and biometrics (what you are) and computer authentication technique include textual and graphical password.

Knowledge-based authentication can be further divided into two categories as follows: 1) recall based and 2) recognition based.In case of Recall-based authentication user to recall the past password. Recognition based techniques require the user to identify and recognize the secret, or part of it, that the user selected in past authentication. One of the most common recall-based authentication schemes used in the computer world is textual passwords. In case of Graphical passwords authenticcation users need recall and recognize pictures to generate password. However, some of the graphical password schemes require a long time to be performed.

Biometrics is about the user personal characteristics which include fingerprint, palm print, hand geometry, face recognition, iris recognition, voice recognition etc. in case of biometric authentication difficulty is not come from the gathering of the actual measurements but from the analysis of these measures. Biometrics is the idea to map measurements of human physical characteristics to human uniqueness.

3-D password creates a 3-D virtual environment using the user's interaction with the specific events or action in 3-D virtual environment and its user choice to select the specific authentication technique will be a part of 3-D password.

4-D password uses the multifactor authentication all the existing authentication using biometrics, graphical and textual passwords are embedded in a 4-D password authentication technique [1]. 4-D password uses both the gesture recognition and time recording so, it is more powerful and secure authentication among all those existing technique and it strengthening the power of strong password.

2. LITERATURE REVIEW

The 3-D Authentication is also one of the strong authentication technique as it support the multifactor authentication technique rather than using single one for authentication in cloud computing.

1. The new scheme should not be either recall based or reconition based only. It contains all those authentication technique which are recall and recognition base with biometric and graphical password authentication.

2. In 3-D password it is user's choice to select authentication technique in the 3-D password which contains the recall and recognition based, biometric authentication, or token base authentication, or it may be a combination of two schemes or more. This choice of selecting authentication is user convenient because it is vary from each user. Some users not like to carry tokens. Some of the user's don't want to provide personal characteristics for authentication, and for some user it is very hectic job to remember it. Therefore, it is better to have user's choice in selection of authentication technique.
3. The new scheme should provide secrets that are easy to remember in the form of short story and it is very difficult for intruders to guess.
4. The password generation in new scheme is not easy to write it down on paper. Moreover, the scheme secrets should not be easy share with others.
5. The new scheme should provide secrets that can be easily revoked or changed. Based on the aforementioned requirements, we propose the 3-D password authentication scheme.

2.1. 3D Password Overview

The 3-D password is a multifactor authentication scheme. The 3-D password authentication is base on the 3-D virtual environment containing various virtual objects [2]. The user navigates through the 3-D environment and interacts with the objects. The 3-D password is the combination and the sequence of user interactions that occur in the 3-D virtual environment. The 3-D password can combines all type of authentication into a single one authentication scheme. This is done by designing a 3-D virtual environment that contains objects in which the information to be recalled, data to be recognized, and to present token, and also to check for biometric authentication. Firstly, the user can go to the virtual environment and type something on a computer that exists in ($x1$, $y1$, $z1$) position, then enter a room that has a fingerprint recognition device that exists in a position ($x2$, $y2$, $z2$) and take his or her fingerprint. Then, the user can go to the virtual parking, where he park car, and turn on the door and turn of the A.C. This combined action and the sequence generated by the previous actions towards the specific objects makes the user's 3-D password. Virtual object is the any real life object but it is not provided physically. Any actions performed by the user and their interactions with the real-life objects generate 3-D environment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3 D environment can be considered as a part of the 3-D password. It provides following objects:
1) A computer system on which the user can perform typing;
2) A fingerprint reader device that need the user's fingerprint;
3) A biometrical recognition device;
4) A paper or a white board that a user can do some writting, or make some painting.
5) An automated teller machine (ATM) that requests a token;
6) A light that can be switched on/off;
7) AC user can on/off.
8) A staple that can be punched;
9) A car that can be driven;
10) A book which can be reliable to use;
11) Any graphical password aythentication scheme;
12) Any real-life object;
13) Any upcoming authentication scheme;

The action toward an object (assume a fingerprint recognition device) that exists in location ($x1$, $y1$, $z1$) is different from the actions toward a similar object (another fingerprint recognition device) that exists in location ($x2$, $y2$, $z2$), where $x1 \_= x2$, $y1 \_= y2$, and $z1 \_= z2$. Therefore, to generate 3-D password, the user must have to follow the same scenario perform by the user. This means interacting with the same objects that reside at the exact locations and perform the exact actions in the proper sequence.

2.2. 3D Password Selection and Inputs

Let us consider a 3-D virtual environment space of size $G \times G \times G$. The 3-D environment space is represented by the coordinates $(x, y, z) \imath [1, \ldots, G] \times [1, \ldots, G] \times [1, \ldots, G]$. The objects are distributed in the 3-D virtual environment with unique (x, y, z) coordinates. We assume that the user can navigate into the 3-D virtual environment and interact with the objects using any input device which may be a mouse, keyboard, scanner to scan iris and fingerprint, card reader, and microphone.The user's 3-D Password is generated on the actions and interactions using the previous input devices. For example, consider a user who navigates through the 3-D virtual environment which consists of an office and conference room. Let's take an example that the user is in the virtual office and the user turns around to the door located in (10, 24, 91) and opens it. Then, the user closes the door. On which the computer is in left side which exists in the position (4, 34, 18), and the user types "FALCON." Then, the user walks to the conference room and picks up a pen located at (10, 24, 80) and draws only one dot in a paper located in (1, 18, 30), which is the dot (x, y) coordinate relative to the paper space is (330, 130). The login button is press by the usre. The starting representation of user actions in the 3-D virtual environment can generated as follows:
(10, 24, 91) Action = Open the office door;
(10, 24, 91) Action = Close the office door;
(4, 34, 18) Action = Typing, "F";
(4, 34, 18) Action = Typing, "A";
(4, 34, 18) Action = Typing, "L";
(4, 34, 18) Action = Typing, "C
(4, 34, 18) Action = Typing, "O";
(4, 34, 18) Action = Typing, "N";

(10, 24, 80) Action = Pick up the pen;
(1, 18, 80) Action = Drawing, point = (330, 130).
This representation is only an example. In order authenticated the user, the user has to follow the sequence and type of actions and interactions toward the objects for the user's original 3-D password.
3-D virtual environments can be designed to include any virtual objects. Therefore, the initial building block of the 3-D password system is for designing the 3-D virtual environment and to determine what objects contained in virtual environment. After the user has performed this action user will be back from the 3-D environment and request will be granted.

3 INTRODUCING THE FOURTH GENERATION

The proposed 4-D authentication is an attempt to make an existing authentication technique more secure and strong using both the gesture recognition and time recording. Proposed authentication technique is to lend more stability and even make it more secure from an unauthorized access [1].

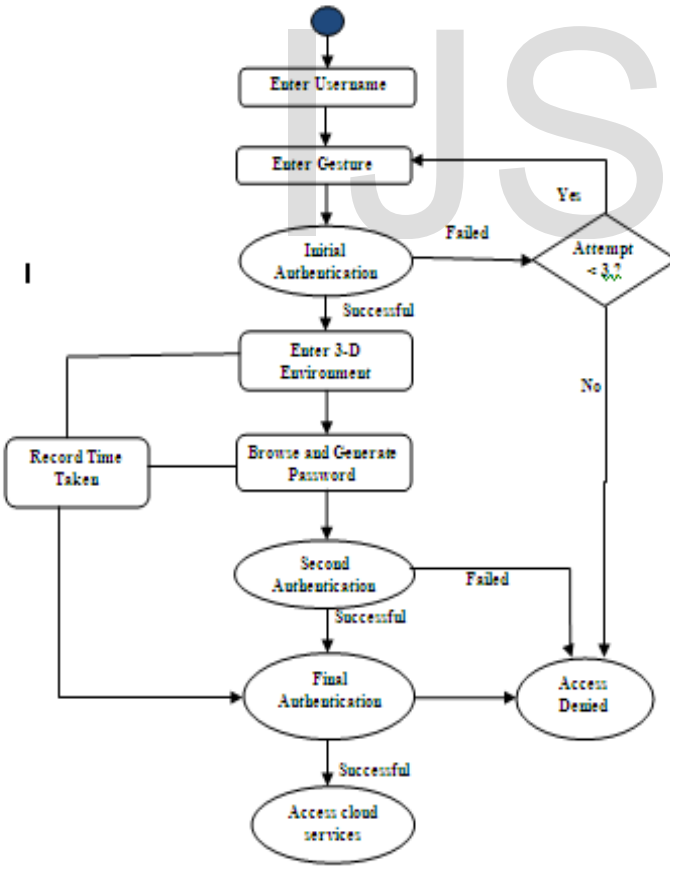

Figure 3.a) Flowchart of 4-D password steps

As shown in fig in proposed 4-D password authentication contain an encrypted string it encapsulate gesture in which user has to make with his hands in front of the webcam, apart from the password. This will make surety about user's physical appearance in login section in the authentication process. Then the users final password is both the combination of hand gestures and the 3-D password.
So, let us see how gesture would generated and saved for that we have an mapping function F(x) and if we put input function V then it becomes F(V) which is new final encrypted key. The user does not have to do anything for it. It is automatically generated by the system. User will only have to remember those gesture which would be captured and generate binary string it. This would be saved as precursor to the 3-D password [1]. Those input string V would then converted it into an encrypted format and then append it to the already existing password.
Hence then the resultant password would be as follows:
P=3-D password + F(V)
This is addition of 3-D password with the encrypted form of input function, but this addition may increase the complexity of the password. The attacker would try to guess the string V as well as try to decrypt the input function F(x), in addition to the complex technique requires to decrypt user's 3-D password itself.

3.1 Signup process

The new user can be sign in authentication phase by applying all those following steps:

1. First of all user has to choose an username
2. Then it helps you to directly go the password generation phase.
3. It needs to enter into a 3-D virtual environment.
4. In those 3-D virtual environment user need to do certain action.
5. Then user has to exit from the 3-D virtual environment and submit this action as we seen earlier.
6. Then user has to perform some gesture movement in front of the webcam. Once this gesture is successfully captured then it will be saved. User need to notify that this action of performing some gesture movement at this time.
7. User need to remember it for subsequent attempt at login sign up process is complete.

3.2 Logging in:

In case of log in section user need to enter username and then perform user's own gesture. After submission and verification of it user need to enter into an 3-D environment and perform password generation into it. Then user will exit and submit it. Once it is verified then it will give you an access to gain the cloud services.

3.3 Significance:

In 4-D password addition of gesture in front of webcam give more secure way of authentication. And it help to ensure that the physically presence of individual person for login session and not an automated program are there.

It also check for the time taken to complete for the 3-D authentication by the user. This time is considered to be a part user's of authentication procedure. Then in each of the subsequent authentication user must have to complete those authentication in same time period which is time taken by user to the last authentication or it may take few seconds more or less is also taken in consideration by the system itself. So each password can assign time window with it.

Here time taken to complete certain task of performing authentication procedure may help to find some unauthorized user's action also, that the time taken by user in last authentication to access to gain cloud service may vary mostly in few second in next subsequent authentication procedure but if it take more than those time it may be an chance of attempting to do illegal action by an unauthorized user or we can call it as hackers tryout.

1. If the whole authentication process takes to less time than those saved time period, then it may be an attempt made by hackers by creating some automated program to crack the authentication procedure for illegal access of cloud services.
2. If the time taken by user for authentication is very large, then it may be possibility of unauthorized user attempt it to do or try to access it illegally.

This addition of time allotment provide more secured region in case of authentication in 4-D password.

4 SECURITY ANALYSIS

As most of the IT companies move towards the cloud computing, and many of the hackers also have take closer look to access those cloud services illegally. Some the possible attacks followed by attackers are as followed.

4.1 Key logger

In this type of attack, attacker installed aninvisible software to capture the typed key by the user from the keyboard. In this way attacker try to know the user's password but in this authentication is not totally based on the textual data so, this attempt of an attacker may get fail.

4.2 shoulder surfing attack

This attack is by direct observation technique, like looking over someone when he is entering a password or attacker may use camera to record user's 4-D password, it is not depends only on textual data it contain gesture recognition plus there is an time recorder also provided as we have seen in proposed work so, if it could visible to the attacker then also it is not possible to match those gesture action with the user and system check it for with the previous recording. So, 4-D authentication technique is good bad guy deterrent in case of cloud security.

4.3 Well studied attack

In this case the attacker study it well the whole authentication procedure followed with the most probable password use by the user and for the 3-D password the attacker try has to know the selection of objects by the user so it is not so easy to accomplish it.

In the 4-D password there is an extra movement of gesture so it is possible for an attacker to match with both the 3-D password plus the gesture recognition so, this attack may also get failed with 4-D password and that's why it is more secure way of authentication while accessing cloud services.

4.4 Timing attack

With timing attack Attacker try to find out the time taken by user to complete authentication process with 4-D password, but this attack is not get successful because it is not give exact hint to the attacker.

5. ADVANTAGES AND APPLICATIONS OF 4-D PASSWORD

5.1 advantages of 4-D password

1. Flexibility: 4-D password authentication support multi-factor authentication it is the combination of all parameters of authentication. It includes biometric, graphical and textual password for the authentication that makes it is more secure.

2. Excellent bad guy deterrent: 4-D password is not totally based on the textual password it support both the biometrics, 3-d password authentication and also it contain an time recorder to record the time taken to generate 3-D password as we have in proposed work so hackers are less attracted towards the system which is protected by 4-D password.

3. Easily remember: You can easily remember it in the form of short story.

4. More secure with 4-D password: It gives us great security while accessing cloud services.

5.2 Applications

1. To access cloud services: "cloud" consisting of thousands

of computer and server, all linked together and accessible via the internet. Many of the IT companies put their sensitive data into the cloud so, it needs more secured authentication technique. 4-D is not only base on the textual password authentication but also uses the biometric authentication with extra security parameters are given in it. Thus, it is better option to use 4-D password in cloud computing

2. Critical servers: Many large organizations have critical servers that are usually protected by a textual password. 4-D password authentication give more secure authentication with extra addition of gesture recognition with the time recorder to record the time taken by user to complete authentication with 3-D password so, it may vary from person to person that's in the critical server application area you can use it.

3. Nuclear and military facilities: 4-D password authentication support multifactor authentication. so, it is more secure way of authentication in nuclear and military services.

4. Airplane and Jet fighter: To secure the most sensitive area like airplane and jet fighter we need a more secured authentication technique so 4-D password is better option among all those existing authentication technique.

6. CONCLUSION

4-D password is the combination of RECALL+ RECOGNITION+ BIOMETRIC Authentication [1]. it support the 3-D password with extra features of gesture recognition and time recorder .In cloud computing , to do secure access towards the cloud services it is better option to use 4-D password authentication and it also protected from many attacks like shoulder surfing attacks, brute force attack etc.

7. REFERENCES

[1] Grover Aman, Narang Winnie,"4-D password: Strenting the authentication scene", *volume 3 Issue 10*, International Journal of Scientific and Research Publications, October-2012, ISSN 2229-5518

[2] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod ,"Secure Authentication with 3D Password", *Volume 2, Issue 2*, page no. International Journal of Engineering Science and Innovative Technology (IJESIT) March 2013

[3] A. Adam and M. A. Sasse,"users are not the enemy: why users compromise computer security mechanisms & how to take remedial measure," *Communication of the ACM*, volume 42,PP. 41-46 1999.

[4] Anu Rathi, Yogech Kumar Anissh Talwar, "Aspects of Security in Cloud Computing", *Volume 2, Issue 4*, International Journal of Engineering and Computer Science ISSN: 2319-7242, Page no. 1361-1363, April 2013.

[5] K. Gihooly,"Biometric: Getting Back to Business,"in Computerworld, may 09, 2005

[6] R. Dhamija and A. Perrig,"Déjà vu: A user study using Iages for Authentication,"in processing of 9th USENIX security Symposism 2000.

[7] Duhan Pooja, Gupta Shilpi, Sangwan Sujata, & Gulati Vinita "Secured authentication: 3D Password"*volume3 242 – 245 .2012*

[8] Mr. Namdev A. Anwat Mr. Dattatray S. Shingate Dr. Varsha H. Patil "A Secure Authentication Mechanism using 3D Password" *Volume 1, Issue 1*, pp. 29-37 International Journal of Advance Research in Science, Engineering and Technology. July 2011

[9] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, *Senior Member, IEEE* "Three-Dimensional Password for More Secure Authentication" *Volume 57, Issue NO. 9*, IEEE SEPTEMBER 2008

[10] Maninder singh and Sarbjeet singh, "Design and Implementation of Multi-tier Authentication in Cloud Computing", *Volume 9 issue 5 No 2*, International journals of Computer Science, September 2012