RESEARCH ARTICLE OPEN ACCESS

Image Based Authentication Using Persuasive Cued Click Points

Ankita R Karia*, Dr. Archana B. Patankar**
*(M.E. Student, Department of Computer Science, Thadomal Shahani Engineering College, Mumbai University, Mumbai-50)
** (Associate Prof. Department of Computer Science, Thadomal Shahani Engineering College, Mumbai University, Mumbai-50)

ABSTRACT
User authentication is one of the most important procedures required to access secure and confidential data. Authentication of users is usually achieved through text-based passwords. Attackers through social engineering techniques easily obtain the text based password of a user. Apart from being vulnerable to social engineering attacks, text based passwords are either weak-and-memorable or secure-but-difficult-to-remember. Researchers of modern days have thus gone for alternative methods wherein graphical pictures are used as passwords. Image based authentication allows user to create graphical password which has advantages over text-based passwords. Graphical passwords have been designed to make passwords more memorable and easier for people to use. This paper focusses on creating a password by using a sequence of images such that one click-point per image contributes to password. Persuasive Technology is used to guide user's choice in click-based graphical passwords, inspiring users to select more random and thus more difficult to guess click-points. Also to enhance the security, a user has to decide a sequence for the images used during registration, which has to be reproduced by him during login phase.
Keywords **–** Authentication, Cued Click-Points, Security, Text-based passwords, bcrypt.

I. INTRODUCTION

Humans are considered as the weakest link in the security chain stating that the problem lies not with the security systems themselves, but with users who are unable or unwilling to comply with security protocols [1]. Authentication done using text-based password is prone to many attacks. Users often create passwords that are easy to memorize giving an opportunity for attackers to guess it. System generated passwords are secure, strong but difficult for users to remember. Despite the vulnerabilities, it's the natural tendency of the users to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attacks. Unfortunately, these passwords are broken mercilessly by intruders by several simple means such as masquerading, eaves dropping and other means such as dictionary attacks, shoulder surfing attacks, social engineering attacks. To address these authentication problems, a new alternative authentication technique have been proposed which uses images as passwords [2]. Image Based Authentication also referred as Graphical User Authentication is an authentication system that works by having the user select from images in a specific order presented in Graphical User Interface (GUI). Image based authentication allows user to create graphical password which has advantages over text-based passwords. Graphical passwords have been designed to make passwords more memorable and easier for people to use. Psychology studies have also revealed that the human brain is better at recognizing and recalling images than text [10]. Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures [11]. The idea of graphical passwords was originally developed by Greg Blonder in the year 1996 [3]. Image based authentication system allows us to create passwords that are resistant to guessing, dictionary attack, key loggers, and social engineering.

In this paper we propose an Image Based Authentication system that allows users choice password and simultaneously influences users to select stronger passwords. To add a layer of security, we ask user to assign a sequence number for each image used during registration phase. The user has to reproduce the same sequence during his login phase.

II. BACKGROUND

Authentication is a process of determining whether a particular individual or a device should be allowed to access a system or an application or merely an object running in a device [4]. Passwords have been the de facto method for authenticating users for many decades, and have proven to be resilient to change [5]. Passwords are classified as shown in Fig.2.1.

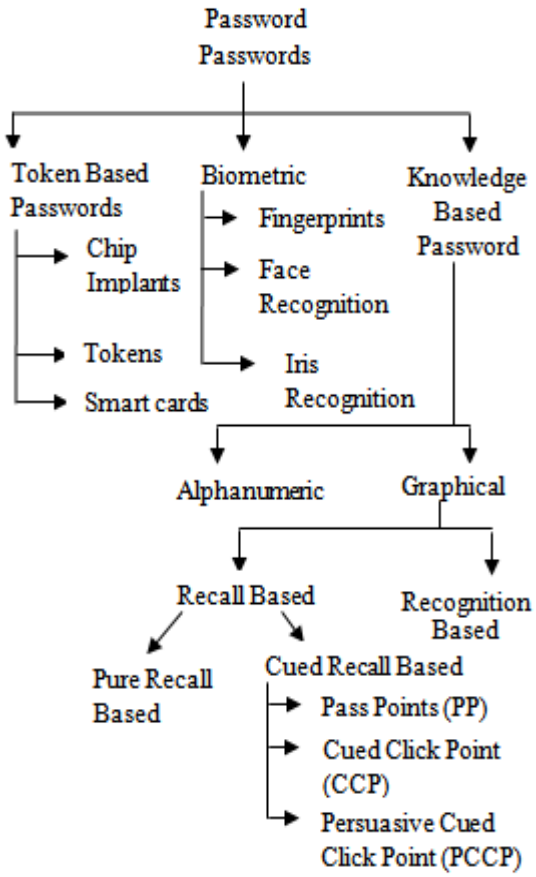

Fig. 2.1.Classification of passwords

2.1. Token Based Authentication

The traditional user name and password/PIN based authentication scheme is an example of the Token Based Authentication. It is based on -- Something You Have. E.g. Smart Cards, a driver's license, credit card, a university ID card etc.

2.2. Biometric Based Authentication

Biometric Authentication is verification of user's identity by means of physical trait or behavioral characteristics. It is based on- Something You Are. It uses physiological or behavioral characteristics like fingerprint or facial scans and iris or voice recognition to identify users [4].

2.3. Knowledge Based Authentication

Knowledge based technique are the most extensively used authentication techniques and include both text based and picture based passwords. Knowledge Based Authentication is based on Something You Know. Knowledge based authentication is further classified into Alphanumeric and Graphical Password.

The major drawback of Token Based and Biometric Based authentication methods is that they are expensive and require special devices. Graphical-based password techniques have been proposed as a potential alternative to text-based techniques, supported partially by the fact that humans can remember images better than text [4].

III. RELATED WORK

Greg Blonder [9] was the one who developed the concept of graphical password. Graphical passwords were introduced to overcome the shortcomings of alphanumeric passwords. In graphical authentication systems a password consists of sequence of one or more images where user can input password with the help of mouse events like click, drag etc. [2]. Graphical passwords have been used in authentication for mobile phones, ATM machines, e-transactions [2]. Graphical Passwords are categorized as:-

3.1. Recognition Based Authentication

In recognition based authentication, a user is presented with a set of images and the user is supposed to pick and memorize several images among a set. While authenticating, the user needs to recognize their registration choice among a set of candidates. Various schemes proposed under this category were as follows [2]:-

3.1.1. Jensen et al Method

PDAs [2] Users selected images with the help of a stylus. A numerical sequence is registered which now acts as a password for the user. At login time user has to recognize same images in same sequence [2]. The main drawback of this method is its small password space, because the numbers of images were limited to 30 as shown in Fig.3.1.

Fig. 3.1. Cats and dogs theme [2]

3.1.2. Passfaces Method

This method was developed by Real User Corporation [2]. During login phase user is presented with a grid of faces. User has to select 4 faces: one from each of 4 grids of 9 faces as shown in Fig.3.2. The user is authorized only if he identifies correctly 4 passfaces two times consecutively. Passfaces can be predictable as they are affected by race, gender and attractiveness [2].

Fig. 3.2. Passfaces Scheme [2]

3.1.3. Sobrado and Briget Method

Sobrado and Briget developed a method to prevent shoulder surfing attack [2]. During registration user had to select objects from number of displayed objects. At login time, the user had to select objects which he had selected during registration time and then click inside the convex hull formed by objects as shown in Fig.3.3. To make password space larger 1000 objects were used at login process [2]. However, the display became crowded and it was difficult to find pass –objects [2].

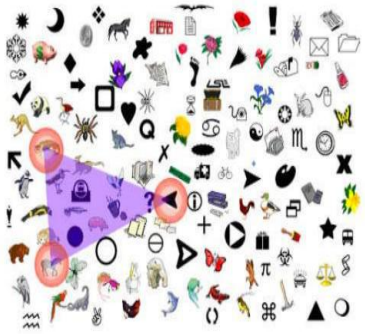
Fig. 3.3.Convex hull shoulder surfing [2]

3.2. Recall Based Authentication

In this technique, a user is asked to reproduce something that he or she created or selected earlier during registration phase. This technique can also be referred as Click Based Graphical Password technique. These are classified into two types:-

3.2.1. Pure Recall Based Technique

In this technique, a user needs to reproduce their passwords without being given any reminder, hints or gesture. Although this category is easy and convenient but it seems that users hardly can remember their passwords. Draw A Secret is one of the scheme which falls under this category. In this scheme during registration user has to draw something on a GRID of size Y x Y as shown in Figure 3.4. The coordinates (X, Y) of the grid were stored in the order of drawing. To log in, a user has to redraw such that the drawing touches the registered sequence of coordinates.

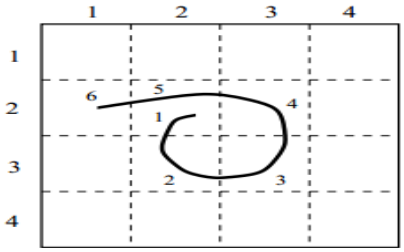

Fig. 3.4. Draw A Secret [2]

3.2.2. Cued Recall Based Technique

In this category, the technique developed a frame which supports reminder, hints and gesture. This in turn helps the user to reproduce their password or to make a reproduction more accurate. Various schemes have been proposed under this technique but the recent types include the following:-

3.2.2.1. Pass Point (PP)

This is click-based graphical password authentication where a user arbitrarily clicks on five points on an image during the registration phase [4]. While logging in, the user has to click on the same points as selected during registration process as shown in Fig.3.5.


Fig. 3.5.Pass Point Scheme [2]

3.2.2.2. Cued Click Point (CCP)

In this method instead of selecting five points on an image, user selects one point per image for five images. The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point as shown in Fig.3.6. The system determines the next image to display based on the user's click-point on the current image. It now presents a one to-one cued recall scenario where each image triggers the user's memory of the one click-point on that image [2]. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect.

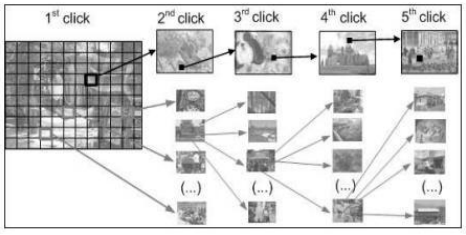

Fig. 3.6. Cued Click Points [2]

3.2.2.3. Persuasive Cued Click Point (PCCP)

Persuasive Technology was first articulated by Fogg [6]. Persuasive feature is added to CCP to encourage users to select less predictable passwords. The viewport [1] is positioned randomly as shown in Fig. 3.7., rather than specifically to avoid known hotspots, since such information might allow attackers to improve guesses and could lead to the formation of new hotspots. Thus it makes it more difficult to select passwords where all five click-points are hotspots Persuasive technology guides and encourages users to select stronger passwords, but not impose system-generated passwords.

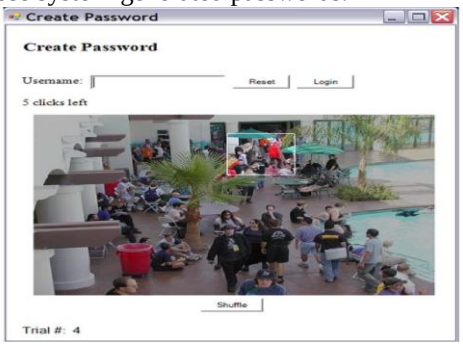

Fig.3.7. PCCP. The viewport highlights part of the image [6]

A comparative study of various Graphical passwords is shown in TABLE 3.1.

Table 3.1. Comparative Study of different Graphical Passwords

Technique	Login Interface	Drawback
Jensen et.al	Select images based on a theme	Small password space
Passfaces	Select face from a grid of faces	Predictable
Sobrado and Briget Method.	Select objects from number of displayed objects	Difficulty in identifying objects from crowded display of objects
Draw A Secret	Redraw such that the drawing touches the registered sequence of coordinates	Difficulty in redrawing precisely
Pass Point	Make sequence of click points on image	Pass points are difficult to learn
Cued Click Point	Make single click on multiple images	Hotspots still remain an issue

IV. SYSTEM ARCHITECTURE

Image based authentication system using persuasive cued click points consists of 3 modules as shown in Fig.5.1. It includes registration module, picture selection module, and login module.

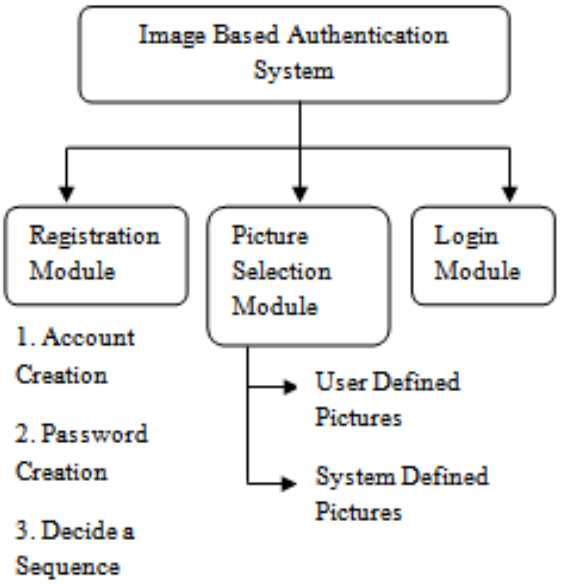

Fig.5.1. System Modules

4.1. Registration Phase

Registration phase is carried out according to the flowchart shown in Fig. 5.2. This registration phase includes Registration module and Picture Selection Module.

4.1.1. Registration Module

This module is divided into 3 stages. First is Account Creation which is followed by Password Creation and finally Deciding sequence of images presented or selected. The user has to successfully create his account first. In this system, each user is identified by a unique username. Hence to make sure that each user has a unique username, the system before creating an account checks for the availability of username. If the Username specified by user already exists, then the system prompts for the availability of that name.

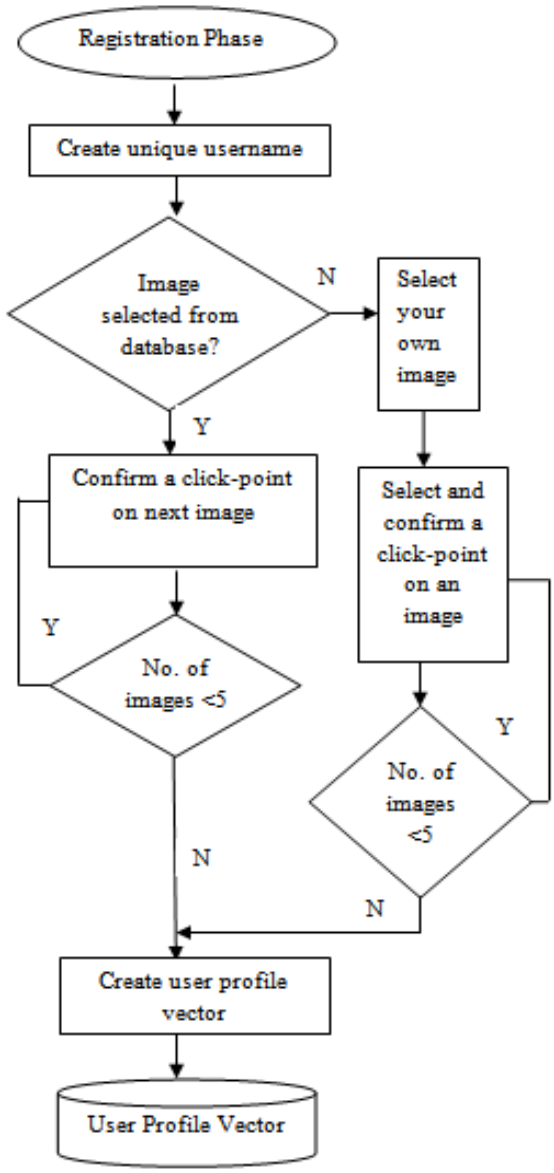

Fig.5.2. Registration Phase

During password creation, user is presented with an image which is slightly faded except for a randomly positioned viewport as shown in Figure 5.3. The shuffle button is also provided which helps the user to reposition the viewport. A user can shuffle the viewport only limited number of times. Once the user is satisfied with the click-point, he confirms his point. This confirmed click-point is then stored in database in encrypted format. brcypt encryption is used here for better security. This process will continue for 5 images.

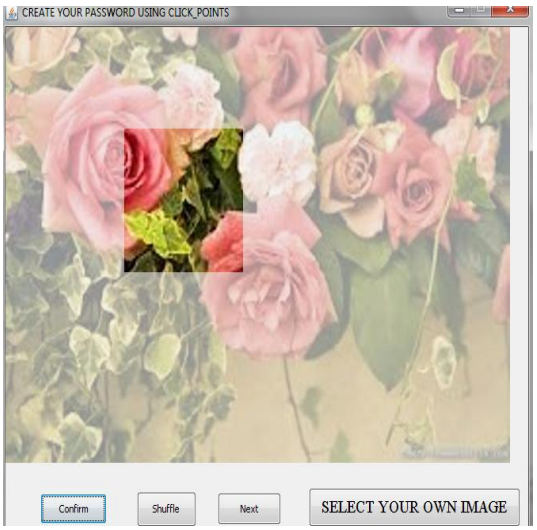

Fig.5.3. Image with randomly positioned viewport

4.1.2. Picture Selection Module

In picture selection phase there are two ways for selecting picture password authentication. The user can select pictures of his choice or can directly get the images from database.

4.12.1. User-Defined Pictures

Pictures are selected by the user from the hard disk or any other image supported devices.

4.1.2.2. System-Defined Pictures

Pictures are selected by the user from the database of the password system.

4.2. Login Phase

The login phase is carried out according to the flowchart shown in Fig. 5.4. During logging to the Image based Authentication System, the user is presented with the first image which he had used during registration time. While logging, the viewport will not be visible and the user has to click on his registered click-point on the image. Since it is practically impossible for a person to click on the exact point, hence a tolerance value is hard coded in the system. The tolerance value (D) indicates the degree of closeness to the actual click-point. Euclidean distance [7] is calculated to find the distance between two click points. Euclidean distance between two points' p and q is given by-

$$d(p\ q) = \sqrt{(p1-q1)^2 + (p2-q2)^2 + \ldots + (pn-qn)^2}$$
$$= \sqrt{\Sigma}\ (pi-qi)2 \quad i=1 \text{ to } n$$

Above distance is calculated for each image and if this distance comes out less than a tolerance value D then only next registered image is displayed. The value of D is taken as 5 in our system.

Thus, if the click-point falls within the system defined tolerance square then only the next

correct image will be displayed to the user, else a random image will be displayed which may lead the user to the wrong path. The next image displayed is always based on the location of the previously entered click-point, creating a path through an image set. Thus a wrong click leads to an incorrect path, with an explicit indication of authentication failure only after the final click [4]. Only on successful completion of this process, the user is presented with 9 images in grid form as shown in Fig. 5.5.

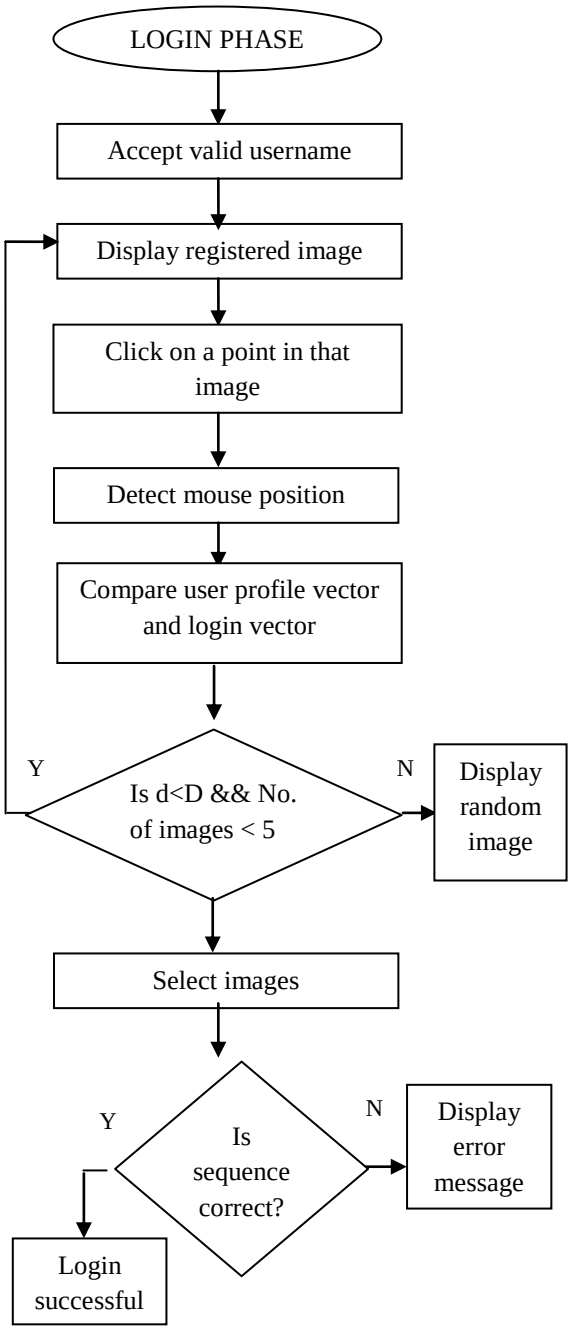

Fig. 5.4.Login Phase

Fig. 5.5.Random Images in Grid Form for Sequence Selection

V. RESULTS & ANALYSIS

Image Based Authentication System using Persuasive Cued Click Points is resistant to may standard security attacks such as Dictionary attack, Brute force attack, Hotspots, Guessing attacks, Capture attacks, etc.

5.1. Brute Force Attack

Text based passwords have password space of 94^N [2]. It is difficult to do this attack on graphical passwords. It is harder for this attack to succeed for graphical passwords

5.2. Social Engineering Attack

For social engineering attacks against cued-recall graphical passwords, a frame of reference must be established between parties to convey the password in sufficient detail [8]. Password sharing through verbal description may be possible for Pass Points. For PCCP, more effort may be required to describe each image and the exact location of each click-point. Graphical passwords may also potentially be shared by taking photos, capturing screen shots, or drawing, albeit requiring more effort than for text passwords [8].

5.3. Capture Attack

Password capture attacks occur when attackers directly obtain passwords by intercepting user entered data, or by tricking users into revealing their passwords. The attacker's task is more difficult for PCCP because not only the popularity of hotspots is reduced, but the sequence of images must be determined and each relevant image collected, making a customized attack per user.

5.4. Hotspots

Hotspots are specific areas in the image that have a higher probability of being selected by users as part of their passwords. If attackers can accurately predict the hotspots in an image, then a dictionary of passwords containing combinations of these hotspots can be built. Hotspots are known to be problematic for Pass Points.

Many user were asked to try the new authentication system i.e. Image Based Authentication system using Persuasive Cued Click Points. Every user was asked to login 8 times to the system at different time intervals. The following TABLE 5.1. shows results with tolerance value 5:-

Table 5.1. Results with tolerance value 5

No. of users	Success Rate	Percentage of Success Rate
1	6/8	75.0
2	7/8	87.5
3	6/8	75.0
4	5/8	62.5
5	7/8	87.5
6	7/8	87.5

The percentage success rate reduces with reduction in tolerance value. The following TABLE 5.2.shows the percentage success rate with tolerance value 4:-

Table 5.2. Results with tolerance value 4

No. of users	Success Rate	Percentage of Success Rate
1	4/8	50.0
2	5/8	62.5
3	5/8	62.5
4	4/8	50.0
5	3/8	37.5
6	5/8	62.5

VI. CONCLUSION

User authentication is fundamental aspect in most computer security context. The proposed Image based authentication scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, PCCP has advantages over CCP in terms of usability and hotspots. PCCP encourages and guides users in selecting more random click-based graphical passwords. A key feature in PCCP is that creating a secure password is the "path-of-least-resistance" [6], making it likely to be more effective than schemes where behaving securely adds an extra burden on users. The approach has proven effective at reducing the formation of hotspots, avoid shoulder surfing problem and also provide high security success rate, while still maintaining usability. The proposed authentication system is also resistant to various attacks such as Brute Force attack; Social Engineering attack, Hotspots etc. Image Based Authentication System using Persuasive Cued Click Points has many benefits such as two factor authentication, easily memorable password, high security etc. thus making it an appropriate authentication system.

REFERENCES

[1] Sonia Chiasson, *Usable Authentication and Click-Based Graphical Passwords*, doctoral diss, Carleton University, Otttawa, Ontario, 2008.

[2] Harsh Kumar Sarohi, Farhat Ullah Khan, Graphical Password Authentication Schemes: Current Status and Key Issues, *International Journal of Computer Science Issues*, 10(2), 2013, 437-443.

[3] P.V.S.Sriram, G.Sri Swetha, A novel 2 step random colored Grid Graphical Password Authemtication System, *International Journal of Computer Science and Engineering Technology, 4(4)*, 2013, 322-325.

[4] Priti C. Golhar, Dr. D.S. Adane, Graphical Knowledge Based Authentication Mechanism, *International Journal of Advanced Research in Computer Science and Software Engineering, 2(10)*, 2012, 48-54.

[5] Georgios Kontaxis, Elias Athanasopoulos, Georgios Portokalidis, Angelos D. Keromytis, SAuth: Protecting User Accounts from Password Database Leaks, ACM, 2013.

[6] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van Oorschot, Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authetication Mechanism, *IEEE Trans. Dependable and Secure Computing*, 9(2), 2012, 222-235.

[7] Saurabh Singh, Gaurav Agarwal, Integration of Sound Signature in Graphical Password Authentication System, *International Journal of Computer Applications*, 12(9), 2011, pp. 11-13.

[8] Iranna A M, Pankaja Patil, Graphical Password Authentication Using Persuasive Cued Click Point, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2(7)*, 2013, 2963-2974.

[9] Mrs. M. L. Prasanthi, Devi Srinivas, Implementation of Knowledge Based Authentication System Using Persuasive Cued Click Points, *International Journal of Mathematics and Computer Research*, 1(1), 2013, 15-19.

[10] Arash Habibi, Lashkari, Farnaz Towhidi, Dr. Rosli Saleh, Samaneh Farmand, A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms, *International Conference on Computer and Electrical Engineering*, pp. 527-532, 2009.

[11] Sonia Chiasson, P.C van Oorschot and Robert Biddle, "Graphical Password Authentication Using Cued Click Points," Springer-Verlag Berlin Heidelberg, LNCS 4734, pp.359-374, 2007.