International Journal of Multidisciplinary Research and Development

IJMRD 2015; 2(3): 763-768
www.allsubjectjournal.com
Received: 10-03-2015
Accepted: 25-03-2015
e-ISSN: 2349-4182
p-ISSN: 2349-5979
Impact Factor: 3.762

Pawar Poonam A
(B.E Computer Engg. Pune University) PREC, Loni, Maharashtra, India.

Gayake Nalini B
(B.E Computer Engg. Pune University) PREC, Loni, Maharashtra, India.

Mane Kalpana T
(B.E Computer Engg. Pune University) PREC, Loni, Maharashtra, India.

Mudpe Ashwini M.
(B.E Computer Engg. Pune University) PREC, Loni, Maharashtra, India.

Correspondence:
Pawar Poonam A
(B.E Computer Engg. Pune University) PREC, Loni, Maharashtra, India.

Graphical Password Authentication with Cloud Securing Method

Pawar Poonam A, Gayake Nalini B, Mane Kalpana T, Mudpe Ashwini M.

Abstract
Now a days for information security authentication is the most necessary factor .It applies strong text based password that give security but for remembering we need to store it in some places .for this there is different method to remove this complication graphical password is used. Computer security depends largely on password in order to authenticate human user. A graphical password is an authentication work by having the user select from image and picture. If any application provided user friendly authentication then is easy to access used that application.
Here we are using the Graphical password because human mind can easily remember picture and then the alphabets and digits. We are using cloud with graphical password with security purpose. When we created graphical password at that time user select two images from set of images. By using this four images password is created.

Keywords: cloud computing, password authentication

1. Introduction
Graphical password provide a programming alternative traditional alphanumeric password. they are attractive since people usually remember picture better than word. Password that are based on images rather than alphanumeric string. The basic idea of password is that it is easy to remember and decreases the tendency to choose assure password [3].
If there are more number of images then the space of graphical password schema may be large. That of the text base and thus appropriately offer better resistance to dictionary attack. because of this reason there is growing interest in graphical password. The Graphical Password is also applied to ATM machine and mobile device for security purpose [6].
There are three types of authentication method [6] :-

1] Token base authentication:
The general concept behind the token based authentication is simple. allows user to enter their username and password in order to obtain a token which allows them to fetch a specific resources without using their username and password once their token has been obtain , the user can offer the token-which offers access to specific resources for a time period-to the remote site. Advantages of this authentication are many as-the user could pass the token ,once they have obtain it onto some other automated system which they are willing to trust for limited time and a limited set of resources ,but would not be willing to trust with their username and password.

2] Biometric Base Authentication:
Biometrics-based authentication offers several advantages over other authentication methods, there has been a several significance in the use of biometrics for user authentication in recent years. It is important that such Biometrics-based authentication systems being designed to overcome the attacks when employed in security-critical applications, especially in unattended remote applications such as e-commerce.

3] Knowledge Base Authentication:
This is most popular technique it uses both text based and image based passwords. Here knowledge base authentication is further divided into Alphanumeric Password and Graphical Password. In this paper we are using cloud for security purpose.

2. Literature Survey

In this graphical password we are using an recognition and recall-based techniques. The main reason behind this is because graphic picture are more recalled than the text password.

Here we are distinguish the graphical password techniques till 2009. This techniques classified into three groups as follows-

1. Recognition Based Technique
2. Pure Recall Based Technique
3. Cued Recall Based Technique

2.1 Recognition Based Techniques

In this techniques user is presented with a collection of image, icons or symbol. During authentication user select the set of candidates .Its Result is(90%) majority of user to remember the password after one or two months. Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique .In this system user have to select no of images from the set of images generated by the program. Below figure shows the random images.

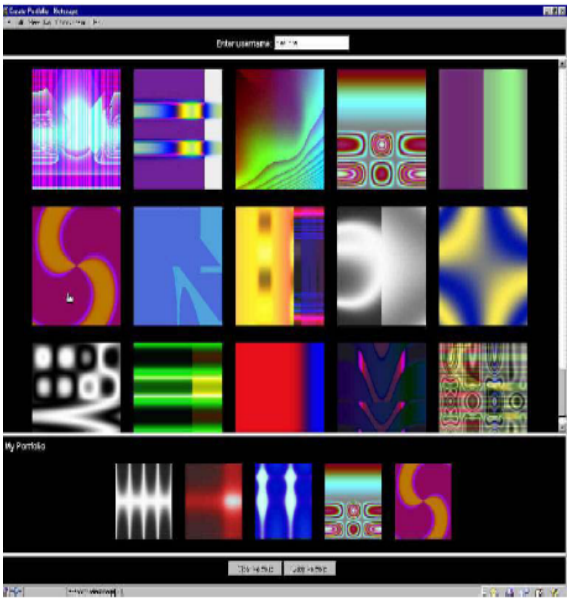


Fig 1: Set of Random Images

2.2 Pure Recall-base Techniques

In this techniques user reproduce their password without using any hint and gesture .user would remember their password just like DAS(1999)and Qualitative DAS(2007).It is provided with varying levels of usability and security features.

It follow many algorithm, which include

A] Passdoodle: - which introduce in 1999. This technique is introduce by Christopher [2]. This is a graphical password which is made up of handwritten designs or text that is normally drawn with a stylus onto a touch sensitive screen.

B] Syukri algorithm (pure recall):- Syukri algorithm proposes a system where authentication is counted by having user drawing their signature using mouse in 2007.Advantage of this technique is that, guessing of any ones signature properly is not easy hence it is difficult to hack the system with this technique

C] Qualitative DAS: To overcome the drawbacks of DAS in 2007 QDAS [2] is introduce

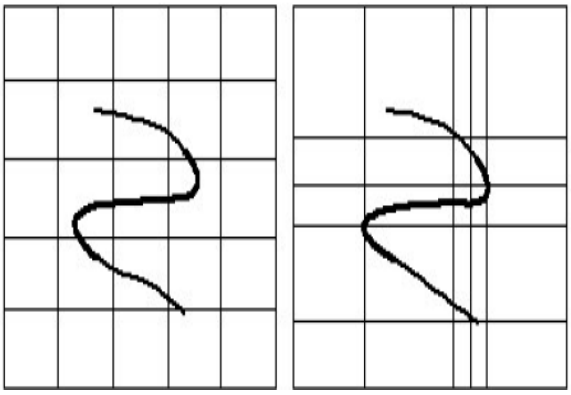


Fig. 2: A sample of qualitative DSA algorithm

D] Draw a Secret: It introduce in 1999.In this system user allow to draw a simple picture onto 2D grid. The interface consisted of a rectangular grid of size G * G. Each cell in this grid was denoted by discrete rectangular coordinates (x,y)

2.3 Cued Recall Based Techniques

In this technique framework of reminder, gesture and hints are consider. Using this technique user reproduce their password or reproduction becomes more accurate.

It follow many algorithm, which include

A] Grid selection (pure recall):- In 2004, Thorpe and Oorschot further studied by impact of password length and stroke – count as complexity property of a DAS scheme.

B] Blonder Scheme (cued recall):- This method was developed by Greg. E. Blonder. To begin with a pre-determined image is presented to the user on a visual display and then the user is supposed tap regions by pointing to one or more predefined locations on the image (in a predetermined order as a way of pointing out his or her authorization to access the resource. According to Blonder this method is secure since it has a million of different regions to pick from.

C] Pass point(cued recall):- Pass point was design in order to cover the limitation of Blonder algorithm. In this method click point method is used.

3] Existing System:

Recognition based Technique:

A] Image based scheme :- in this scheme we are using a different kinds of images as background .Including photo graphics ,artificial picture or other kinds of images.

we further divide into two subclasses.

1] single-image based: in this user provide a single image as background, they have to provide a particular select points.

Fig 3:.BlonderScheme

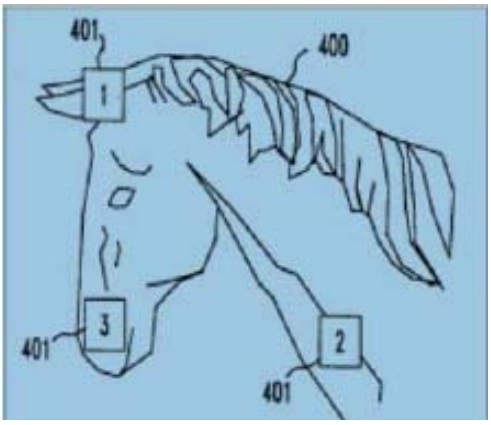


Fig 4: Viskey

The pass point scheme by Wiedenbecket ,al [35,37] extented Blonder's idea by eliminating the predefined and allowing arbitrary images to be used .as a result user can click on any images password is create

Fig.5.Passpoint

2] Multiple Image Based:
In this user provide multiple images to select any one of them. Passface is a technique developed by Real user corporation[5] . the password is the collection of k faces ,each selected from a distinct set of n>1 faces. we used k=4 and n=9. choosing her password images are unique and do not appear more than once .In the story scheme , a password is a sequence of k unique images selected by the user to make a story from a single set of n>k images, each derived from a distinct category of image types .

Fig 6: Story Scheme

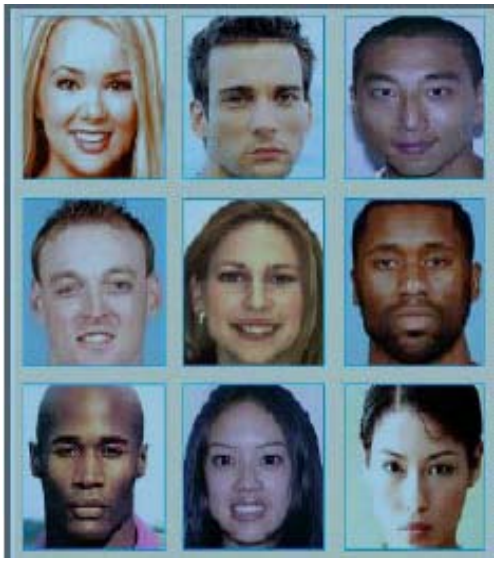


Fig.7.Pass Faces

Advantages:
User easily remember the password.
Disadvantages:
It is a very long process of selection of images.

B] DAS Scheme:
Jemyn,et al. proposed a technique, called " Draw a secret[4] , which allows the user to draw their unique password . A user is asked to draw a simple picture on a 2D grid , grids are stored in the order of drawing. During authentication, user is asked for re-drawing the picture. If thus drawing of picture touches the same grids in the same sequence than the user is authenticated.

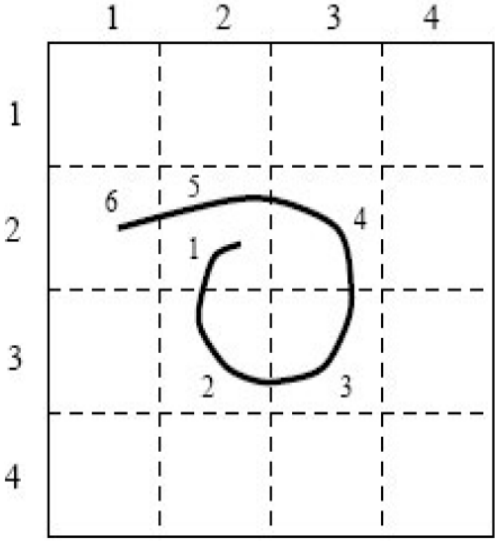


Fig 8: Draw a secret on grid

Advantages:
Grid is simple object there are no extra displays are needed.
Disadvantages:
Sequence can be changed during authentication or grid may be different as it is a drawing.

C] Triangle based scheme:
In this scheme user provide a convex-hall formed by all the pass object ,in which it make the password hard to guess .In this scheme user select a point and forming triangle as a password [1].

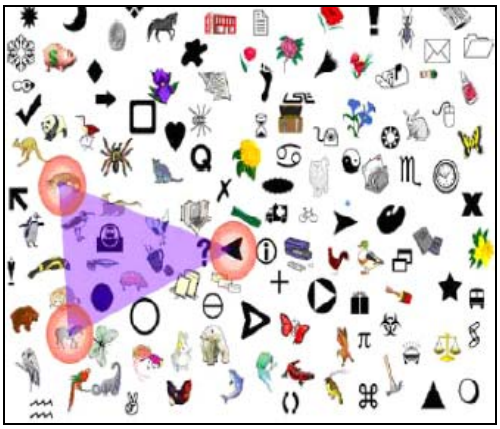
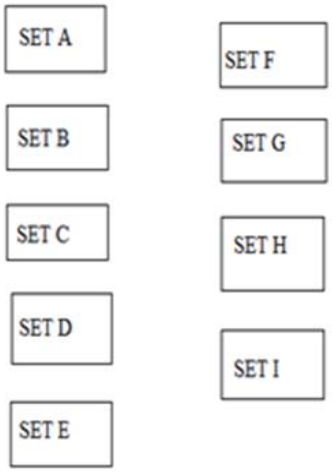


Fig 9: Triangle Based Scheme

Advantages:
Surface are very crowded and image almost same so ,it is difficult to distinguish.
Disadvantages:
Convex surface assigning process takes longer time.

4] Proposed system
Proposed system of our project will be explained in detail with the help of following few steps this steps gives us the information about the password selection.
Step1: start
This is the initial step required for the password selection.
When cloud services started with option to select. For the registration user have to pass through authentication process. At the server side process will be started on the basis of username and basis of result of calculation set of images which will be provided to user.
Step2: calculation by using user name
Here, the calculation based on the username is done.
At the 1st position of alphabet which are in the username are calculated at server side. After that the sum of all that position is done and then from that sum the first digit will be considered for the next calculation.
Result of calculation: E+F+G+H = 5+6+7+8 = 26
Here in this calculation the first digit of the sum is 2. And hence consider for the next calculation.
Step3: How to assign image

In this step finally the images are assign as password.
Here at the server side the set of images has already made. As per the result of calculation which are done in 2nd step the set of images are assigned.
We can assign the 1-9 numbers to the set of images as A=1, B=2,……I=9.
It conclude that if 1st digit of sum is 3 then set of images assigned will set of 'C'. If first digit of that sum is 1 then set assigned will 'A'.



E Every set contain 100 diff images.

C Calculation:

A A=1, B=2, C=3,.....X=24, Y=25, Z=26.

If If username is EFGH then sum is = 5+6+7+8 =26

If If username is PQRS then sum is = 16+17+18+19= 70

2 2 & 7 are forwarded for further calculation

A Assigning set of images:

F For username EFGH as sum is 26 & 2is forwarded

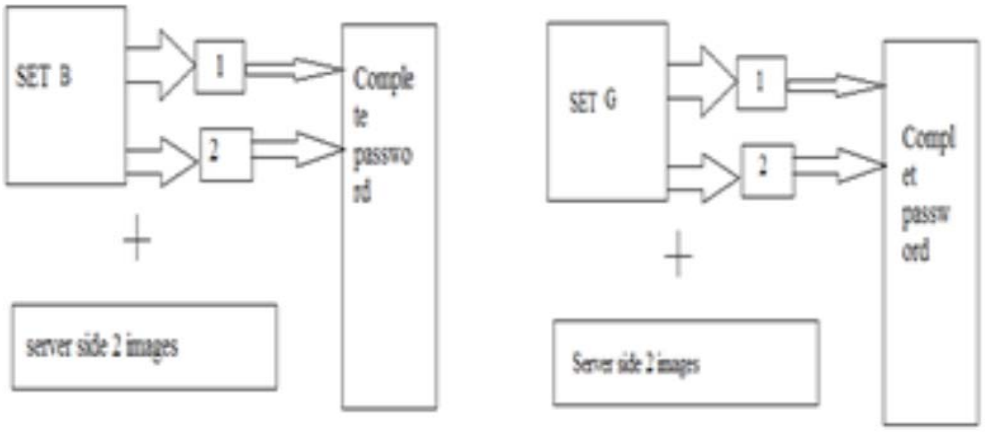
Set of images will be assigned of B

For username PQRS as sum is 70 is forwarded

Set of images will be assigned of G

Selection of password

For username EFGH set is: For Username PQRS set is:



5] Block Diagram of Proposed System

In proposed system the user accessing cloud services they will be provided sign in and sign up option. calculation at server side in sign up registration is created for user base on algorithm. User have to enter username from the particular image set.1st username is check in this algorithm b calculating set of images will be provided to user. Two images user have to select and two images will be provided by server side, so password stored in database of server.

During sign in user have given user name and password is selected from given set of images. After that validation of user is done and cloud access given to the particular user and access of account is done by providing many activities like downloading and uploading.

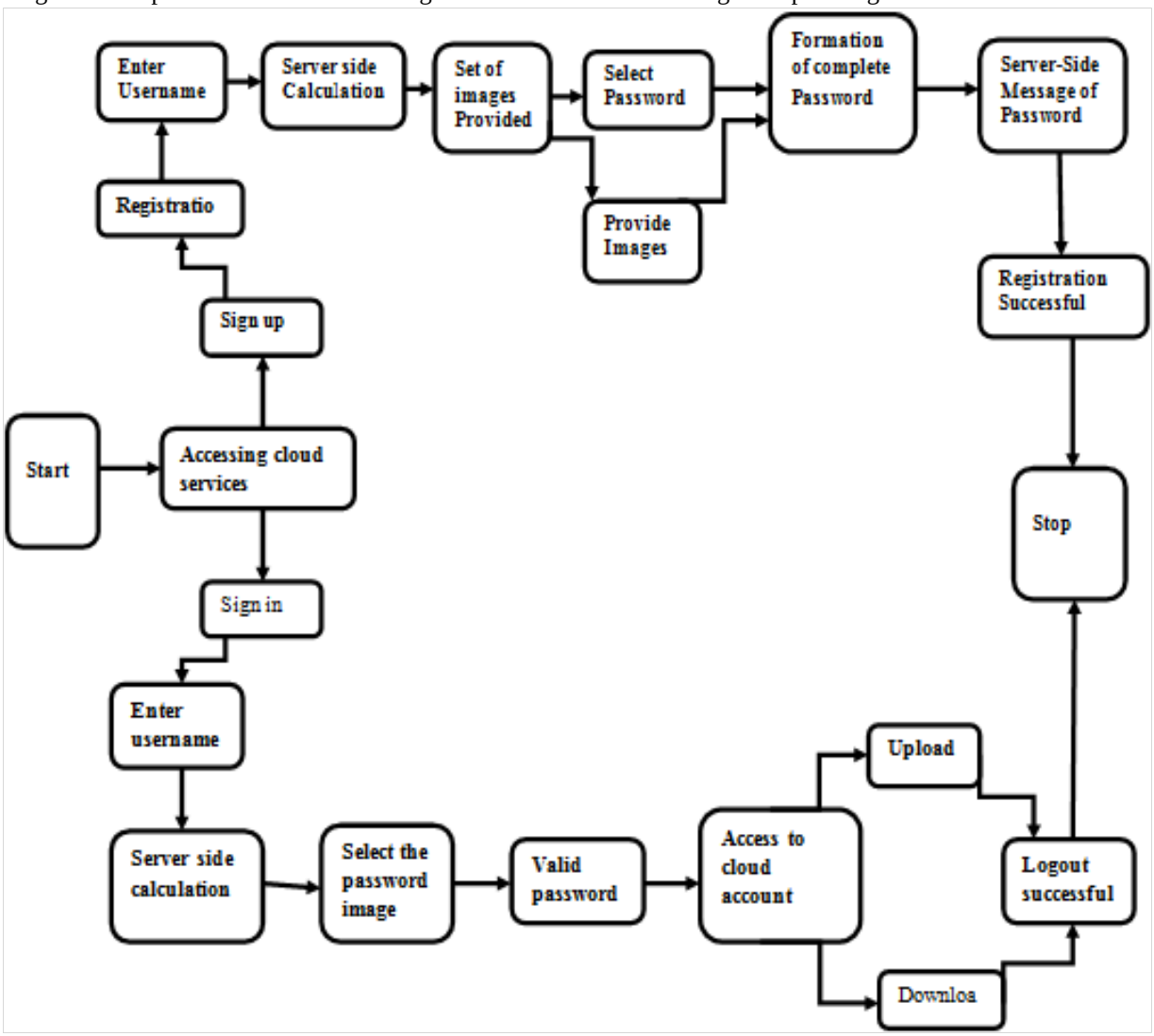


Fig.10 .Block Diagram of Proposed System

6] Use of Graphical Password for Cloud Security:

Graphical password are more secure than alphanumeric password, alphanumeric password uses plane text and easy password .when we conform the alphanumeric password there is some hint option provided by which hacker can easily enter in system .Where in Graphical Password selectable images are used. Images are different for each case so it will take more time for hacker to guess the correct password.

Conclusion:

Graphical password authentication can be given by taking cloud as a platform. The new scheme provides solves the many problems of existing system .By using Graphical password people are better at memorizing Graphical password than text based password.

It can also be useful for user in security point of view .We will also implement this in mobile with android operating system.

References

1. Graphical password authentication for cloud securing scheme by Shraddha M. Gurav, Prathmey k.Rane, Nilesh R. Khochare, Leena S. Gawade 2014 IEEE International Conference on Electronic Systems, Signal Processing and Computing Technologies
2. A Survey on Recognition-Based Graphical User Authentication Algorithms FarnazTowhidi Centre for Advanced Software Engineering, University Technology Malaysia Kuala Lumpur, Malaysia
3. Authentication Using Graphical Passwords: Basic Results Susan Wiedenbeck Jim Waters, College of IST Drexel University Philadelphia, PA, 19104 USA
4. Security Analysis of Graphical Passwords over the Alphanumeric Passwords by G. Agarwal ,1Deptt.of Computer Science, IIET, Bareilly, India 2,3 Deptt. of Information Technology, IIET, Bareilly, India 27-11-2010
5. Graphical Passwords,FABIAN MONROSE AND MICHAEL K. REITER, August 5, 2005
6. A Survey on Recognition-Based Graphical User Authentication Algorithms Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice Susan Wiedenbeck Jim Waters College of IST Drexel University Philadelphia
7. Graphical Passwords as Browser Extension Implementation and Usability Study1, Kemal Bicakci1, Mustafa Yuceel1, Burak Erdeniz2, Hakan Gurbaslar2, NartBedin Atalay3
8. Pass-Go, a New Graphical Password Scheme,HAITAOThesis submitted to the Faculty of Graduate and Postdoctoral Studies Electrical and Computer Engineering University of Ottawa© Hai Tao, Ottawa,Canada, June, 2006
9. Graphical Password Authentication system in an implicit manner,SUCHITA SAWLA*, ASHVINI FULKAR, ZUBIN KHAN Department of Computer Science, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, MS, India. March 15, 2012
10. Authentication for Session Password Using Colour and Images by jai patel,SNJB's COE Computer Engineering Department, University Of Pune.
11. Mandler, J.M. and Ritchey, G.H. (1977). Long-term memory for pictures. *Journal of Experimental Psychology: Human Learning and Memory*, 3, 386-396.
12. Morris, R. and Thompson, K. (1979). Password security: A case study. *Communications of the ACM*, 22, 594-597.
13. Norman, D.A. (1988). The Design of Everyday Things. Basic Books, New York.
14. Paivio, A., Rogers, T.B., and Smythe, P.C. (1976) Why are pictures easier to recall then words? *Psychonomic Science*, 11(4), 137-138.
15. Patrick, A. S., Long, A. C., and Flinn, S. (2003). HCI and security systems. In *Proc. CHI 2004*, ACM Press, 1056-1057.