Graphical Authentication Based Techniques

V. Bhusari

College of Computer Engineering, JSPM, BhivarabaiSawant Institute of Technology and Research (W),
Pune-411043, India
Corresponding Author Email: **vrundabhusari82@gmail.com**

Abstract- The password techniques used in market are very insecure. The textual passwords which we normally use suffer with both security and usability problems. Therefore in this extended abstract, we have discussed different graphical password authentication systemssuch as Cued Click Points (CCP), a cued-recall graphical password technique and other techniques which uses sound signature for password authentication.Various techniques for password authentication have been discussed in details.

***Keywords*-**CCP; pass points;POI.

I. Introduction

User authentication is a most important component in most computer security. It provides user with access control and user accountability [1]. As we know there are many types of user authentication systems in the marketbut alphanumericalusername/passwords are the most common type of user authentication. They are many and easy to implement anduse. Alphanumerical passwords need to satisfy two requirements. First and foremost requirement is they should be easily remembered by a user, while they should be hard to guess by fraudulent person [2]. If short passwords are used then they are easily guessableand are target of dictionary and brute-forced attacks [3, 4, and 5]. Whereas if strong passwords are enforced a policy sometimes leads to an opposite effect, as a user may write his or her difficult-to-remember passwords on notes or on the notepad and if seen by some other user exposes it to direct theft that is misuse can be done.

The textual passwords used are easily guessed. To sort out these problems the market was provided with techniques like OTP (One Time Password). But the OTP password is provide by token devices. These token devices are very expensive. It has normally been told to use an easy to remember long phrases (passphrase) rather than a single word [6].

Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords [7]. The selection of regions from an image can be done rather than typing characters as in alphanumeric password approaches.Graphical passwords are better alternative than the traditional alphanumeric passwordsas memorization of pictures is easier than words. So other systems which we have discussed have been developed to overcome the problems of predefined regions, predictable patterns and password attacks, a new method called Cued Click Points (CCP) is a proposed as an alternative to PassPoints. In addition selection of the sound signature can be done corresponding to each click point which can be used by the user in recalling the click point on an image.

II. RESEARCH ELABORATIONS

Graphical Passwords

As discussed earlier the graphical passwords uses images (also drawings) as passwords and are easy to remember, as humans remembersimages better than words [8]. Moreover the passwordhas to be more resistant to bruteforce attacks as the search space is infinite [7].

Basically the graphical passwords techniques are dividedinto: recognition-based and recallbasedand cued recall graphical techniques [7, 9]. In recognition-based techniquesa user chooses images during the registration stageand is said to be anauthenticated user only when he/ she identifies one or more images. In recall-based techniques, a user selects images during the registration and is askedto reproduce something that he or she created during the registration phase.Passfacescomes under the recognition-based technique in which a useris authenticated if he/she is able to recognizehuman faces [10]. An early recall-based graphical passwordapproach was introduced by Greg Blonder in 1996 [11].In this approach, a user creates a password by clicking onseveral locations on an image during the registration phase. During authentication phase, theuser must click on those locations only then he/she is said to be the authenticated user or else is said to be fraudulent.

Graphical Based Authentication Technique

In Graphical Based Authentication Technique, a user creates a password by first entering a picture he or she chooses at the time of registration. The pictures are stored in the database. As soon as the option of pictures is clicked they are retrieved from the database and are displayed to the user. The user chooses one of the images from number of images and then chooses several point-of-interest (POI) regions in the image. Each POI, is described by a circle (center and radius). For eachPOI theuser types a word or phrase whichwill be combined with POI. If the user does not type any text after selecting POI then that POI is combined with an empty string. The user can choose either to enforcethe order of selecting POIs (stronger password), or to makethe order insignificant [12].

For example if a user creation ofgraphical password has to be done. The user chooses apicture of his or her parents by pressing "Load Image button".Then the user clicks on the parents faces suppose clicks are done in the order of theirages (order is enforced). For each of the selected region, the usertypes the parents name or nickname. This is done under registration. Now for authentication or for login, the user first enters his or her username. Then thedisplay of the image stored in the database during registration phase is done. Now the user has to correctly pick the POIsand typethe same words which were selected and typed during registration phase. At any time, typed words are eithershown as asterisks (*) or hidden [12].

The advantages of this system are that, a free selection of picture from number of pictures can be done by user,POIs and corresponding words. If strong authentication is the main criteria then the order and number ofPOIs can be kept has one of the main constraints.Together,these parameters allow for a very large password space.The next advantages arethat:

- Combination of graphical and text-based passwords is done and triedto achieve the best of both worlds.
- It provides multi-factor authentication (graphical, text,POI-order, POI-number) in a friendly intuitive system [12].

Various methods of graphical Password Authentication Techniques

As said earlier graphical password schemes can be grouped into three general categories: recognition, recall, and cued recall [7, 8]. Recognition based password is the easy technique for human memory whereas pure recall is most difficult as the information must be accessed by user with no triggers. Cued recall falls somewhere between the two as it offers a cue which should establish context and trigger the stored memory [13].

Among existing graphical passwords, CCP is almost close to Passfaces [14], Story [9], and PassPoints [19, 20].In implementation it is most similar to PassPoints.Passfaces [14] is a graphical password scheme based on recognizing human faces. During password creation, selection of a number of images from a larger set is done by the user. To log in, users must identify one of their pre-selected images from amongst several decoys. Users must correctly respond to a number of these challenges for each login.

Davis et al. [9] implemented own version called Faces and conducted a long-term user study. Results showed that users could accurately remember the images but disadvantage was that the user-chosen passwords were predictable to the point of being insecure.Therefore Davis et al. [9] proposed a scheme calledStory which used everyday images instead of faces and also required that users select their images in the correct order. Users needed create a story in their memory. But the disadvantage with this was that it was somewhat worse than Faces for memorability [9], but user choices were much less predictable.

The idea of click-based graphical passwords originated with Blonder [11] who proposed a scheme where a password consisted of a series of clicks on predefined regions of an image. Later, Wiedenbeck et al. [15, 16] proposed PassPoints, wherein passwords consisted of several (e.g., 5) points which could be anywhere on an image.

Cued Click Points (CCP)

As seen in the earlier methods the user has to choose the click points in the same image and is also insecure in security point of view. So the CCP technique was introduced.Whereas CCP password consists of one click-point per image. That is in the graphical based authentication technique the user has to remember many points in one image and this is the major disadvantage of graphical password authentication technique.

In the CCP technique the usersare required to rememberonly one point in one image. The images are stored in the database as in the earlier methods too. This is done for a sequence of images. That is the user has to do the selection in sequential order only that is in the same order in which he or she did during registration.The next image is displayed only when the user clicks on the click point of previous image correctly. So the users receive immediate implicit feedback whether they are on the correct track or not when logging in. So the Cued Click Pointstechnique not only improves usability but also security. The observation for this method was that selecting and remembering only one point per image is much simpler or easier. Moreover seeing each imagetriggers theuser's memory of where the corresponding point was located. The CCP technique provides higher security than PassPoints asthe number of images increases the workload for attackers [14]. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning) [13].

So each right click results in showing a next-image, in effect leading users down a "path" as they click on their sequence of points. That is if suppose during the registration phase five images were chosen that is five points were chosen then the user has to choose the images in the same sequence. The user can go the second image only when he chooses the first image click point correctly. Similarly the user can go to third only when he chooses last two image click points correctly. At last, the user goes to last that is fifth only when he chooses last four image click points correctly. A wrong click leads down an incorrect path and the indication is given explicitly by the system about the authentication failure. If the user dislikes the resulting images, creation of a new password involving different click-points could be done to get various images. [13].

In CCP a user has a client device (which displays the images) to access an online server (which authenticates the user). Through SSL/TLS the images are stored server-side with client communication. It initially functions like PassPoints. A method called discretization is used to find a click-point's tolerance square and corresponding grid during the creation of password. This grid is retrieved from the database and used to find if the click-point falls within tolerance of the original point and this is done for each click-point in a subsequent login attempt. With the help of CCP, we further need to find which next-image to display.

Suppose for example if we take images of size 451x331 pixels and tolerance squares of 19x19 pixels. If we used robust discretization, we would have 3 overlapping candidate grids each containing approximately 400 squares and in the simplest design, 1200 tolerance squares per image (although only 400 are used in a given grid). A function f (username, currentImage, currentToleranceSquare) is use which uniquely maps each tolerance square to a next-image. A minimum set requirement of 1200 images is suggested at each stage. There may be an argument against fewer images and having multiple tolerance squares map to the same next-image, that this could result in misleading implicit feedback in (albeit rare) situations where users click on an incorrect point yet still see the correct next-image [13, 17].

Each 1200 next-images would have 1200 tolerance squares and thus require 1200 next-images of them. With this the number of images would quickly become large. So re-using the image set across stages is done. By reusing images, there is a slight chance that users see duplicate images. During 5 stages in the password creation, the image indices a1,..,a5 for the images in the password sequence are each in the range 1 _ ab _ 1200. When computing the next-image index, if any is a repeat (i.e., the next ab is equal to ac for some c < b) then the next-image selection function f is deterministically perturbedto select a distinct image [13, 17].

The system selects user's initial image based on some user characteristic (like an argument to f above we have used username). Each time a user enters the password the sequence is re-generated from the function. If an incorrect click-point is entered by the user, then the sequence of images from that point onwards will be incorrect and thus the login attempt will fail. This cue will not be helpful for an attacker who does not know the correct sequence of images.

A major usability improvement over PassPoints is the fact that legitimate users get immediate feedback about an error when trying to login. When incorrect image is seen by the user he/she understands that the latest click-point was incorrect and can immediately cancel the attempt and try again from the beginning [13]. Another usability improvement is that being cued to recall one point on each of five images appears easier than remembering an ordered sequence of five points on one image.

The following are the steps which have to be followed in CCP:

Password creation phase: The point selection has to be done on each of the image. That is if there are five images first point will be selected on first image, second point will be selected on the second image and so on. That if a user wants to create a password he has to perform this step [13].

Confirm phase: Confirmation of password is done by re-entering it once again. If the password typed is incorrect then the user has to return to step 1. Even if a new password is started with the same initial image, but generally includes different images thereafter, depending on the click-points [13].

MRT: Complete a Mental Rotations Test (MRT) puzzle [10]. A paper based task is given to the user to distract him/her for a minimum of 30 seconds. It is generally a visual task in order to clear his/her working memory [13].

Login phase: Now if the user wants to Log in he/she must know ID and password. The user can cancel the login attempt and try again if an erroris noticed by the users during login. The creation of the new password can be done, by returning to Step 1 of the trial with the same initial image as a starting point if the user doesn't remember the password. The user could skip this trial and move on to the next trial if he/she feels too frustrated with the particular images to try again [13, 18].

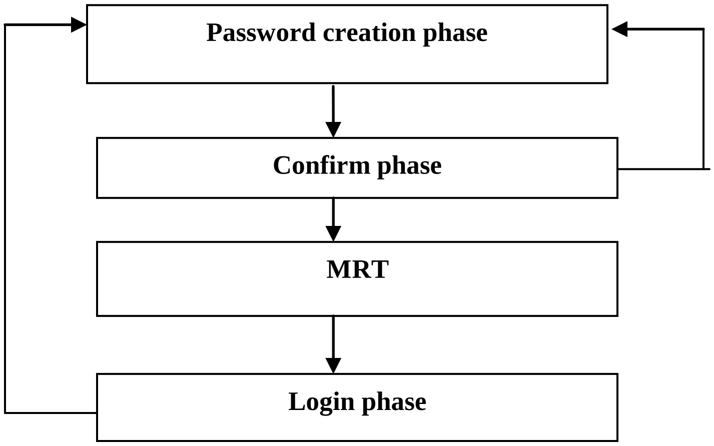


Figure 1: Cued Click Points Steps

Cued Click Points with sound signature

Previously we have seen different graphical authentication techniques. In CCP we just used to click one point in one image and this is done for number of images as discussed previously. But in the CCP with sound signature we also have go select sound as a signature as this will provide the user with better authentication. The sounds of different birds or animal or the user’s preferable sound will be stored in the database. Then when the user chooses the points in each image after this the user is asked to select the 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. That is here a graphical password system with a supportive sound signature helps to increase the remembrance of the password is designed. Verygood performance has been shown by the system in terms of ease of use, speed and accuracy. Users preferred CCP as compared to Pass Points, as remembering only one point per image was easier and sound signature helped them considerably in recalling the click points [19].

As this system has been integratedwith sound signature it helps in recalling the password. It has been said that sound signature or tone can beused to recall facts like images, text etc[19, 20]. In daily life we seevarious examples of recalling an object by the sound related tothat object [19, 20]. Our idea is inspired by this novel humanability.

The system creates user profile as follows-
Master vector User ID, Sound Signature frequency, Tolerance
Detailed Vector Image, Click Points

Steps in Cued Click Points with sound signature

Registration Process

As shown in the fig.2 if the user doesn’t have the id and password then he needs to register himself/herself or create a new id. So if the user doesn’t have id he will get a unique user id and password. After the selection of id he/ she need to select sound signature.The user also needs to select the tolerance level [21]. After this the user selects the image and click on pass point. This is saved in the database.The sound frequency is selected. A tolerance value is selected which will decide that the user is authenticated or fraudulent and the same sound frequency is selected which he/she wants to be played at login time To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is also created [19].

Now the system asks whether the user wants to select more images or not. If the user clicks on no then the data gets stored in the database and the user is asked if he/ she wants to continue or not. If the user click yes then again the user has to select the next image and click on the pass point and again the system will ask whether the user wants to select the next image or not. This can be done five times if we have kept the limit of five.

In this system user has to remember the click point’s for each image. Also user need to upload the images by own. The user needs to remember the click points as well as the images very well. If he/she fails to remember then user will not be allowed to perform the login session. The user also needs to remember the path that the sequence of the images clicked as password otherwise he/she fails to perform the login session.

After creation of the login vector, system calculates the Euclidian distance between login vector and profile vectors stored. Euclidian distance between two vectors **p(x, y)** and **q(a,b)** is given by-

$$\boxed{\mathbf{D\ ((x,\ y),\ (a,\ b)) = \surd(x - a)^{2} + (y - b)^{2}}}$$

Above distance is calculated for each image if this distance comes out less than a tolerance value D. The value of D is decided according to the application and may be also selected by the user.

At last the user profile vector will be created and stored in the database so that the information can be used if a user login the system.

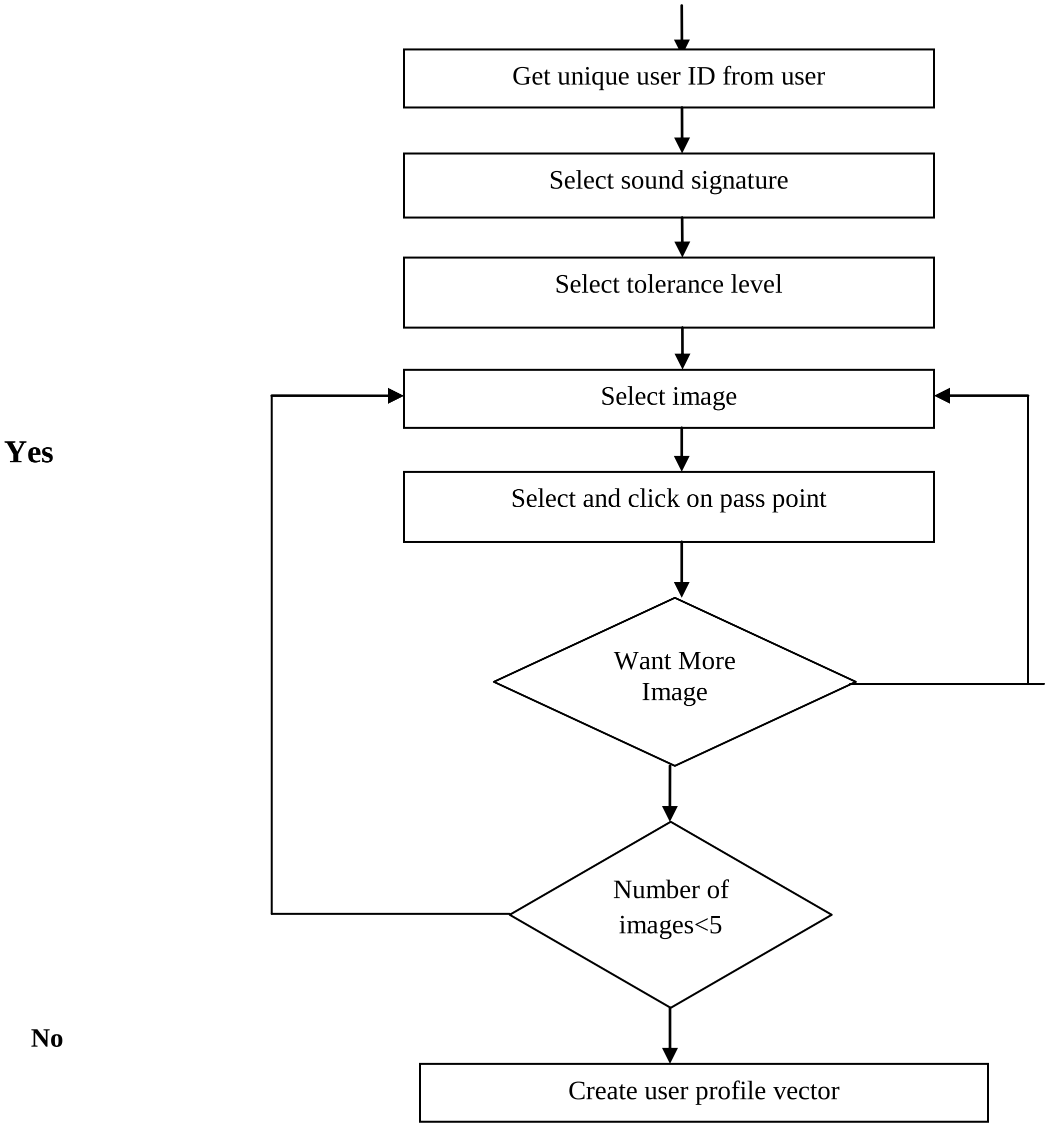
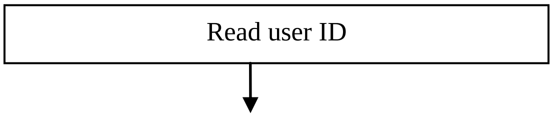


Figure 2: Registration Phase of Cued Click Points with sound signature

Login

This is the next phase after the registration has been done. Login is allowed to be performed only when the user is registered user otherwise first he has to register himself/herself first and then he/ she can perform the login.



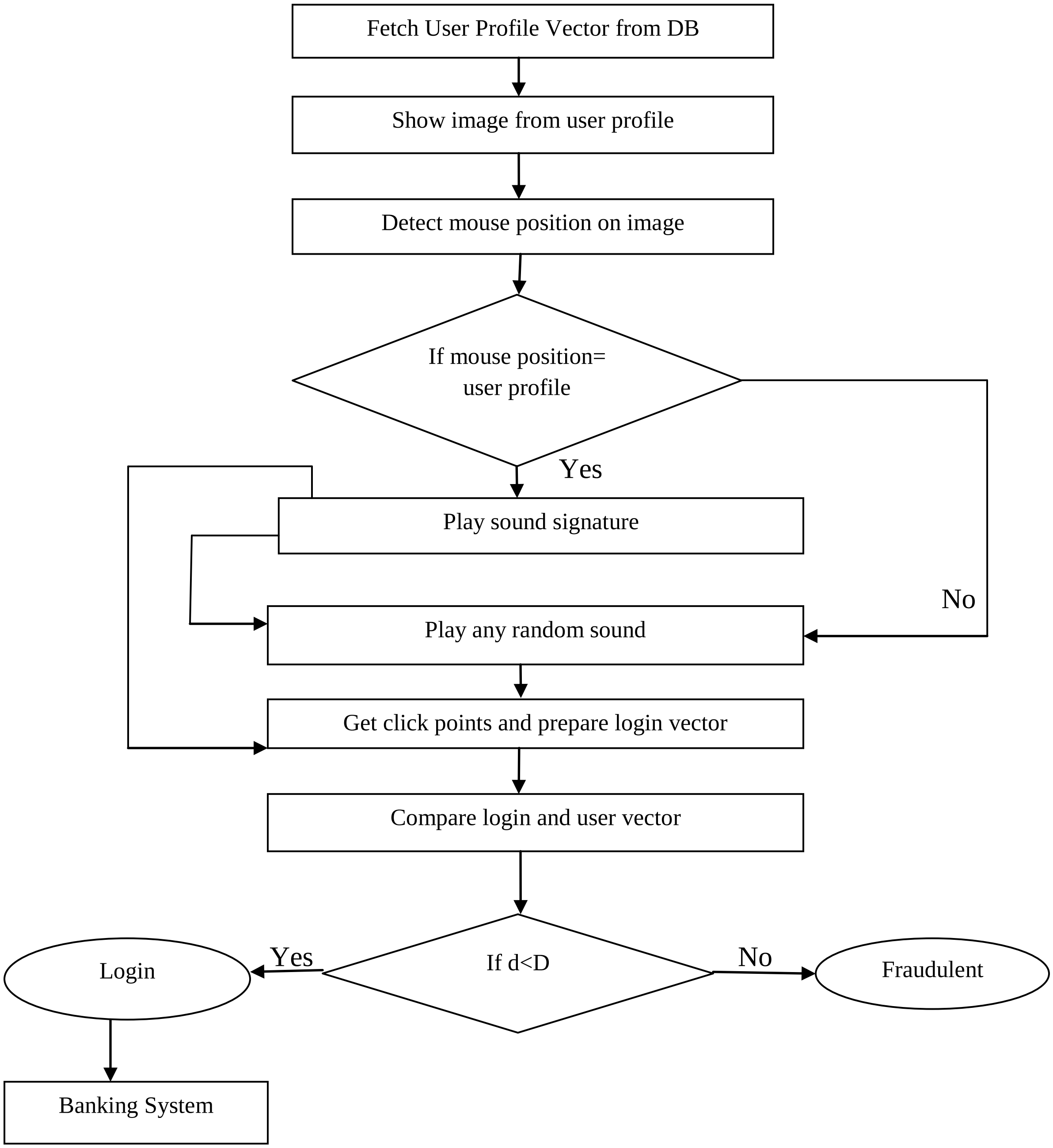

Fetch User Profile Vector from DB
Show image from user profile
Detect mouse position on image
If mouse position= user profile
Yes
No
Play sound signature
Play any random sound
Get click points and prepare login vector
Compare login and user vector
If d<D
Yes
No
Login
Fraudulent
Banking System

Figure 3: Login phase of Cued Click Points with sound signature

Now once the registration has been done by the user and he/she does the login. First of all theuser ID is read. Then the user profile vector is stored in the database during the registration phase so it is fetched from the database. The image which is selected during registration phase is retrieved from the database and the image is displayed.The user needs to select the same points which he chooses during the registration phase [22]. The user also has to select the same position which he selected during the registration phase. If suppose the mouse position is equal to user profile then the sound signature is playedand the click points are obtained and the preparation of login vector is done. Now the comparison of login and user vector is done. If d<D then the login is successful and the user is assumed to be the authorized person else the user is assumed to be fraudulent. If the user is authenticated then he is allowed go into the banking module. If mouse position is not equal to user profilethen the random sound is played then the user obtains the click points and prepare login vector. Then comparison of login and user vector is done.

Banking system

The user can access this module only if his user id and the password are correct that is only the authenticated user is allowed to perform this session. In this module various operations could be performed such as Net Banking Menu, Account Menu, Creating New Account, Update Personal Details, Pin code Generated, View Account Details, Transaction, Loan Request, View Loan Details etc [23].

After typing the correct username and password the user will be transferred to the banking module where he/she has to choose one of the options from all the given options. The various options are loan, account, transaction, personal details and sign out. If the user wants to open a new account he/she has to click on accounts option under which there are two options. First is new account and second is glance on account details [24]. If the user clicks on the open account option then he/she can open new account and if he/she wants to just view the account details then he/she can click on the option glance on account details. If the user wants to fill up all the user personal details then the user has to go to personal details option and fill up the details.If the user wants to perform the transaction he/she has to put account number and the pin number and click the submit button.If the user wants to request for the loan he can do so by clicking on the loan option and then apply for the loan.If the loan details have to be viewed by the user it can be viewed by the user by clicking the option loan details.If the user forgets the password of his/ her account he/she has to choose the option forget password. After clicking on the option security question will be displayed which the user has to answer.After answering the question correctly the password is be sent on the mail id.

Comparison of alphanumeric password authentication systems and graphical password authentication systems

Alphanumerical username/passwords are the most common type of user authentication while graphical passwords are not much in use. But day by day the use of graphical password is increasing. Alphanumeric passwords are easy to implement and use and also graphical passwords are easy to implement and use. The requirement of the alphanumeric passwords is that they should be easily remembered by a user, while they should be hard to guess by fraudulent person [2]. These both requirements are for graphical passwords too and it gets satisfied as remembering images are much easier than remembering textual passwords. If short passwords are used then they are easily guessable and are target of dictionary and brute-forced attacks [3, 4, and 5]. Whereas if strong passwords are enforced a policy sometimes leads to an opposite effect, as a user may write his or her difficult-to-remember passwords on notes or on the notepad and if seen by some other user exposes it to direct theft that is misuse can be done. Whereas is graphical passwords are used these all problems do not arise.

Comparison of OTP systems and graphical password authentication systems

The first and foremost advantage of OTP is that the user doesn’t need to remember the password it is directly sent to the user to his / her mobile or email, while the graphical passwords are required to be remembered though remembering them is easy because human brains can easily remember images. But the OTP password is provided by token devices andthese token devices are very expensive. While providing graphical passwords is not expensive and doesn’t need any device for generation.

Comparison of Cued Click Points (CCP) and Cued Click Points with sound signature

In CCP password consists of one click-point per image. That is in the CCP technique the users are required to remember only one point in one image. The images are stored in the database as in the earlier methods too. This is done for a sequence of images. That is the user has to do the selection in sequential order only that is in the same order in which he or she did during registration. The next image is displayed only when the user clicks on the click point of previous image correctly. So the users receive immediate implicit feedback whether they are on the correct track or not when logging in. So the Cued Click Pointstechnique not only improves usability but also security.

Previously we have seen different graphical authentication techniques. In CCP we just used to click one point in one image and this is done for number of images as discussed previously. But in the CCP with sound signature we also have go select sound as a signature as this will provide the user with better authentication. The sounds of different birds or animal or the user’s preferable sound will be stored in the database. Then when the user chooses the points in each image after this the user is asked to select the 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. That is here a graphical password system with a supportive sound signature helps to increase the remembrance of the password is designed. Very good performance has been shown by the system in terms of ease of use, speed and accuracy.

The observation for this method was that selecting and remembering only one point per image is much simpler or easier. Moreover seeing each image triggers the user’s memory of where the corresponding point was located. The CCP technique provides higher security than PassPoints as the number of images increases the workload for attackers [14]. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning) [13].

Users preferred CCP as compared to Pass Points, as remembering only one point per image was easier and sound signature helped them considerably in recalling the click points [19]. And if the system has been integrated with sound signature it helps in recalling the password. It has been said that sound signature or tone can be used to recall facts like images, text etc [19, 20]. In daily life we see various examples of recalling an object by the sound related to that object [19, 20]. The system creates user profile as follows-

Master vector	User ID, Sound Signature frequency, Tolerance
Detailed Vector	Image, Click Points

IV CONCLUSION AND FUTURE WORK

Various techniques for graphical authentication was discussed and found that the graphical authentication is much more useful than the other types of authentication techniques. It is also very easy to use than the alphanumeric password or OTP technique. Due to the use of graphical based techniques a brute force attack are avoided and is the most important advantage of graphical based password. In the CCP technique the users are required to remember only one point in one image and the next image is displayed only when the user clicks on the click point of previous image correctly. A graphical password system with a supportive sound signature is much more helpful as it helps to increase the remembrance of the password and has shown very good performance.

IV. REFERENCES

[1] W. Stallings, L. Brown, “Computer Security: Principle and Practices”, Pearson Education, 2008.
[2] S.Wiedenbeck, J. Waters, J.C.Birget,A.Brodskiy, N. Memon, “Passpoints: design and longitudinal evaluation of a graphical password system”,*International Journal of Human-Computer Studies*, vol. 63,2005, pp.102–127.
[3] R. Morris, K. Thompson,“Password security: a case history”,*Communications of the ACM*, vol. 22, 1979, pp. 594–597.
[4] D.V. Klein, “Foiling the Cracker: A Survey of, and Improvements to, Password Security”, In *Proceedings of the 2nd USENIX UNIX Security Workshop*, 1990.
[5] E.H. Spafford, “Observing reusable password choices”, In *Proceedings of the 3rd SecuritySymposium.Usenix*, 1992, pp. 299–312.
[6] S.N. Porter,” A password extension for improved human factors”,*Computers & Security*, ed. 1, vol. 1,1982, pp. 54– 56.
[7] X. Suo, Y. Zhu, G.S, “Owen. Graphical passwords: A survey”,*In Proceedings of Annual Computer Security Applications Conference*, 2005, pp. 463–472.
[8]A.D.Angeli, L.Coventry, G.Johnson, K.Renaud,”Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems”*International Journal of Human-Computer Studies*, vol.63, 2005, pp.128–152.
[9] D. Davis, F. Monrose, M.K. Reiter, “On User Choice in Graphical Password Schemes”,*13th USENIX Security Symposium*, 2004.
[10] Real User Corporation, “The science behind passfaces”, 2004.
[11] G. E. Blonder,“Graphical password. U.S. Patent 5559961, Lucent Technologies”, Ed. NJ: Murray Hill, 1995.
[12]A. Almulhem,A Graphical Password Authentication System, 2011, pp. 223-225.

[13] S. R. Chiasson, R. Biddle, P.C. van Oorschot,” A Second Look at the Usability of Click-based Graphical Passwords.ACM SOUPS”, 2007.
[14]Passfaces, http://www.realuser.com Last accessed 2006.
[15]S. Wiedenbeck, J.C. Birget, A. Brodskiy,N. Memon,”Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. ACM SOUPS”, 2005.
[16]S. Wiedenbeck,J. Waters, J.C. Birget, A. Brodskiy, N. Memon,”PassPoints: Design and longitudinal evaluation of a graphical password system”,*International Journal of Human-Computer Studies*, 2005, vol. 63, pp.102-127.
[17]J. C. Birget, D. Hong,N. Memon, “Graphical Passwords Based on Robust Discretization. IEEE Trans. Info. Forensics and Security”, 2006, ed.3, vol.1.
[18] K. Renaud,“Evaluating Authentication Mechanisms” Chapter 6 in [4].
[19]S. Singh, G. Agarwal,“Integration of Sound Signature in Graphical Password Authentication System”, *International Journal of Computer Applications*, ed. 9, vol. 12.
[20] R. N. Shepard, "Recognition memory for words, sentences, and pictures",*Journal of Verbal Learning and Verbal Behavior*, vol. 6, 1967, pp. 156-163.
[21] Vienna, Austria: ACM, 2004, pp. 1399-1402.
[22]Graphical Passwords. ACM SOUPS, 2007.
[23]Cranor, L.F., S. Garfinkel. Security and Usability.O’Reilly Media, 2005.
[24] Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

AUTHOR

Prof. Vrunda KishoreBhusari
Qualifications: M.Tech. (Computer), B.E. (Computer)
College: College of Computer Engineering, JSPM, BhivarabaiSawant Institute of Technology and Research (W),
Pune-411043, India
Corresponding Author Email: **vrundabhusari82@gmail.com**