International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Special Issue 31(September, 2015), PP. 29-36

USING PERSUASIVE TECHNOLOGY IN CLICK BASED GRAPHICAL PASSWORDS

Ms. Shilpa Veerasekaran [1], Prof. Alka Khade [2], Prof. V.B Gaikwad [3]
Dept of Computer Engineering, Terna Engineering College
Nerul, Navi-Mumbai-400706, India
[1]shilpaveerasekaran@gmail.com
[2] khade.alka@gmail.com
[3] vb_2k@rediffmail.com

Abstract : **Knowledge based authentication mechanisms have several problems that are well known. The knowledge based authentication mechanisms include several techniques like text passwords, biometric passwords and graphical passwords. Users often tend to choose passwords which are easy to remember. Using easier passwords allows hackers to easily crack the passwords using various hacking techniques. Unfortunately, the use of text based passwords can be very difficult, if users select different passwords for better security. In such a situation remembering different passwords will be a difficult task in itself. Graphical Passwords is a widely used reliable authentication mechanism. Traditional authentication mechanisms are prone to hacking. We propose a methodology where users are given a choice to select a stronger password using Persuasive Cued Click Points.**

Keywords : Graphical Passwords, Knowledge Based Authentication Mechanism, Persuasive Cued Click Points, Persuasive Technology

I. INTRODUCTION

Among the authentication schemes, graphical passwords are passwords that are based on images instead of alphanumeric strings. Graphical Passwords are brought into use for greater memorability and to reduce the tendency of choosing insecure passwords. Its is expected that using images as passwords should increase overall password security. Graphical passwords were introduced by Blonder (1996) [3],[6]. According to the description given by Blonder, the image will be displayed on the screen and the user will have to click on a few regions. If the user clicks on the correct regions, the user is authenticated. Two key human factors to be considered here are memorability and efficiency of the input. In the graphical password system, the user has to choose memorable locations in an image as a password. Selecting memorable locations in the image depends on the nature of the image itself and the specific sequence of click points. In the graphical password system based on recognition, the user has to recognize previously seen images, based on the choices that either the image is known or unknown. In this password system an intermediary form of recollection between pure recall and recognition that is cued recall is used. Scanning an image for finding their previously chosen locations in the image is cued recall because viewing the image reminds, or cues users about their click areas. Graphical Password can be classified into several techniques. The following figure represents the authentication schemes under the graphical passwords.

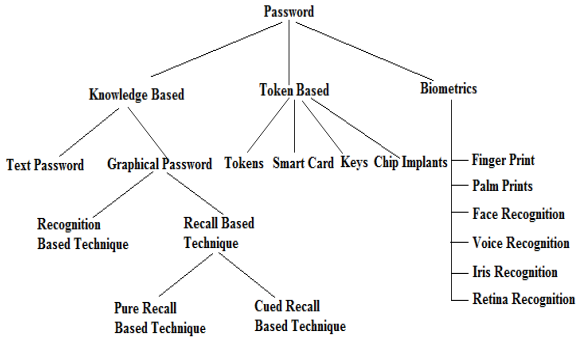


Figure 1.1 Classification of Passwords [1]

The difficulty with text based password is that user creates memorable password which can be broken easily and also that the text password has limited length password which means that password space is small. Biometric based authentication techniques are a bit pricey, slow and erratic and therefore not preferred by many [4]. Token based authentication system has high security, usability and user-friendliness in comparison to the other techniques [4]. The system also makes use of the knowledge based techniques to boost the security of token based system. But the setback in token based system is that if the token gets lost, the security is also compromised.

Generally, the graphical password techniques can be classified into two categories [3],[4]:

(1) recognition-based graphical techniques
(2) recall-based graphical techniques.

II. RELATED WORKS

2.1 Recognition Based Graphical Techniques

Using recognition based graphical techniques, a user is presented with a set of images and the user passes the authentication phase by recognizing and identifying the images he or she selected during the registration stage. There are many graphical password authentication schemes which are designed by using recognition-based techniques [3]. They are discussed below.

Jensen et al. had proposed a graphical password scheme based on "picture password" intended specially for mobile devices. In the password creation process , the user has to first select the theme from the given choices (e.g cats and dogs, mountains, seashore) which consists of thumbnail photos. The user then selects and registers a sequence of the selected thumbnail photo to form a password (Figure. 1.2).

Figure 2.1 Cats and Dogs Theme [3]

The user needs to recognize and identify the previously seen photos and touch it in the correct sequence using a stylus in order to be authenticated .

2.2 Recall Based Graphical Techniques

In recall-based systems, the user is asked to repeat what he/she had created or selected previously during the registration phase. Recall based schemes can be classified into two groups, that is pure recall-based technique and cued recall-based technique.

In the pure recall based technique, users are expected to reproduce the passwords without any assistance or reminder. Some of the examples of pure recall based techniques are Draw-A-secret Scheme, Grid selection, Pass Doodle [3].

Draw-A-Secret scheme is the scheme in which the password is a pattern drawn on a two dimensional grid of size G*G. The grid is composed of cells where each cell is represented by distinct rectangular coordinates (x, y) [3].

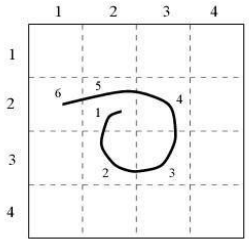


Figure 2.2 Draw A Secret Scheme [3]

In 2004, Thorpe and Van Oorschot proposed the Grid selection method to enhance the password space of Draw A Scheme(DAS) [3]. For improvement of the DAS security level, the Grid Selection technique was suggested, where the selection grid is large at the beginning. The user selects a drawing grid from the fine grained grid, a rectangular area to zoom in on, in which the user has to enter the password as shown in Fig.1.4 This technique is expected to increase the password space of DAS, which also improves the security level at the same time. This technique only improves the password space of DAS however carries over DAS weaknesses.

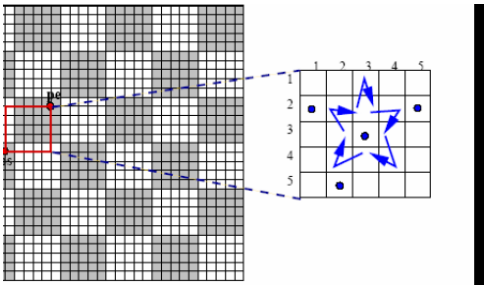


Figure 2.3 Grid Selection [3]

In Cued Recall Based Techniques, the system provides some clues to the users that help users to reenter their passwords with high accuracy. These hints are given as hot spots within an image. The user needs to choose some of these regions to register as the password and will have to choose the same region in the same order to log in. The user must remember the chosen click regions and keep them undisclosed. Blonder scheme and Pass Point scheme are the examples of implementation.

Figure 2.4 Pass Point [1]

In the PassPoint scheme, the user has to choose any 5 different click points on a single image. In the password creation phase, user can select any pixel in the given image as a click point [1],[5]. For every chosen click point, tolerance is calculated. And during the authentication phase, user has to repeat the same sequence of click points. In order

to get authenticated, the user has to click within the tolerance.

III. EXISTING SYSTEM

Cued Click Point was proposed by S. Chiasson et al. with the intention of reducing the hotspot and pattern formation attack [1],[2],[8],[14].

Unlike PassPoint where user has to choose five clickpoints on one image, Cued Click Point offers user to choose one click point on five different images. In Cued Click Point, the preceding click point determines the next image to be displayed. The next image to be displayed also depends on the user specific random value generated by the deterministic function. In this scheme, the password entry becomes a pure cued recall scenario where each image triggers the memory of corresponding click point.

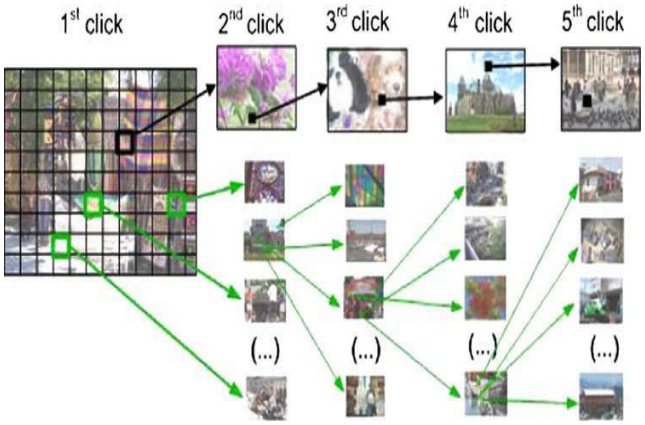


Figure 3.1 Cued Click Point Scheme [14]

3.1 Persuasive Technology

Fogg had coined the term Persuasive Technology, a concept to motivate and influence people to behave in a desired manner. Persuasive Technology when applied in an authentication system ought to guide and encourage users to select stronger passwords, but not enforce system-generated passwords. The users must not ignore the persuasive elements and the resulting passwords must be memorable to make this technique more effective [1],[2].

The path of slightest opposition for users is to select a stronger password that is not comprised entirely of known hotspots or following a predictable pattern. The formation of hotspots is reduced as click points are more randomly distributed. Persuasive Cued Click Point's design follows Fogg's Principle of Reduction by making the task of choosing a strong password easiest. This scheme also follows the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password [1],[2],[12],[13].

IV. PROPOSED SYSTEM

The proposed methodology uses Persuasive Cued Click Points. In the proposed system, the user will be validated based on a set of certain images along with the approximate pixel of the click made by user. This mechanism will enhance the security of the application. The proposed system comprises of following modules.

- User Registration
- Image Password Creation
- Image Password Authentication
- File Transfer

Persuasive Cued Click Point (PCCP) makes use of persuasive technology which encourages the user to select stronger passwords in a more secured way.

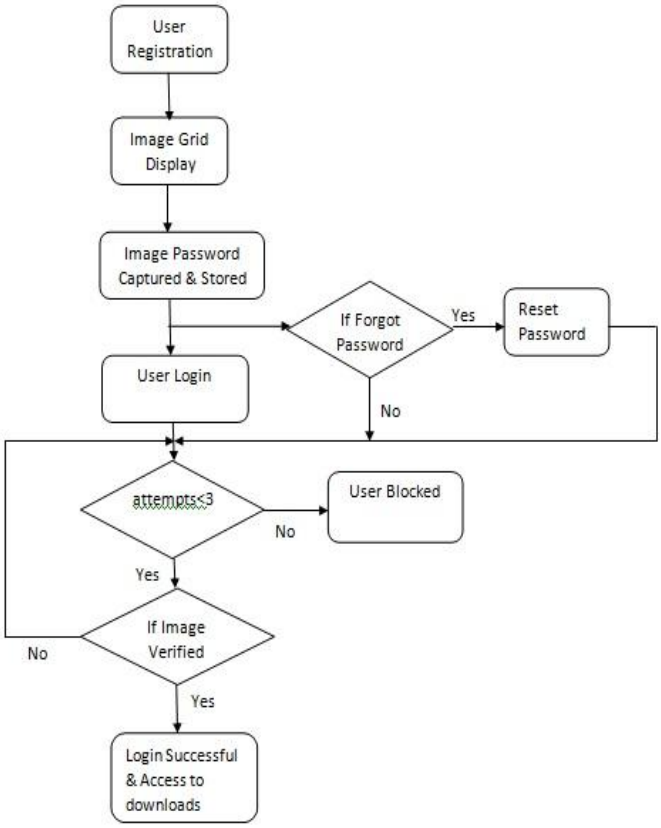


Figure 4.1 Block diagrammatic representation of the proposed system.

The block diagrammatic representation of the proposed system is as given above in the Figure 4.1. The flow begins with the registration process where user must enter details such as name, date of birth, email-ID, and text passwords. On saving the user's personal identification details, it moves on to Image grid display. The image grid has a set of images from which user must choose a sequence for the password. This image password will be captured by the application and stored in the database against the user-ID that is generated on completing registration.

Now, on successfully completing the registration process, user must login providing his/her username, user-ID and text password first. Once logged in, user can choose to download the file that was uploaded by the admin or can edit the account details. To download the file, the user must clear the image authentication process. If the image sequence entered by the user is correct, the user gets access to files, else user has three attempts to enter the correct image password. On third wrong attempt, user's account gets blocked, and user must wait to get the account released.

The other option that a user has is to simply click on the ***Forgot Password*** option, and the user will receive a 7 digit random alphanumeric code to reset the password in the email entered during the registration process.

4.1 User Registration

In the user registration module, the user is prompted to click on the ***new user registration*** button as shown in Figure 4.1a).

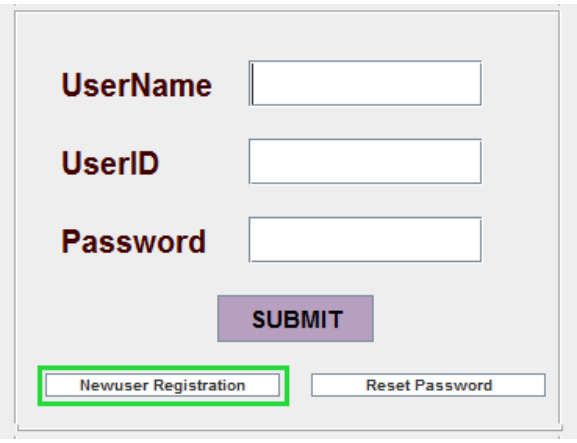


Figure 4.2 a) Login Page

Thereby redirecting the user to a page to fill in personal unique identification details. On clicking the New user Registration button, the system generates a unique user ID assigned to every individual user like mentioned in the below Figure 4.2 b).

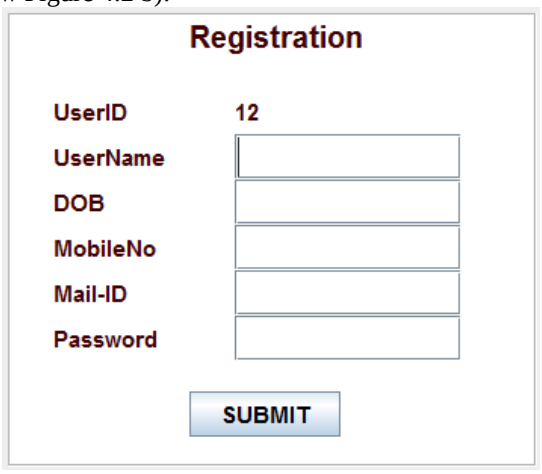


Figure 4.2 b) Registration Page

On submitting the details and the text password, it leads to the next module, where user has to create image password.

4.2 Image Password Creation

In the second module of PCCP, a sequence of images will be displayed to the user to choose a password from. The images from which the user should select the click points for the correct login shall be generated to the user in a random manner in an image grid (Figure 4.2c). The user must select one click point per image during the password creation phase.

Figure 4.2 c) Image grid display

4.3 Image Password Authentication

In the third module, the user must login with *Username*, *UID(generated by the system)* and *text password* to login and view the image grid (Figure 4.2d), to be able to go through the correct sequence of click points.

The user must click on the same images he/she had chosen as the password. And most important it necessarily has to be in the same sequence as chosen while creating the password.

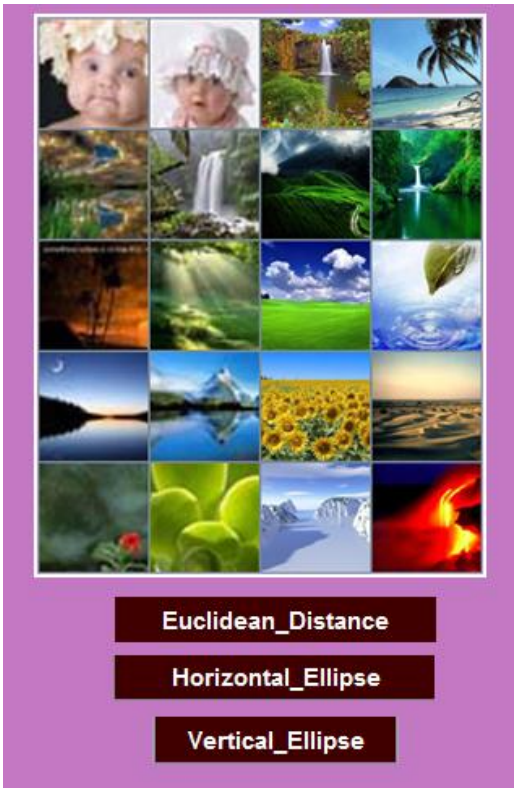


Figure 4.2 d) Image grid display

On clicking the image from the image grid display, the image zooms in giving user a larger view of the picture like in Figure 4.2e). The user can click on the point he/she had chosen as password while password creation. The user must continue the same procedure until all the five images are selected with their respective click-points.

Figure 4.2 e) Image click-point

The click-point in every image chosen refers to x-y coordinates. These coordinates are saved in the database with respect to the images chosen against every user id.
After clicking on the final image and its click-point, the user is given the freedom to choose any of the algorithms.
In our implemented system, we provide user with three algorithms.

- Euclidean Distance
- Horizontal Ellipse
- Vertical Ellipse

From the above algorithms, Euclidean distance is the most feasible solution and a more commonly sought algorithm.

$$r = \sqrt{(x1 - x2)^2 + (y1 - y2)^2} \qquad (1)$$

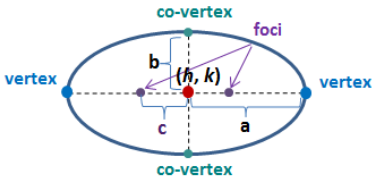
The Euclidean distance is otherwise also called as "Equation of a circle". This formula can be used to find the distance between two points. The logic is to verify if the chosen point lies in a area acceptable with the actual point. In our implemented system, ***r*** is considered as the threshold value and (***x1,y1***) are the ***registered*** coordinates saved in the database during registration process. (***x2,y2***) are the ***login*** coordinates. If the resultant value is less than or equal to the threshold value, then the login coordinates are accepted by the system and user is allowed to login as a legitimate user.

Working: Consider the following coordinates
(**x1,y1**) = (145,132)
(**x2,y2**) = (147,130)

$=\sqrt{(145 - 147)^2 + (132 - 130)^2}$
$=\sqrt{(-2)^2 + (2)^2}$
$=\sqrt{(4) + (4)}$
$= \sqrt{8} = 2.828 < 5$

Therefore, the point lies within the circle with radius, r=5.

To make a comparison, we decided to use an algorithm that has not been used before, as our own contribution. Hence we came up with the idea of using ***Equation of an Ellipse*** for the authentication process.
Ellipse can be of two types, Horizontal & Vertical. The Figures 4.3a) & b) refer to the Horizontal and Vertical ellipse with their respective equations and their major and minor axis.

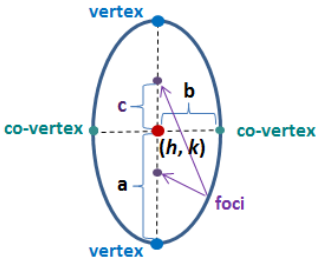


At (0, 0): $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$

General: $\frac{(x-h)^2}{a^2} + \frac{(y-k)^2}{b^2} = 1$

$a^2 - b^2 = c^2$

Figure 4.3 a) Horizontal Ellipse



At (0, 0): $\frac{x^2}{b^2} + \frac{y^2}{a^2} = 1$

General: $\frac{(x-h)^2}{b^2} + \frac{(y-k)^2}{a^2} = 1$

$a^2 - b^2 = c^2$

Figure 4.3 b) Vertical Ellipse

$$\frac{(x-h)^2}{a^2} + \frac{(y-k)^2}{b^2} = 1 \qquad (2)$$

x - registered x-coordinate (*during password creation*)
y - registered y-coordinate (*during password creation*)
h - login x-coordinate
k - login y-coordinate
a - 1st threshold
b - 2nd threshold

In ellipse, we have two radii. The diameters are called as major and minor axis. For this simple reason we have two threshold values unlike in Euclidean distance there was only one.

Working: Consider the following coordinates
(**x1,y1**) = (145,132)
(**x2,y2**) = (147,130)
Say, Major axis = a = 14 ; Minor axis = b = 8;

$$\text{L.H.S} = \frac{(145-147)^2}{14^2} + \frac{(132-130)^2}{8^2} = \frac{(-2)^2}{196} + \frac{(2)^2}{64}$$

$$= \frac{4}{196} + \frac{4}{64} = \frac{1}{49} + \frac{1}{16}$$

$$= \frac{65}{784} \quad = 0.0829 < 1 \text{ (R.H.S)}$$

Therefore point lies within the ellipse. Hence the user clears the authentication procedure and gets access to files.

The time taken by both algorithms varies. Also the complexity would vary. Given the fact that user has options to choose from to authenticate, using Ellipse gives room for user to click at an approximate click point when the user is not very sure of the exact click-point chosen during registration process.

PCCP system will be difficult for attackers to breakthrough as the sequence of image cannot be predicted easily. This method does not alert the user, if the chosen image is erroneous. It will be acknowledged to the user only after the final click point. So the likelihood of guessing the password sequence is meagre. At first, registration process takes place where selection of image sequence will be done. This method of authentication can be applied and prove useful in the banking sector or in any other organization or workplace where security of the system.

V. RESULTS

The empirical study was conducted to investigate ways of increasing the percentage of recognition efficiency and conducted lab studies to compare different algorithms & their time taken for execution.

5.1 Percentage of recognition efficiency

This experiment involved 5 participants. Each participant were asked to participate in registration process where the user must enter the details such as name, date of birth, mobile number, email ID and text password. After which they must choose the image password sequence that consists of five click points on five different images. During each trial, participants were given a set of question on Likert-scale that corresponds to the previously cited studies. Likert-scale is the method of ascribing quantitative value to qualitative data to make it amenable to statistical analysis. In the questionnaire, the Likert Scale is a five (or seven) point scale which is used to allow the individual to express how much they agree or disagree with a particular statement. The below figure 5.1 is the screenshot of the result of survey conducted on recognition efficiency using Likert-Scale.

Users	User1	User2	User3	User4	User5
Questionnaire(5-point scale)					
How easy is to create a Graphical Password?	4	5	5	5	5
Graphical Password is easy to remember	4	4	4	4	3
How many attempts did you make to enter the correct password?	5	5	5	5	4
Overall, are you satisfied with security provided by PCCP mechanism?	4	4	4	4	5
Persuasive Cued Click Points is convenient to use with practice.	4	4	4	5	5
Text Passwords are preferable than Graphical Passwords	1	3	3	5	5

Figure 5.1 Recognition Efficiency (User-Survey)

5.2 Login Success Rate

Login success rate is reported on the first attempt and if successfully logged in within the first three attempts. First attempt is reported to be successful when the user enters the image password correctly on the first try itself, without making an error. If user logs in successfully within first three attempts means user has made lesser than three mistakes, which increases the login success rate. We've used Likert-scale here as well to get a survey from ten participants on how many users could log in successfully on the first attempt (Figure 5.2).

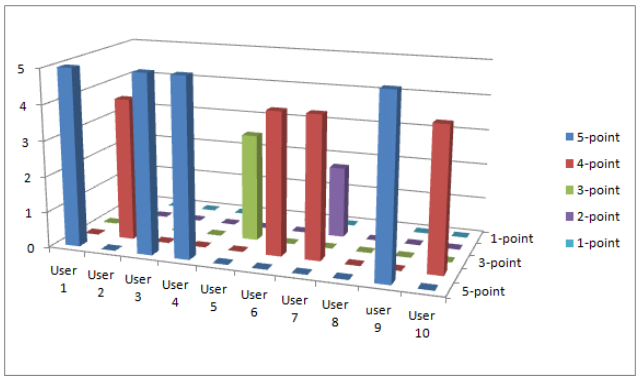


Figure 5.2 Login Success Rate (User-Survey)

5.3 Time taken for execution

Now that we are using three different algorithms here, namely, Euclidean distance, Horizontal Ellipse and Vertical Ellipse, time taken for execution varies from algorithm to algorithm. Initially five participants are considered for the experiment.

Each participant is allowed to register and create image password sequence. Then the participant logs into their respective account using one algorithm at a time.

The execution time is calculated from the point user clicks on the algorithm button to submit password for authentication till the participant views the files to download on successful user login. Based on the time taken for execution by the three algorithms, the data was retrieved from the database and the following result is represented using a bar graph like shown in Figure 5.3

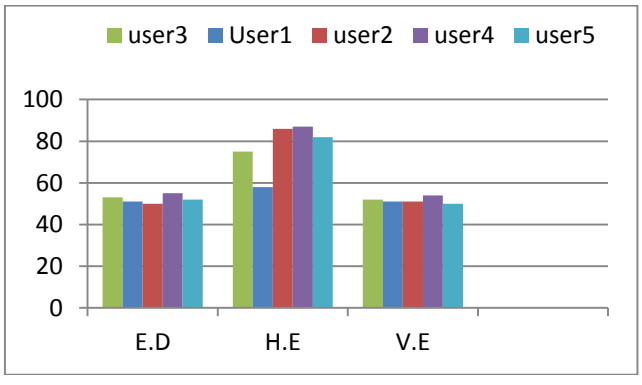


Figure 5.3 Time taken by algorithms for execution

x-axis – algorithms;
y-axis – Time (in milliseconds)

VI. CONCLUSION

We have implemented a password based authentication that can provide more security to effectively increase the password space, login success rate and security. This can be obtained in the proposed system using user choice and has been implemented using Persuasive Cued Click Points. This technique will be very much appropriate for places where high level security is requisite.

A core aspect in PCCP is that creating a harder to guess password is the path of least resistance. This can be achieved in this method, possibly making it more effective than other schemes where secure behaviour adds further burden on users.

This system will be tricky for attackers where the sequence of image cannot be predicted easily. This method will not provide any alert message or acknowledge the user, if the chosen image is wrong. It will be known to the user only after the final click point. So the chance of guessing or predicting the progression is very low. This security system can be preferred in organizations where high security is required. Without clearing the authentication process the user may not be able to access the system.

VII. ACKNOWLEDGMENT

I express my sincere thanks to my project guides Prof.V.B. Gaikwad and Prof. Alka Khade of Computer Department for their guidance and supervision, assisting with all kinds of support and inspiration, excellent guidance and valuable suggestions throughout this investigation, preparation and implementation of this project.

REFERENCES

[1] Uma.D.Yadav, Prakash.S.Mohod ,"Adding Persuasive feautures in Graphical Password to Increase the capacity of KBAM", *2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology*, 2013

[2] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. van Oorschot, "Persuasive Cued Click Points: Design, Implementation, and Evaluation of a Knowledge Based Authentication Mechanism" , *IEEE Transactions on Dependable and Secure Computing, Vol.9, No.2, March/April 2012*.

[3] Ashwini Fulkar, Suchita Chawla, Zubin Khan, And Sarang Solanki, " A study of Graphical Passwords and various Graphical Authentication Schemes", *World Research Journal of Human Computer Interaction*, 2012.

[4] Wei Hu, Xiaoping Wu, Guoheng Wei, "The security analysis of Graphical Passwords", *2010 International Conference on Communications and Intelligence Information security*, 2010

[5] Paul C. van Oorschot, Amirali Salehi-Abari, Julia Thorpe, "Purely Automated attacks on PassPoints Style Graphical Password", *IEEE Transactions on Information Forensics And Security*, September 2010.

[6] Farnaz Towhidi, Maslin Masrom, "A Survey on Recognition-Based Graphical User Authentication Algorithms", *International Journal of Computer Science and Information Security*, Vol.6, No.2, 2009.

[7] S. Chiasson, P. C. van Oorschot, and R. Biddle, "A second look at the usability of click-based graphical passwords," in *Proc. 3rd Symposium of Usable Privacy and Security* , Pittsburgh, PA, 2007.

[8] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Proc. Eur. Symp. Research in Computer Security*, Dresden, Germany, 2007.

[9] Mohammad Sarosh Umar, Mohammad Qasim Rafiq and Juned Ahmad Ansari, "Graphical User Authentication: A Time Interval Based Approach", IEEE Conference, 2012.

[10] Gaurav Agarwal, Saurabh Singh, Ajay Indian," Analysis of knowledge based graphical password authentication", *The 6th International conference on Computer Science and Education*, August 2011.

[11] Susan Weidenbeck, Jim Waters, Jean Camille Birget, Alex Brodskiy, Nasir Memon, "*Authentication using Graphical Passwords*".

[12] Karthhik.K, Keerthana.R, Porkodi.A, Udhayakumar.S, Kesavan.S, Mr.Balamurugan.P, "Defenses against large scale online password guessing by using persuasive cued click Points", *International Journal of computer Science and Mobile Computing*, 2013.

[13] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better, passwords: Persuasive cued click-points," in *Proc. HCI, British Computer Society*, Liverpool, UK, 2008.

[14] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," *International Journal of Information and Security*, vol. 8, no. 6, 2009.

AUTHORS

Shilpa Veerasekaran received the B.E degree in Computer Science and Engineering from Erode Sengunthar Engineering College affiliated to Anna University, Chennai in 2009 and is currently pursuing M.E. degree in Computer Engineering from Terna College of Engineering affiliated to Mumbai University.

Prof. V.B Gaikwad has received B.E. degree in Computer Engineering & M.E. degree in (Computer Science and Engineering) from Walchand College of Engineering, Sangli, Shivaji University in 1997 & 2004

Prof. Alka Khade has received the B.E degree in Electronics from PDVVP College of Engineering affiliated to Pune University, and M.E degree in E/T from Terna Engineering College, affiliated to Mumbai University in 1994 and 2008 respectively. She is currently working in Terna Engineering College.