OVERCOMING LOW SECURITY THROUGH GRAPHICAL PASSWORD AUTHENTICATION TECHNIQUES

HUSSAIN
RESEARCH SCHOLAR
Research Scholar
SHRI JJT UNIVERSITY
Rajasthan

ABSRTACT:

Graphical passwords provide a promising alternative to traditional alphanumeric passwords. they may be appealing given that humans generally recollect images better than phrases. In a cutting-edge time, the greatest prominent user authentication machine which is appreciably makes use of the out-dated approach. It comprises of "username" and "password", which is commonly thru text. This system has honestly found out negative aspects which can not be overlooked. but, strong text passwords are hard to remember, thus the customers incline to write them down or try to shop them on as files on digital approach. Now, numerous laptop systems, networks and net based condition are demanding the use of graphical authentication method. therefore, base of an authentication gadget is to stimulate users to select more healthy password, which increases protection, usability and also refining the password space.

KEYWORDS: *Graphical passwords, Alphanumeric passwords, Graphical authentication.*

INTRODUCTION:

structures like conventional password structures consisting of word based password system, graphical gadget are generally used for authentication. but those systems are at risk of dictionary assault, shoulder browsing attack, accidental login. consequently the phrase-based totally Shoulder browsing resistant graphical password schemes have been proposed. The shoulder browsing assault is an assault wherein unlawful person can get legal consumer's password by using watching over his shoulder when he enters his password. although, as maximum handlers are greater conscious with word-based passwords than graphical passwords . the existing phrase-based totally shoulder surfing resistant graphical password structures are not secured and powerful sufficient any other vulnerability assault regarding textual password is prime loggers. In Key loggers any key pressed by the consumer is monitored with the aid of unauthorized customers. A key logger can be both software program or hardware. with the aid of the usage of Key logger a person can scouse borrow the victim's private statistics, transmission may be interrupted by way of hackers, it can prove very risky for those who are using online cash websites, or whilst they're typing their passwords. In diverse proposed device, the consumer can genuinely and successfully login to the gadget with out the usage of any keyboard. it's far very cozy for the consumer to login. It has grow to be very tough to bet the password because of textual content and coloration combination. The structures offer greater protection.

most of the authentication system now-a-days uses a combination of username and password for authentication. due to the limit of human memory, most users incline to select brief or simple passwords which can be clean to take into account. Graphical passwords use snap shots instead of phrase-primarily based passwords and are comparatively inspired via the fact that customers can don't forget pictures more clearly than a string of characters. A graphical password is an validation technique wherein the person ought to pick from photographs, in a certain order, reachable in a graphical person interface. Graphical passwords may additionally provide improved security than phrase-based passwords due to the fact numerous individuals, in an attempt to do not forget word-based totally passwords, use simple words. In diverse proposed systems one time passwords are used for protection purpose. An OTP is a hard and fast of characters which can act as a shape identification for one time best. as soon as the password is used, it can't be used for any extra authentication. even though the hacker receives the password, it is viable that it turned into formerly used once, because it was being conveyed, consequently unusable to the hacker. some other way used for supplying increased security is consultation passwords. consultation passwords are passwords which are used only as soon as. while the session is completed, the consultation password is no greater beneficial. For each single login technique, customers input diverse passwords. The session passwords offer higher security in opposition to dictionary and brute force assaults as password changes for each consultation. The planned authentication systems use text and colors for generating session passwords.

Banking system:

The person can get admission to this module simplest if his person identity and the password are accurate this is most effective the authenticated consumer is allowed to perform this consultation. in this module numerous operations can be done along with net Banking Menu, Account Menu, creating New Account, update personal info, Pin code Generated, View Account details, Transaction, mortgage Request, View loan info and so forth. After typing the correct username and password the user might be transferred to the banking module where he/she has to pick one of the options from all of the given options. The various alternatives are loan, account, transaction, non-public info and sign out. If the user wants to open a brand new account he/she has to click on on accounts option underneath which there are options. First is new account and second is look on account details. If the user clicks on the open account option then he/she will open new account and if he/she desires to just view the account information then he/she will click on on the choice look on account information. If the person desires to refill all of the user non-public information then the person has to go to personal information choice and fill up the information. If the consumer wants to perform the transaction he/she has to position account wide variety and the pin quantity and click the submit button. If the consumer wants to request for the loan he can achieve this through clicking on the loan choice and then practice for the mortgage. If the loan information have to be viewed via the user it could be viewed by the consumer by means of clicking the choice loan information. If the user forgets the password of his/ her account he/she has to choose the option overlook password. After clicking on the option protection question can be displayed which the person has to reply . After answering the question efficiently the password is be despatched at the mail identification. contrast of alphanumeric password authentication structures and graphical password authentication structures Alphanumerical username/passwords are the maximum not unusual form of person authentication at the same time as graphical passwords aren't tons in use. but every day using graphical password is growing. Alphanumeric passwords are clean to put into effect and use and also graphical passwords are smooth to put into effect and use. The requirement of the alphanumeric passwords is that they must be without problems remembered via a user, at the same time as they should be hard to wager via fraudulent man or woman. these both requirements are for graphical passwords too and it gets happy as remembering pictures are an awful lot easier than remembering textual passwords. If quick passwords are used then they may be effortlessly guessable and are goal of dictionary and brute-forced attacks. while if strong passwords are enforced a policy on occasion ends in an contrary impact, as a person may also write his or her tough-to-consider passwords on notes or at the notepad and if seen by means of some different user exposes it to direct robbery that is misuse can be carried out. while is graphical passwords are used these all problems do now not get up.

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 and these 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 includes one click on-factor according to picture. this is within the CCP technique the customers are required to don't forget best one factor in a single photograph. The images are stored within the database as in the sooner methods too. that is done for a sequence of photographs. that is the consumer has to do the choice in sequential order best that is in the identical order wherein she or he did all through registration. the next photograph is displayed only whilst the user clicks on the press point of previous image effectively. So the users obtain immediately implicit remarks whether they are on the best music or no longer whilst logging in. So the Cued click on factors approach no longer best improves usability however also security. formerly we've visible one of a kind graphical authentication strategies. In CCP we simply used to click on one point in a single image and that is achieved for wide variety of images as discussed previously. but inside the CCP with sound signature we also have move pick sound as a signature as this will provide the user with better authentication. The sounds of different birds or animal or the consumer's most suitable sound can be stored within the database. Then when the person chooses the points in every photo after this the consumer is requested to pick the sound signature similar to each click on point this sound signature may be used to assist the user in recalling the press factor on an picture. that is right here a graphical password gadget with a supportive sound signature helps to boom the remembrance of the password is designed. excellent overall performance has been proven by using the machine in terms of ease of use, velocity and accuracy. The statement for this technique changed into that selecting and remembering most effective one point consistent with photo is plenty simpler or less difficult. furthermore seeing every image triggers the user's memory of where the corresponding point turned into placed. The CCP method provides higher security than bypass factors as the number of pictures increases the workload for attackers. It offers cued-recall and introduces visible cues that instantly alert legitimate customers in the event that they have made a mistake whilst coming into their modern click on-point (at which point they are able to cancel their try and retry from the beginning).

LITERATURE REVIEWS:

Almulhem . A ,(2011) , Graphical passwords offer a promising alternative to traditional alphanumeric passwords. they're attractive considering humans usually consider photographs better than phrases. in this prolonged summary, we advocate a easy graphical password authentication gadget. We describe its operation with some examples, and highlight essential components of the machine.

Davis.D ,et.al.., (2004) , He biggest posted empirical assessment of the outcomes of person choice on the safety of graphical password schemes. We show that permitting user selection of passwords in two graphical password schemes, one primarily based at once on an existing business product, can yield passwords with entropy a long way under the theoretical finest and, in some instances ,which can be especially correlated with the race or gender of the user. For one scheme, this impact is so dramatic as a way to render the scheme insecure. A end of our paintings is that graphical password schemes of the type we have a look at might also commonly require a extraordinary posture to- ward password choice than textual content passwords, wherein selection by way of the consumer stays the norm nowadays.

Johnson.G,(2005), okay.Renaud, The graphical method substitutes the exact remember of alphanumeric codes with the recognition of formerly learnt snap shots, a ability at which people are remarkably gifted. so far, little interest has been devoted to usability, and initial research has failed to conclusively establish large reminiscence improvement. This paper reviews consumer studies evaluating numerous implementations of the graphical approach with PINs. effects reveal that snap shots may be a solution to some troubles pertaining to to traditional know-how-primarily based authentication however that they may be not a easy panacea, due to the fact a bad design can eliminate the photo superiority impact in reminiscence.

Suo.X, et.al.., (2005), This technique has been proven to have significant drawbacks. for example, users have a tendency to pick passwords that may be without difficulty guessed. then again, if a password is hard to guess, then it's miles frequently hard to don't forget. To address this hassle, some researchers have advanced authentication techniques that use images as passwords. on this paper, we conduct a comprehensive survey of the existing graphical password techniques. We classify these techniques into two categories: reputation-based and do not forget-primarily based approaches.

Weinshall.D, et.al.., (2004), We become aware of a huge range of human memory phenomena as capacity certificate of identity. these "imprinting" behaviors are characterized by way of sizable ability for complicated stories, which can be diagnosed without apparent attempt and but can't be transferred to others. they are appropriate for use in near 0-knowledge protocols, which limit the quantity of mystery information uncovered to prying eyes while identifying an man or woman. We cartoon numerous examples of such phenomena[1-3], and observe them in comfy certification protocols. This offers a unique technique to human-pc interfaces, and raises new questions in numerous traditional regions of psychology.

METHODOLOGY:

The proposed authentication gadget works as follows.on the time of registration, a user creates a graphical password through first entering a photo she or he chooses. The person then chooses several point-of-hobby (POI) regions in the picture. every POI is described by using a circle (center and radius). For each POI, the user sorts a word or word that could be associated with that POI. If the person does now not kind any textual content after choosing a POI, then that POI is related to an empty string. The user can select both to put into effect the order of selecting POIs (more potent password), or to make the order insignificant.

whereas CCP password consists of one click on-point in step with picture. that is in the graphical based authentication technique the person has to don't forget many factors in one picture and that is the major downside of graphical password authentication technique. in the CCP approach the users are required to bear in mind simplest one point in one photograph. The photos are saved in the database as in the sooner strategies too. that is achieved for a sequence of snap shots. this is the consumer has to do the selection in sequential order best that is within the equal order in which he or she did for the duration of registration. the next photograph is displayed simplest while the user clicks on the press point of preceding photograph correctly. So the customers get hold of instantaneous implicit remarks whether they're on the right music or not while logging in. So the Cued click points approach not only improves usability however additionally protection. The remark for this approach changed into that deciding on and remembering handiest one point in keeping with photo is a great deal simpler or simpler. moreover seeing each picture triggers the consumer's reminiscence of wherein the corresponding point become located. The CCP technique affords better protection than bypass points as the quantity of pics increases the workload for attackers. It offers cued-don't forget and introduces visual cues that right away alert valid users if they have made a mistake whilst coming into their contemporary click-factor (at which factor they can cancel their strive and retry from the beginning).

So every right click effects in showing a next-photograph, in effect leading users down a “direction” as they click on their sequence of points. that is if assume in the course of the registration segment five photos had been chosen that is five factors had been chosen then the person has to pick out the pictures inside the equal sequence. The person can cross the second one photograph best while he chooses the primary image click point effectively. further the user can visit third most effective while he chooses remaining two picture click on points efficaciously. At remaining, the person goes to last this is 5th simplest whilst he chooses last four photo click points correctly. A wrong click on leads down an incorrect route and the indication is given explicitly via the machine approximately the authentication failure. If the consumer dislikes the ensuing photographs, advent of a new password related to extraordinary click on-points may be accomplished to get various pix.

In CCP a person has a patron tool (which displays the images) to get admission to an internet server (which authenticates the consumer). via SSL/TLS the photographs are saved server-facet with consumer communication. It to start with features like bypass points. a technique known as discretization is used to find a click on-point's tolerance square and corresponding grid all through the introduction of password. This grid is retrieved from the database and used to find if the clicking-point falls within tolerance of the unique point and this is carried out for each clickpoint in a subsequent login try. With the assist of CCP, we further want to locate which subsequent-photo to display. suppose as an example if we take snap shots of size 451x331 pixels and tolerance squares of 19x19 pixels. If we used robust discretization, we would have three overlapping candidate grids every containing about four hundred squares and within the simplest design, 1200 tolerance squares according to photo (despite the fact that best four hundred are used in a given grid). A characteristic f (username, cutting-edge image, modern-day Tolerance square) is locate which uniquely maps every tolerance rectangular to a next-photo. A minimum set requirement of 1200 pictures is suggested at every level. There can be a controversy in opposition to fewer snap shots and having multiple tolerance squares map to the same next-picture, that this may result in misleading implicit remarks in (albeit rare) conditions wherein users click on an wrong factor yet nevertheless see the appropriate subsequent-photo. each 1200 next-pics would have 1200 tolerance squares and as a consequence require 1200 next-pics of them. With this the number of photos could fast become huge. So re-the use of the photograph set throughout stages is accomplished. by reusing photographs, there is a moderate threat that users see replica snap shots. throughout 5 levels within the password advent, the photograph indices a1,..,a5 for the images inside the password sequence are every inside the variety 1 _ ab _ 1200. while computing the subsequent-image index, if any is a repeat (i.e., the subsequent ab is same to ac for a few c < b) then the subsequent-photograph selection characteristic f is deterministically perturbedto select a distinct picture. The machine selects consumer's preliminary image based totally on a few person function (like a controversy to f above we've used username). on every occasion a person enters the password the collection is re-generated from the feature. If an wrong click-point is entered through the person, then the collection of photographs from that point onwards will be incorrect and hence the login strive will fail. This cue will now not be useful for an attacker who does now not know the suitable series of pictures.

a major usability improvement over skip points is the reality that legitimate users get instantaneous comments about an mistakes when trying to login. whilst incorrect photo is seen through the person he/she knows that the state-of-the-art click-factor changed into incorrect and might right away cancel the strive and try once more from the start. another usability development is that being cued to recall one factor on each of 5 pix seems simpler than remembering an ordered sequence of 5 factors on one picture. the following are the steps which ought to be observed in

CCP: Password advent segment: The point selection must be performed on each of the picture. that is if there are 5 photos first point could be decided on on first photograph, 2d factor could be selected on the second one photograph and so on. That if a person desires to create a password he has to perform this step.

affirm phase: affirmation of password is finished via re-coming into it yet again. If the password typed is inaccurate then the consumer has to return to step 1. even supposing a new password is started with the identical preliminary image, but typically consists of special pics thereafter, depending on the press-points.

MRT: complete a mental Rotations take a look at (MRT) puzzle. A paper based totally mission is given to the user to distract him/her for at the least 30 seconds. it is generally a visible challenge with the intention to clear his/her working memory.

Login segment: Now if the consumer wants to Log in he/she need to know identification and password. The consumer can cancel the login try and try again if an blunders is observed with the aid of the customers at some stage in login. The creation of the brand new password can be completed, with the aid of returning to Step 1 of the trial with the same initial picture as a place to begin if the consumer doesn't recollect the password. The consumer could pass this trial and flow directly to the next trial if he/she feels too frustrated with the unique pictures.

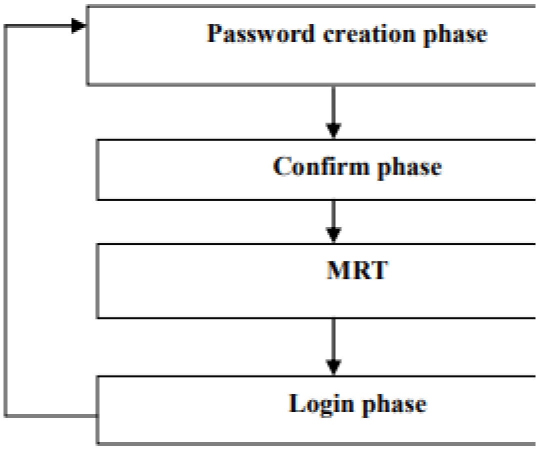


FIG 1: Cued Click Points Steps.

Cued Click Points with sound signature:

previously we have visible exceptional graphical authentication techniques. In CCP we just used to click one point in a single picture and that is executed for wide variety of images as discussed formerly. however in the CCP with sound signature we also have move pick out sound as a signature as this may provide the consumer with higher authentication. The sounds of different birds or animal or the person's optimum sound can be stored in the database. Then when the person chooses the points in each picture after this the consumer is asked to pick out the sound signature corresponding to each click on point this sound signature will be used to assist the user in recalling the clicking factor on an photograph. that is right here a graphical password machine with a supportive sound signature enables to increase the remembrance of the password is designed. very good performance has been proven by means of the system in terms of ease of use, velocity and accuracy. users favored CCP in comparison to pass points, as remembering only one point in line with photo changed into easier and sound signature helped them significantly in recalling the clicking points. As this gadget has been included with sound signature it enables in recalling the password. it has been said that sound signature or tone may be used to do not forget data like snap shots, text and so forth. In each day existence we see diverse examples of recalling an item by the sound related to that item.

Our idea is inspired by this novel human ability. The system creates user profile as follows:

1. Master vector User ID,
2. Sound Signature frequency,
3. Tolerance Detailed Vector Image,
4. Click Points

Steps in Cued Click Points with sound signature:

Registration Process:

As proven inside the fig.2 if the consumer doesn't have the identity and password then he needs to sign in himself/herself or create a new identification. So if the consumer doesn't have identity he will get a completely unique person identity and password. After the choice of id he/ she want to choose sound signature. The consumer also wishes to pick the tolerance degree. After this the person selects the photo and click on on bypass factor. this is stored in the database.

The sound frequency is selected. A tolerance price is chosen on the way to decide that the consumer is authenticated or fraudulent and the same sound frequency is chosen which he/she wants to be played at login time To create specified vector consumer has to choose collection of photographs and clicks on every photograph at click on points of his desire. Profile vector is also create.

Now the device asks whether the person wants to select extra pics or now not. If the user clicks on no then the facts gets stored within the database and the user is requested if he/ she wants to hold or not. If the user click on sure on the other hand the person has to select the following photo and click on the pass point and again the gadget will ask whether or not the user wants to select the subsequent photograph or no longer. this can be performed 5 times if we've got saved the restriction of five.

in this device user has to do not forget the press point's for every photograph. additionally user need to upload the photographs by using own. The person desires to bear in mind the press points in addition to the photographs very well. If he/she fails to don't forget then person will no longer be allowed to perform the login session. The consumer also wishes to take into account the path that the series of the photographs clicked as password in any other case he/she fails to carry out the login consultation.

After introduction of the login vector, machine calculates the Euclidian distance among login vector and profile vectors stored. Euclidian distance among two vectors p(x, y) and q(a,b) is given with the aid of

$$D\left((x, y), (a, b)\right) = \sqrt{(x - a)^2 + (y - b)^2}$$

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.

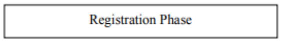
At last the user profile vector will be created and stored in the database so that the information can be used if a user login the system.

Login:

that is the next phase after the registration has been carried out. Login is allowed to be done best whilst the user is registered user otherwise first he has to check in himself/herself first and then he/ she can carry out the login.

Now as soon as the registration has been carried out by means of the person and he/she does the login. first of all the user identification is examine. Then the consumer profile vector is stored inside the database throughout the registration section so it's miles fetched from the database. The picture which is chosen at some stage in registration segment is retrieved from the database and the photo is displayed. The user wishes to pick the same factors which he chooses during the registration phase. The person also has to pick the same function which he decided on during the registration section. If suppose the mouse position is same to consumer profile then the sound signature is performed and the press factors are acquired and the guidance of login vector is executed. Now the evaluation of login and person vector is executed.

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



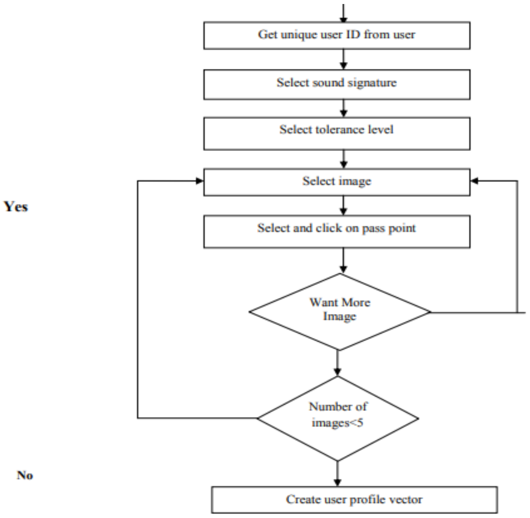
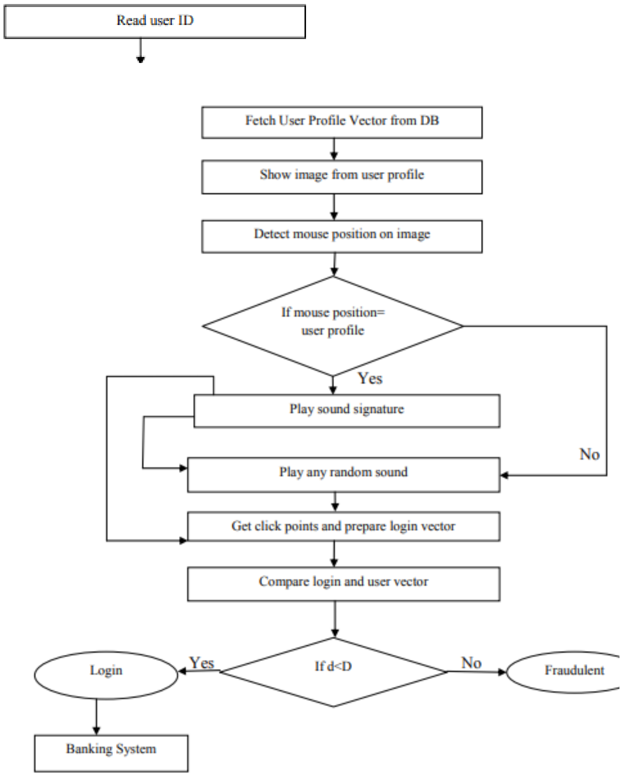


Fig 3: Login phase of Cued Click Points with sound signature


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

RESULTS:

Our initial analysis suggests that it's far extra difficult to break graphical passwords the use of the conventional attack methods which includes brute pressure search, dictionary assault, or spyware. universal, the current graphical password strategies are still immature. lots more studies and consumer studies are wanted for graphical password strategies to attain better stages of maturity and useful ness Graphical passwords schemes provide a way of creating greater human friendly passwords. here the security of the device could be very excessive. Dictionary assaults and brute pressure seek are infeasible.

CONCLUSION:

various techniques for graphical authentication turned into mentioned and found that the graphical authentication is lots more beneficial than the alternative sorts of authentication techniques. it is also very smooth to use than the alphanumeric password or OTP method. due to the use of graphical based totally techniques a brute pressure attack are prevented and is the maximum essential benefit of graphical primarily based password. in the CCP method the users are required to consider handiest one factor in a single image and the next photograph is displayed handiest when the user clicks on the press point of previous picture correctly. A graphical password machine with a supportive sound signature is tons greater useful as it helps to boom the remembrance of the password and has shown very good performance.

REFERENCES:

[1]. A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops).Ft. Lauderdale, Florida, USA., 2003.

[2]. K. Gilhooly, "Biometrics: Getting Back to Business," in Computer world, May 09, 2005.

[3]. A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33,pp. 168-176, 2000.

[4]. D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in

Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402

[5]. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13thUsenix Security Symposium. San Diego, CA, 2004.

[6] X. Suo, Y. Zhu, G.S, "Owen. Graphical passwords: A survey", In Proceedings of Annual Computer Security Applications Conference, 2005, pp. 463–472.

[7]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.

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

[9] Real User Corporation, "The science behind passfaces", 2004.

[10] G. E. Blonder, "Graphical password. U.S. Patent 5559961, Lucent Technologies", Ed. NJ: Murray Hill, 1995.

[11]A. Almulhem, A Graphical Password Authentication System, 2011, pp. 223-225.