IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
**ISSN: 2320 - 8791**
**www.ijreat.org**

# Implementing Authentication Providers Using Image And Sound Signature

**[1]P.Elamathi, [2]S.Saranya, [3]E.Elamathi,**
**Department of CSE,**
**[123]Apollo Priyadarshanam Institute Of Technology, Tamilnadu.**

**ABSTRACT**

Here a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. In proposed work a click-based graphical passwordscheme called Cued Click Points (CCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point per image. In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image. System showed very good Performance in terms of speed, accuracy, and ease of use. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points.

***Keywords:*** *Sound signature, Authentication*

## 1.Introduction

Passwords are used for –
1.Authentication (Establishes that the user is who they say they are).
2.Authorization (The process used to decide if the authenticated person is allowed to access specific information or functions) and
3.Access Control (Restriction of access-includes authentication & authorization).
Mostly user select password that is predictable. This happens with both graphical and text based passwords. Users tend to choose memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. Number of graphical password systems has been developed; Study shows that text-based passwords suffers with both security and usability problems. According to a recent news article, a security team at a company ran a network password cracker and within 30 seconds and they identified about 80% of the passwords. It is well know that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic.
Graphical authentication mechanisms incorporate a graphical component in the authentication processes so users can select an image, draw a shape or choose colors instead of entering alphanumeric passwords.

One of the biggest problems with the ever-present username-password authentication system is the difficulty users have in remembering secure passwords. As a result, users often use simple passwords, which are easy to guess with social engineering techniques or crack with dictionary attacks, and even use the same password for different applications.

To eliminate these weaknesses, traditional alphanumeric passwords can be replaced by new graphical authentication systems, which can vary depending on the action the user is to perform. These systems can involve users:a.Identifying one or more images out of a group. b.Touching points of an image or moving one of the objects appearing in it.c.Drawing a line on a grid.

In all of the above cases, graphical authentication is based on the fact that our capacity for *recognizing* is much greater than our capacity for *remembering*, which means it is always going to be easier for us to recognize something that we have seen before (e.g., an image) than remember something without having a clue to prompt us.As well as being **easier to remember** for the user, graphical passwords are **more robust**, as it is much more difficult to apply brute force attacks to images than to text. Graphical passwords also make it impossible for there to be groups of passwords that are more common than others.Furthermore, for the same length,

alphanumeric passwords have a limited password space; i.e., they are always combinations of the same ASCII characters. Whereas, the inventory of possible graphical passwords is practically infinite.

## 2. Existing System

Graphical password, the user chooses several predefined regions in an image as his or her password. But Problem were faced in above system as maximum 12 clicks would be required for adequate security which becomes tedious for user for some images. In CCP, users click five points on one image. It also makes attacks based on hotspot analysis more challenging. Each click results in showing a next-image, in Effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. The number of predefined regions is small.The password may have to be up to 12 clicks for adequate security. Another problem of this system is the need for the predefined regions to be readily identifiable.

## 3. Proposed System

In proposed work a click-based graphical password scheme called Cued Click Points (CCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point per image. In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image.Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points. In the proposed work we have integrated sound signature to help in recalling the password. No system has been devolved so far which uses sound signature in graphical password authentication.It is used for more security purpose. System showed very good Performance in terms of speed, accuracy, and ease of use.Each participant was asked to register himself/herself and then each was invited to for login.

## 4.Implementation

### 4.1 Create An User Account

In User Account the current details of the user like User id, Password, Mail id, Contact no etc., are created. Once user information are updated we cannot change the information. Addition to this user information, Tolerance for Cued Click Points and Password for Sound Signature are created.The created User Details are then stored in Database. From the Database we can retrieve the User Details for Login purpose.

Master vector -

(User ID, Sound Signature frequency, Tolerance)

Detailed Vector - (Image, Click Points)

As an example of vectors -

Master vector (Smith , 2689, 50)

Detailed Vector

$$\begin{pmatrix} \text{Image} & \text{Click points} \\ I_1 & (123,678) \\ I_2 & (176,134) \\ I_3 & (450,297) \\ I_4 & (761,164) \end{pmatrix}$$

4.2 Image Selection And Sound Signature

To create User Profile, user has to **select** an Image then Click a particular point from the selected image. After that, the Click Points get stored in the Database. For Sound Signature, user has to give specific answer for Original question and also have to select one duplicate question for Sound verification, also stored in the Database. Profile vector is created by,

| No. | Login ID | Login Trails | Times Accepted | Times Rejected |
|---|---|---|---|---|
| 1 | U1 | 5 | 5 | 0 |
| 2 | U2 | 5 | 4 | 1 |
| 3 | U3 | 5 | 5 | 0 |
| 4 | U4 | 5 | 5 | 0 |
| 5 | U5 | 5 | 5 | 0 |
| 6 | U6 | 5 | 3 | 2 |
| 7 | U7 | 5 | 5 | 0 |
| 8 | U8 | 5 | 5 | 0 |
| 9 | U9 | 5 | 5 | 0 |
| 10 | U10 | 5 | 4 | 1 |
| 11 | U11 | 5 | 5 | 0 |
| 12 | U12 | 5 | 5 | 0 |
| 13 | U14 | 5 | 5 | 0 |
| 14 | U14 | 5 | 5 | 0 |
| 15 | U15 | 5 | 5 | 0 |
| 16 | U16 | 5 | 5 | 0 |
| 17 | U17 | 5 | 5 | 0 |
| 18 | U18 | 5 | 5 | 0 |
| 19 | U19 | 5 | 5 | 0 |
| 20 | U20 | 5 | 5 | 0 |

### 4.3 User Login

User Login is the starting page for the log-in customer. When the user is new one for the Login Page, have to select "Create a new account" button. Suppose the user select the "Login" button , error will display in the Prompt box. Only existing user can log in by using their user id and password. User may use Link Button for solving some Queries. Now the User can gain access to Member Self Service(MSS). Enter User id, Select correct Click Points on Image, Select one Sound Frequency, which will decide that the user is legitimate or an imposter. Euclidian distance between two points,

$$d(\mathbf{p},\mathbf{q}) = \sqrt{(p_1-q_1)^2+(p_2-q_2)^2+\cdots+(p_n-q_n)^2} = \sqrt{\sum_{i=1}^{n}(p_i-q_i)^2}.$$

In our system this value is used by the user,

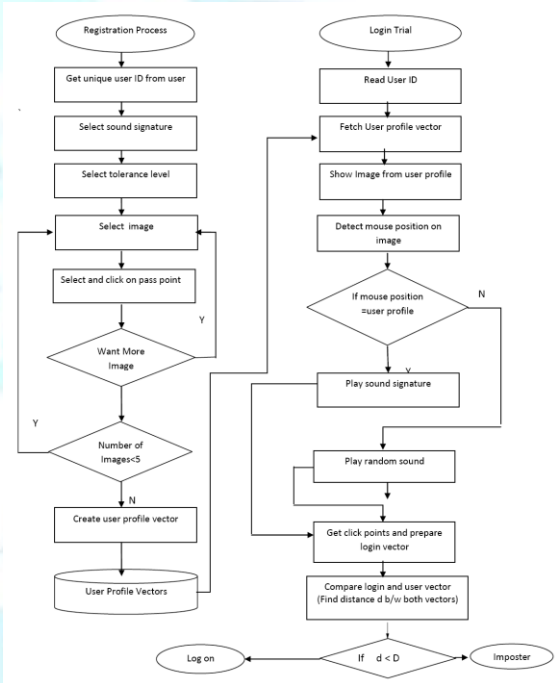
| No. | Login ID | Login Trails | Times Accepted | Times Rejected |
|---|---|---|---|---|
| 1 | U1 | 5 | 0 | 5 |
| 2 | U2 | 5 | 0 | 5 |
| 3 | U3 | 5 | 0 | 5 |
| 4 | U4 | 5 | 1 | 4 |
| 5 | U5 | 5 | 0 | 5 |
| 6 | U6 | 5 | 0 | 5 |
| 7 | U7 | 5 | 0 | 5 |
| 8 | U8 | 5 | 0 | 5 |
| 9 | U9 | 5 | 0 | 5 |
| 10 | U10 | 5 | 0 | 5 |
| 11 | U11 | 5 | 1 | 4 |
| 12 | U12 | 5 | 0 | 5 |
| 13 | U14 | 5 | 0 | 5 |

### 4.4 Password Recovery

In Password Recovery, Password are recovered from different Databases for Login purpose. In Admin, defence, Navy and Air force some Secret Files are uploaded that can be viewed by using Image and Sound Signature. The Click Points in the Image and Password from Sound

Frequency are used for Security purpose. It shows a good performance.

## 5.Architecture




## 6.Conclusion

We have concluded that authentication providers using sound signature to recall graphical password click points. No previously developed system used this approach this system is helpful when user is logging after a long time.

## 7. Future Enhancement

In future systems other patterns may be used for recalling purpose like touch of smells, study shows

that these patterns are veryuseful in recalling the associated objects like images or text.

## 8. References

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

[2]Blonder, G.E(1996). Graphical Passwords.United States Patent 5,559,961.

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

[4]Cranor, L.F., S. Garfinkel(2005). Security and Usability.O'Reilly Media.

[5]Davis, D., F. Monrose, and M.K. Reiter(2004). On User Choice in Graphical Password Schemes. 13th USENIX Security Symposium.

[6] Dirik, A.E., N. Menon, and J.C Birget. Modeling user choice in the PassPoints graphical password scheme.ACM SOUPS, 2007.

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

[8]http://freepastry.org

[9] http://www.lemurproject.org

[10] http://w.w.w.getdata.com

[11]http://w.w.w.microsoftlibrary.com