ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 2, February 2014 Page No. 3920-3923

Authentication of System using Text, Image and Audio

Vikash Kumar Agarwal[1], Bhaskra Nand[2], Lalitendu khandagiri[3]

[1]Dept. of Information technology, BIT Mesra,
Ranchi 835215, India
vikash_rs_258@yahoo.co.in

[2]Dept. of Information technology, BIT Mesra,
Ranchi 835215, India
bhaskarnand4046@gmail.com

[3]Dept. of Information technology, BIT Mesra,
Ranchi 835215, India
lalit449@gamil.com

Abstract: Cyber-attacks has increased at a tremendous rate in the last decade. Due to this sensitive data like Bank Account details, login details of the accounts are not safe. Thus to counter this we need a robust authentication method. In recent years different types of fast authentication systems are already being developed such as token based, biometrics system, captcha etc. Each of the existing methods have their own merits and demerits. So in this paper we proposed a new model for the authentication using traditional text based password system with an integration of sound and image based password system. The Integrated system is difficult to spoof and the security principles cannot be breached easily.

Keywords: **Authentication, Password, Cyber-attacks, sound.**

.

1. Introduction

In today's fast changing hi tech environment where systems are converted into Smart phones, the probability of attack on the sensitive data stored in the system are very high. Today peoples are making transaction on their Smart phones using Apps, checking mails and doing many online activities. This results in movement of large data from system to the outside world, and there are more chances of the attack on this data. Attackers tries to get the login details such as password. The password is a very common and widely used authentication method[9] but due to its excessive use in many applications like data transfer, emails login, validating accounts ,online transactions etc., drawbacks of normal password appears(such as stealing of password, forgetting the password, providing a weak password, etc.). So it is required to have a strong authentication method to secure all our applications. The password are used for Authentication (Identify the user is who they say they are), Authorization (user is the authenticated person access specific information or not), Access Control (Restriction of access-includes authentication & authorization). Generally text based authentication is used to authorize a user, and user mostly select predictable password such as ***abcde, 12345678, password etc.*** User tries to choose passwords that are easy to memorize, but it falls into a predictable pattern which are easier for attacker to guess.

Number of other type of system such as Biometric system [7, 8] using fingerprint, retina, captcha based system, token based system [10] as in ATM are developed. But each of these have their demerits. Study shows text based password suffers with security problems. Many Security teams have the system to run network password cracker and within few minutes they identified the complete password.

The vulnerabilities of this technique have been well known generally. Dictionary attack is the common method used by the hackers to break the alphanumeric password. This attack is very effective because it only takes a small time to discover the user's passwords. Another drawback of text based password [1] is to remember the password. System using text Image [2, 5] and sound techniques have been proposed as an alternative to alphanumeric based techniques. The proposed model is designed to overcome the known weakness of traditional alphanumeric password. It makes the passwords more memorable, secure and easier to use. Based on the two assumptions; firstly humans can remember pictures and music better than alphanumeric characters and secondly a picture is worth a thousand passwords

2. Types of authentication method

The authentication methods are classified into three categories: token based (something the user has), biometrics based (something the user is) and knowledge based (something the user knows) authentication.

i. Biometrics Based Authentication

Biometrics authentication systems recognizes individual based upon one or more physical or behavioral traits. Biometrics systems authorizes the users by asking questions who he or she is? According to Zhu [6] biometrics provides the highest level of security among all other techniques. One characteristics of this method is physiological, related to the shape of the human body. Physiological characteristics includes fingerprints, iris recognition, face recognition and DNA [7]. It provides the best level of security, but still cannot be used because of its high costs. This cutting edge technology involves cost of device, cost of deployment and cost of support. There are some environmental issues which make the usage of biometrics difficult. For example, it is not reliable to use a sound recognition based technique in a noisy environment.

ii. Token Based Authentication

It is a two-step authentication technique. In this method user have to use an external device as a token to get into his/her account. This method is combined with other methods such as knowledge based to increase the level of security. Here, ATM cards [10] or smart cards is used with a combination of PIN or password. For example ATM cards with a combination of PIN is hard to crack and it proves the used identity electronically.

Here, token is used in the place of password or with a combination of token and password to confirm the used identification. This token based authentication is more strong compared to other ones. But each method have some demerits, as suggested by Microsoft article, the authentication algorithm must be installed on the centralized database and each client must have hardware to read the token and algorithm to process the data. The installment and replacing cost a lot to the company.

iii. Recognition Based Techniques.

In this method user have to choose several figures form a pool of figures and to create a picture password [4, 6], User have to memories this picture pattern also. During authentication phase user have to identify the correct images that they have selected earlier. This selection of pattern and memorizing it is the drawback of the above technique.

The most commonly used recognition based is Hash visualization, pass Faces, Jansen Model etc.

iv. Recall Based Techniques.

Recall based technique uses a graphical password [4] like an image and user has to enter the same password while login into his/her account. There are two types of recall-based techniques. One is Draw A Secret (DAS) and the other one is Pass Points [3].

3. Proposed system

The proposed system is designed using traditional text based password system with an integration of Sound and Image. Many system have been developed using the sound, but in the proposed system we used the play paused technique to integrate the sound. Study says that sound signature or tone can be used to recall facts like images, text etc. Here we play an audio source for some duration, User have to pause the audio clip at a particular time, a tolerance value is also selected with will decide that the user is legitimate or an impostor. To compare or authenticate user a Vector is created using text password, sound time and image coordinate. The vectors are as:

Vectors for authentication:-

The vector in the proposed system are as:

Sound password - (User ID, Sound Time value)

Image password- (User ID, Image number, coordinate x, coordinate y)

As an example of vectors for sound password and image password (Table 1.1) are as shown below.

Sound password (Abc, 26(in seconds))

Table 1.1: User details for Image password

User ID	Image	Coordinate x	Coordinate y
Abc	1	123	234
Abc	2	176	134
Abc	3	350	297
Abc	4	201	354
Abc	5	205	206

The flow diagram of the proposed system are as shown in figure 1. The algorithm for sign up during the registration phase and sign in during the login phase and the matching of the login credentials are as follows:

Algorithm of sign up

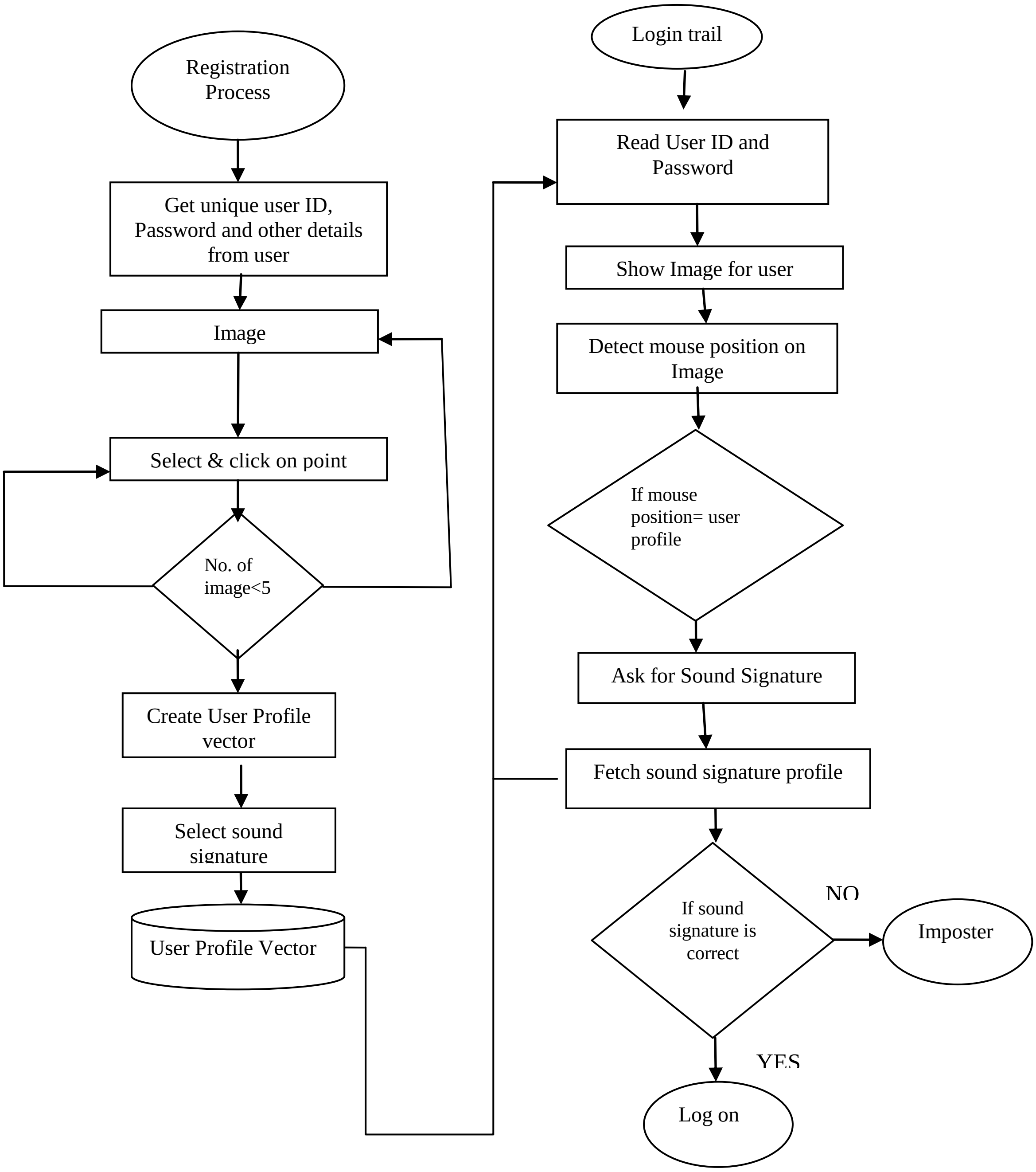
```
Start server
{
Wait for client request
On client request
{
Request=sign_up/sign_in
If (requests==sign_up)
{
Check if member is already register
If not then check other details and store in the database
Prompt for graphical password
Check whether it already stored or not
After checking all details store coordinates of all images
Prompt for sound password
Store sound frequency in the database
}
}
```

Algorithm of sign in

```
Start server
{
Wait for client request
On client request
{
Request=sign_up/sign_in
If (request==sign_in)
{
Check user_id and password is correct or not
If yes then prompt for graphical password
Read the graphical password and match with stored data
If matches then prompt for sound password
Read the sound password and match with stored data
If matches the redirect to his/her account
}
}
```

Here in the proposed algorithm first of all user have to enter the textual password, then a random image will appear, user have to click on the specific position which on authorization play an audio clip. User have to pause the audio at the specific position where he/she has paused during registration phase.

Figure 1: Flow diagram of the model


Registration Process
Get unique user ID, Password and other details from user
Image
Select & click on point
No. of image<5
Create User Profile vector
Select sound signature
User Profile Vector
Login trail
Read User ID and Password
Show Image for user
Detect mouse position on Image
If mouse position= user profile
Ask for Sound Signature
Fetch sound signature profile
If sound signature is correct
NO
Imposter
YES
Log on

.

4. Experimental Results

The system is developed I Vusual Studio 2010. The coding part is implemented in ASP.NET using C#. MySQL is the database which contains the details of 50 user. This user are the students of age group 20-28. First of all each user are asked to sign up, then different cyber-attacks are applied on the system.

Table 2: Result

User	No. of User	Accepted Trails	Rejected Trails
Legitimate	20	18	2
Imposter	20	1	19

From Table 2 as shown above, the result obtained shows that the proposed system is difficult to bypass as imposter are unable to get the login credentials.

4. Conclusion and Future Enhancement

With respect to the tolerance experiment, conclusion is that the smaller tolerance of 10 **x** 10 pixels seriously impaired users' memory, and correspondingly increased their password input time. Generally, they were able to identify the area of their point but had not stored sufficiently precise knowledge about the points. This effect would be likely to decrease with long-term use of the system and the regular use of the password, i.e., as their performance became more automated. However, if that precise memory decayed over a long lapse in usage, the user would again be susceptible to failure because of the small margin of error.

The proposed system is much more secure compared to the existing system as this system uses three level of authentication.

5. References

[1] Shepard R. N., "Recognition memory for words, Sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.

[2] Weinshall D. and Kirkpatrick S., "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[3] Chiasson, S., Biddle R., and P.C. van Oorschot." A Second Look at the Usability of Click-based Graphical Passwords". ACM SOUPS, 2007.

[4] Birget, J.C., D. Hong, and N. Memon."Graphical Passwords Based on Robust Discretization". IEEE Trans. Info. Forensics and Security, 1(3), September 2006.

[5] Dhamija R., Perrig A., "A User Study Using image for Authentication", in proceedings of 9th USENIX Security Symposium Denver, Colorado, USA: pp. 45-48.

[6] Suo X., Zhu Y., Own G. S., "Graphical Password: A Survey", Computer Security Applications Conference IEEE, 21st Annual, Tucson AZ: Dec 2005, pp. 472.

[7] Ratha, N.K., Thomas J., Bolle, R.M "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, 2001

[8] Chao L., Yi-xian Y., Xin-xin N.,"Biometric-based personal identity-authentication system and security analysis ", The Journal of China Universities of Posts and Telecommunications Volume 13, Issue 4, December 2006, Pages 43–47.

[9] Akula S., Devisetty V.,"Image Based Registration and Authentication System"Midwest Instruction and Computing Symposium, 2004.

[10] Han, Fengling et al. "A novel hybrid crypto-biometric authentication scheme for ATM based banking applications." Advances in Biometrics (2005): 675-681.