International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 07 | Oct-2015 www.irjet.net p-ISSN: 2395-0072

Accessing Cloud Services Using Graphical Password Authentication

S.A.Gade, Alpesh Valvi , Suraj Birdawade, Datta Tambe.

M.E(Computer) , S.V.I.T, Chincholi ,Nasik , Maharashtra- 422102
B.E(Computer) , S.V.I.T, Chincholi ,Nasik , Maharashtra- 422102
B.E(Computer) , S.V.I.T, Chincholi ,Nasik , Maharashtra- 422102
B.E(Computer) , S.V.I.T, Chincholi ,Nasik , Maharashtra- 422102

Abstract - ***Information security authentication is the most necessary factor. Graphical password is best substitute solutions to alphanumeric password as it is quite difficult to remember alphanumeric password. According to psychological studies the human mind can easily remember graphical symbols and images than alphabets or digits. When any other application that provide user friendly authentication then it is more effective to access and use that application securely. We have planed cloud with graphical security by means of image password. In this paper we are going to represent the authentication to cloud by using graphical password authentication process. We are providing an effective algorithm which is based on selection of username and images as a password. By this paper we are to try to give set of images on the basis of alphabet sequence position of characters in username. At the bottommost cloud is provided with these graphical password authentication schemes.***

Key Words: *Graphical password, cloud security.*

1. INTODUCTION

When anyone wants to access the network, for security purposes every web application provides user authentication. In a Network, we have various issues to work with our services, data & today Cloud computing provides convenient on demand network access to a shared pool of configurable computing resources. The resources can be rapidly deployed with great efficiency and minimal management overhead. Cloud is an insecure computing platform from the view point of the cloud users, the system must design mechanisms that not only protect sensitive information by enabling computations with encrypted data, but also protect users from malicious behaviors' by enabling the validation of the computation result along with an effective authentication mechanism to the user, from the past timing we have a various scheme to authorize any interface here also in order to access a cloud we use textual password which is not much secure in terms of authentication because textual password might be easy to guess & lot of brute force attack has been already done on textual based attack in current world so that still here we are finding an efficient way where we can get a reliable authentication to correct user, one of the way which we got is object password or graphical password to authenticate interface.

We have proposed cloud with graphical security by means of image password. We are providing one of the greatest algorithms which are based on selection of username and images as a password of our cloud. We are trying to give set of images on the basis of alphabet series position of characters in username. Finally cloud is provided with this graphical password authentication scheme.

1.1 Need

Cloud security can also be given by alphanumeric password but thing matter is that use of alphanumeric is not that much of secure and easy to remember. One more important thing is that every time users have recalled the password. User has to give priority to security beyond their need so as to satisfy their work. Graphical password is one of the best alternative solutions to the alphanumeric password as it is very dusty process to remember alphanumeric password to cloud. When any application is provided with user friendly authentication then it becomes easy to access and use that application securely. One of the leading reasons behind these methods according to psychological studies human mind can easily remember images than alphabets or digits. In this system we are representing the authentication given to cloud by using graphical password it means choose images as password.

1.2 Basic Concept

The knowledge based authentication system includes the text password and graphical passwords. Typically text passwords are string of letters and digits, i.e. they are alphanumeric. Such passwords have the disadvantage of being hard to remember .Weak passwords are vulnerable to dictionary attacks and brute force attacks where as strong passwords are hard to remember. Hence we are

using textual passwords for less confidential data. Though, users have hard remembering a password that is deep and random arrives. Instead, they create cut short, simple and insecure passwords. By using this graphical password scheme, users click on images or the type alphanumeric characters. For the more confidential data we are using Cued-Click points (CCP) and Persuasive Cued-Click Points (PCCP) techniques.

2. EXISTING SYSTEM

Recognition based Technique:
A] Image based scheme: In this Passwords scheme we are using a different kinds of images as background. Including artificial picture, photo graphics, or other kinds of images. We are further divide into two subclasses.
1] single-image based: In this scheme user provide a single image as background; they have to provide a particular select points.

Fig -1: Blonder Scheme

The passpoint scheme by Wiedenbecket, al [35,37] extended 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

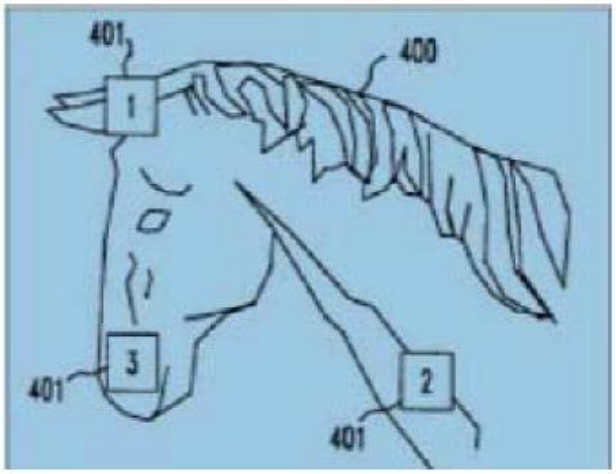


Fig -2: Viskey

Fig -3: Passpoint

2] Multiple Images Based: In this scheme user provide multiple images to select any one of them. Passface is a technique developed by Real user corporation 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- 4: Story Scheme

Fig -5: Pass Faces

Advantages:

Users easily remember the password.

Disadvantages:

It is a very long process of selection of images.

BJ DAS Scheme: Jemyn, et al. proposed a technique, called '' Draw a secret, which allows the user to draw their uncommon password. A user is asked to draw a simple picture on a 2D grid base; grids are stored in the order of drawing. During the authentication, user is asked for redrawing the picture. If thus drawing of picture touches the same grids in the same sequence than the user is authenticated.

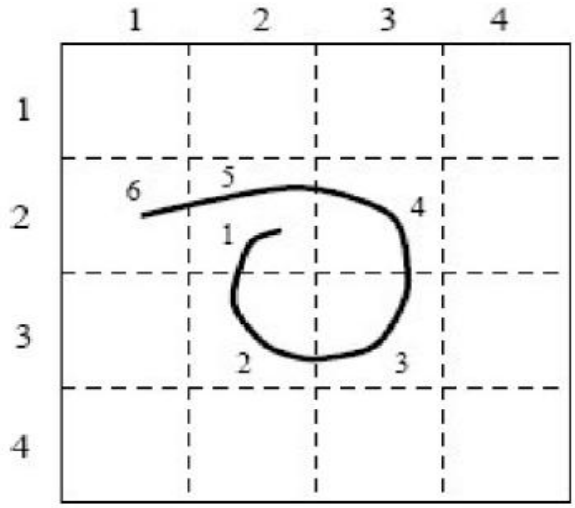


Fig- 6: Draw a secret on grid

Advantages:

Grid is the easy and simple object there are no extra displays are needed.

Disadvantages:

Sequence can be changed at the time of 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.

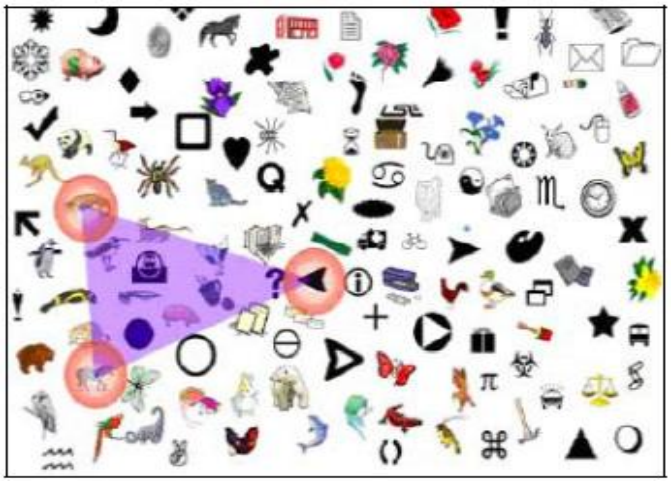


Fig- 7: Triangle Based Scheme

Advantages:

Surface are very crowded and image almost same so, it is difficult to distinguish.

Disadvantages:

Convex surface assigning process takes longer time.

3. THE PROPOSED WORK AND TOOL

A. How to start

When we start the cloud service they will be provided more than one options to select. For registration user have to pass through authentication process. In that on the basis of username, process will be started at the server-side. Set of images which will be provided to user are based on result of calculation.

Username: ABCD

B. Calculations on the basis of username

At the server-side position of username's alphabet in alphabet sequence will be calculated. Then addition of all the positions is done. First digit of that sum will be considered for further next calculations.

Alphabets	A	B	C	D
Position	01	02	03	04

Finding the set to be assigned

Calculation of Result: A+B+C+D= 01+02+03+04= 10

This first digit is 1, forwarded for further calculation.

C. Assigning set of images

There are total 26 alphabets present in alphabet series. We know that any two digit number can start with number 1-9 itself. Server has already made set of images. Set of images will be assigned according to result of calculation which server has got at the second step. 1-9 numbers will be assigned to that sets like

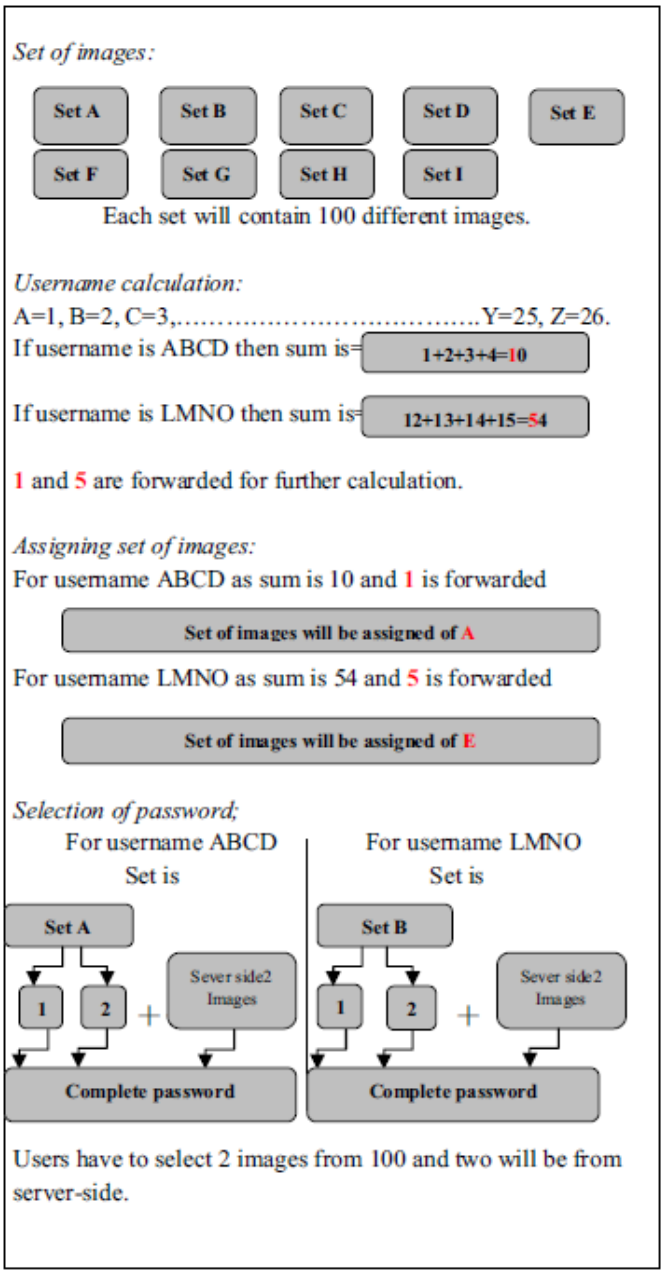
A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9

Means what if first digit is 1,then set assigned to it will set of A. If first digit is 2, then set assigned to it will be B.

D. Selection of password

In this complete password is divided in two sections first is based on user selection, second is based on server provided sets of images. For user selection, from given set of images user has to select two images as the password. From sever end two images will be provided to user so as to form complete password

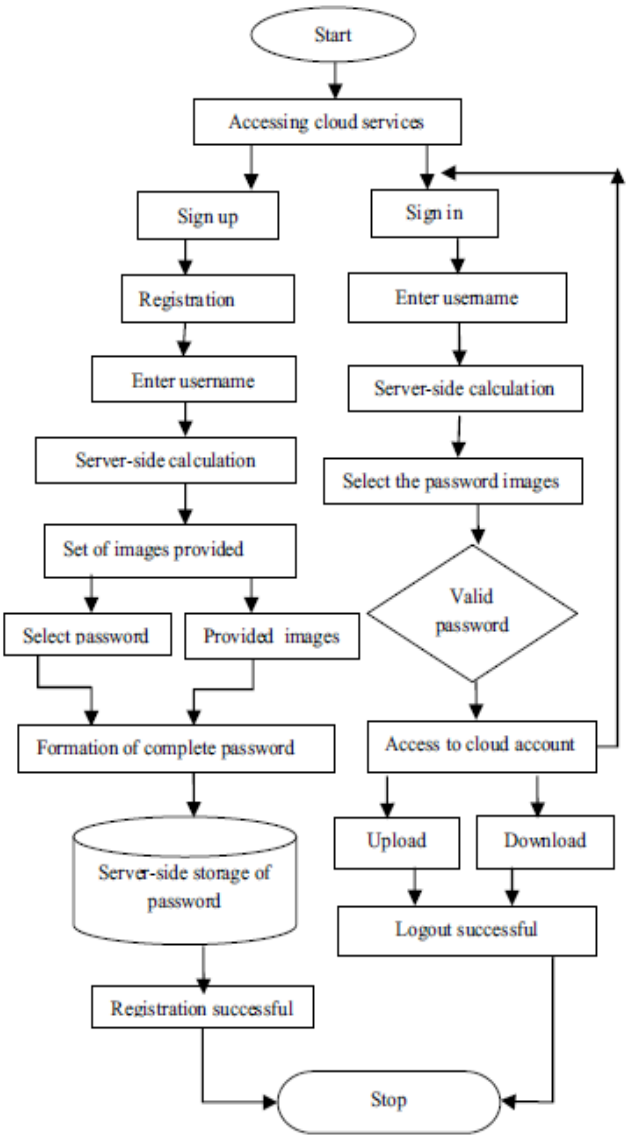
Flow of Proposed System



FLOWCHART OF PROPOSED SYSTEM

In this method when any user try to access the cloud services they will be provided with two options sign in and sign up . At server side calculation in sign up registration is made for user. User have to enter the username based on that particular image set which will be provided to them on the basis of algorithm. In this algorithm first username is checked. After calculation set of images will be provide to user. User have to select two images as client side

selection and other two will be given from server side as server side selection. So the complete password will be stored in database of server. In sign in the user have to give username which he or she has given during sign in and select the password from given set of images. Validation of user is done then cloud access is given to particular user. They access their account with uploading and downloading facility.



Fig– 8: Flowchart for Proposed System

COMPARISON WITH OTHER METHODS

• Drawback is that if one user has number of accounts, to remember all those passwords, is simply not possible.
• In some of the cases it may happen that one can forget the password when there is no frequent use of particular account.
• Providing simple password can also be one solution to that, but they are easily guessable. So there has to be some technique for security. Password can be provided using multiple ways, but there are different drawbacks of that which can be overcome by graphical password.[1][2]
• Most of today's authentication scheme provides username and password of at least eight characters so it become too large to remember.[3]
• Why to choose graphical password for cloud security
Graphical password provides more security than alphanumeric password. Most of the alphanumeric authentication choose a plain text or easy password to avoiding the confusion. whenever we confirm the alphanumeric password there is some hint option provided, using this hackers can easily gain entry to the system in less time. Most of the system provides image related password i.e. Graphical password. In this method selectable images are used , user can have more number of images on each page and among all of this password is selected. Images are different for each case, so if hackers try to match the each combination to find the correct password it will take millions of year. In alphanumeric password eight characters password is needed to gain entry of particular system, but in graphical password user have to select the images that in front of him/her and confirm the password. Whenever user pass through the authentication process it is easy to remember images whatever they have chosen previously. Graphical password is providing more memorable password than alphanumeric password which can reduce the burden on brain of user.

4. CONCLUSIONS

Thus graphical password authentication can be given by taking cloud as a the platform. The new scheme provides solves the many problems of existing system. It can also be useful for user in security point of view.

REFERENCES

[1] A Survey on Recognition-Based Graphical User Authentication Algorithms FarnazTowhidi Centre for Advanced Software Engineering, University Technology Malaysia Kuala Lumpur, Malaysia

[2] Authentication Using Graphical Passwords: Basic Results Susan Wiedenbeck Jim Waters ,College of IST Drexel University Philadelphia, PA, 19104 USA

[3] 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

[4] Graphical Passwords,FABIAN MONROSE AND MICHAEL K. REITER, August 5, 2005

[5] A Survey on Recognition-Based Graphical User Authentication Algorithms

[6] Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice Susan Wiedenbeck Jim Waters College of IST Drexel University Philadelphia

[7] Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme Susan Wiedenbeck and Jim Waters College of IST Drexel University Philadelphia, PA 19104 USA

[8] Graphical Passwords as Browser Extension: Implementation and Usability Study1,Kemal Bicakci1, Mustafa Yuceel1, Burak Erdeniz2, Hakan Gurbaslar2, NartBedin Atalay3

[9] 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

[10] 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

[11] Authentication for Session Password Using Colour and Images by jai patel,SNJB's COE Computer Engineering Department, University Of Pune. Ganeshkhind,Pune.