International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 2 246 – 248

Digital Identity on Internet

Supriya Khadake, Bernice Nadar, Sonal Ramteke, Sonali Pakhmode
Dept of Information Technology,
P.V.P.P.C.O.E, Sion, Mumbai
sdk4leo@yahoo.co.in, cmbernice@gmail.com, sonal6303@gmail.com, s_pakhmode@rediffmail.com

***Abstract*—** Security is an important issue in accessing various applications because of increasing threats in computer systems. There are various password schemes or graphical password software in market. An important goal for any authentication systems is to support users in selecting passwords of higher security. The concept of usable security aims at enhancing the authentication process by expanding the effective password space. The aim is to develop an application for digital identity using two level authentication techniques i.e. Username and Password followed by Graphical Password (Cued click point) to make it more secure.

Keywords- *CCP, Passpoint, Graphical Password, Usable Security.*

*****

I. INTRODUCTION

Most of the applications use text-based password for authentication, however it is more vulnerable to usability and security problems. While users are used to with this password scheme, the weakness is how users choose and manage them [1].

So as to increase the efficiency along with text-based password technique we make use of graphical password which includes images for authentication thus intended to be more memorable and usable [2]. Graphical password scheme is easier to recall as it is anytime easy to remember images and it also reduces the burden on users to greater extent [3]. Most of the system uses password scheme i.e. one level authentication which is less efficient. However, to make it more efficient this paper aims to develop an application using two level authentication i.e. text-based and graphical password techniques.

II. LITERATURE SURVEY

A. Graphical Password Techniques

Graphical password techniques are divided into three categories:

- Recognition Based Technique
- Recall Based Technique
- Cued Recall Based Technique [3]
- Recognition Based Technique: - In this a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he selected during registration stage.
  - Dhamija and Perrig: - In this user selects images out of many choices and identify them later in authentication.
  - Sobrado and Birget Scheme:-In this system displays a number of pass-objects (pre-selected by user) among many other objects, user click inside the convex hull bounded by pass-objects.
- Recall Based Technique:-In this a user is asked to reproduce something that he is created or selected earlier during the registration stage.
  - Draw - A - Secret (DAS) Scheme: Here user draws a simple picture on 2D grid displayed. While log in user has to draw the same picture in the exact sequence which is difficult to remember.
  - Pass point Scheme: In this user selects many password points on an image.
- Cued Recall Based Technique:-
  - Cued Click Point (CCP) scheme: Here user selects a password point on each image. Hence this technique helps user to recall the password point during log in stage. Also this technique provides better security than above mentioned techniques.

B. Existing System

Alternatives such as biometrics and tokens have their own drawbacks such as it is expensive and the identification process is slow.

Existing System contains text based password technique which includes Username and Password. At the time of finding the Identity of a person computer doesn't understand who is seated at client side whether he is that person or someone else. Users often create weak password that are easy for attackers to guess [2].

Pass point technique includes only one image where the user has to select multiple password points on that particular image itself. Here the user has to remember the order and position of click points [4]. While login process the user will have to select those multiple points on one image. Here the points might be closely located and that can cause error while authenticating if the point position is slightly changed while clicking. Also remembering all the points on one image and the sequence of points is difficult. This is the major disadvantage of this technique.

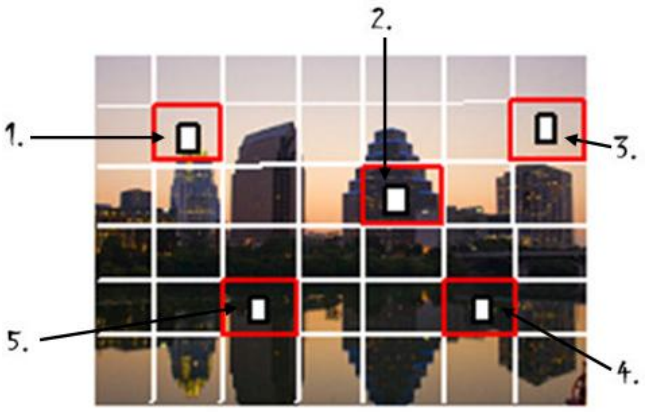

Figure 1: Passpoint technique (Points on one image)

III. PROPOSED SYSTEM

In the proposed system we are using two level for authentication i.e. text based password and graphical password technique. Text based password authentication is done through username and password whereas graphical password authentication is done through Cued Click Points (CCP).

Alternative for passpoint is Cued Click Point (CCP) which is a proposed technique. In CCP, users click one point on each of images rather than on different points on one image.

Images will occur only when user succeeds in the first level. For proper authentication the user will have to insert correct username and password. Once this is done and validated the next level will be crossed with images. Now first image will be displayed where the user will have to select correct password point on that particular image. Depending upon this click the next image will be displayed. If the click point in the previous image is correct the next image will be displayed and the process is same for the rest images. This way the images will occur in sequence and the user will have to select correct and accurate point for every image for proper and complete authentication. A wrong click leads down an incorrect path, with indication of authentication failure.

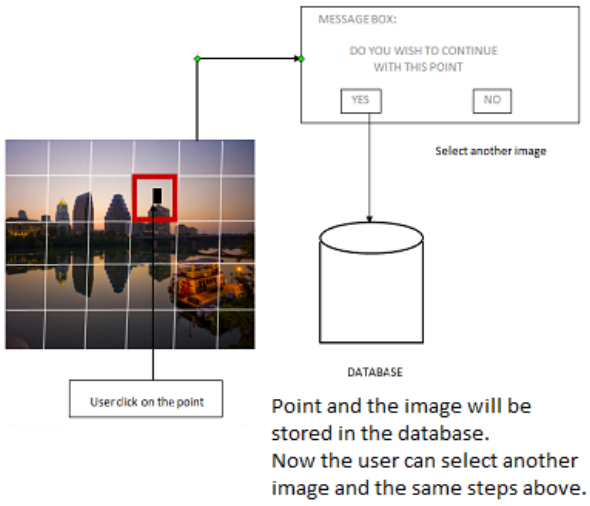

Figure 2: CCP technique

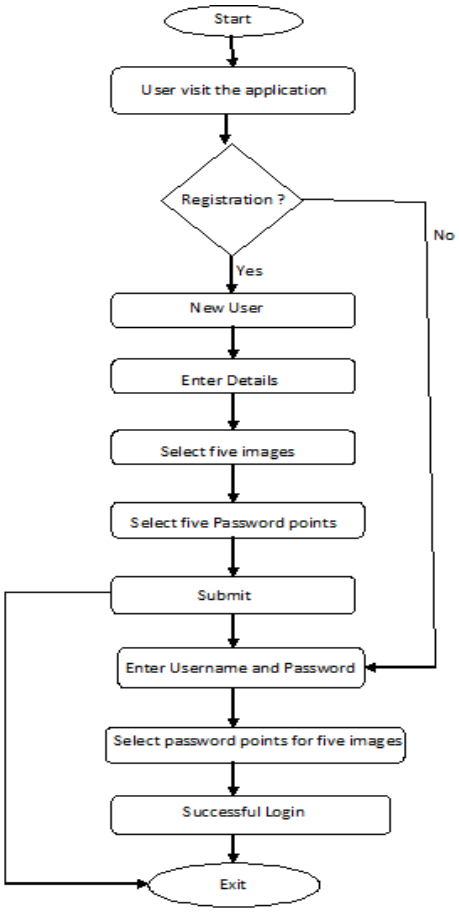

Figure 3: Flowchart of Digital Identity

IV. CONCLUSION

Taking security into consideration this proposed system ie text based and graphical password technique shows promise as a memorable authentication mechanism. By taking advantage of easily identifying image, CCP is more efficient and has advantages over Pass Point in terms of usability. It is anytime easy to remember one point on one image rather than remembering multiple series of points on one image. From this we conclude that CCP is more secure than Pass Point. Pass Point is more prone to hack as finding points on one image is easy for the intruder as it consists less permutation and combination and thus CCP increases the workload for them to first find set of images and then the points on each image.

V. FUTURE SCOPE

In future development we can also add challenge response interaction. In challenge response interactions, server will present a challenge to the client and the client need to give response according to the condition given. If the response is correct then access is granted. Also we can limit the number a user can enter the wrong password.

ACKNOWLEDGMENT

We thank our internal guide Mrs. Sonali Pakhmode, our Head of Department Mrs. Prachi Kshirsagar, our Principal and our Project Convener Mrs. Vidya Kawatikwar for their valuable guidance, help and constant encouragement to explore the topic. We thank our teachers for their support to understand the concept of the project.

REFERENCES

[1] Conklin, A.Dietrich, G.Walz, D. "Password based Authentication: A System Perspective" in Proceedings of the 37th Hawaii International Conference on System Sciences-2004.

[2] "Knowledge Based Authentication Mechanism Using Persuasive Cued Click", International Journal of Engineering Research & Technology (IJERT), Vol.2, Issue 6, June-2013.

[3] J.Biskup and J. Lopez, "Graphical Password Authentication Using Cued Click Points" ESORICS 2007, September 2007.

[4] "A Persuasive Cued Click-point based Authentication Mechanism with Dynamic User Blocks", International Journal of Research in Engineering and Advanced Technology (IJREAT), Volume 1, Issue 1, March, 2013.