ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

GRAPHICAL IMAGE AS AUTHENTICATION APPROACH IN CLOUD COMPUTING

Komal More*, Trupti Bothara, Aruna Patil, Kanchan Kunjir, Prof. Suchita Wankhade

*Computer Department ,Trinity College Of Engineering & Research,Pune, India.

ABSTRACT

Graphical password is easy to remember as compared to alphanumerical password. Users tend to pick passwords that can be easily guessed. In case, if user choose hard then it is difficult to remember. Graphical password schemes is a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text. We have proposed cloud with graphical security by means of image password. We are using one of the algorithm which is use user name and images as a password. We are trying to give set of images by using position of alphabet character in user name and cloud is provide secure graphical password authentication.

KEYWORDS— Graphical password, cloud security.

INTRODUCTION:

Problems with Alphanumeric Password:

Human has difficulties to remember password for long time. Once a password has chosen the user should be able to recall it to every time at log in. But, human can forget their passwords sometimes. Password is competing with the item in memory and prevents its accurate recall. If a password is not used frequently it will be even more chances of forgetting password. A complication is that users have many passwords for different web sites. As the number of passwords increases difficulties lead to forgetting or confusing passwords. Users mostly cope with the password problem by decreasing their memory load by using different ways. First, people write down their passwords on page or different things. Second, when they have multiple accounts, they use single password for all systems. In terms of security, a password should be made up of a string of 8 characters, digits, special characters, also including upper and lower case alphabetic characters. A random password does not have meaningful content then it has difficult to memorize. As a result, users are known to ignore the recommendations on password choice. According to new survey have shown that users choose short,simple passwords that are easily guessable, for example, "password," as a personal name or names of pets or dictionary words.They are unlikely to give priority to security over their immediate need to get on with their real work.

Graphical password provides a programming alternative traditional alphanumeric password. They are attractive since people usually remember picture better than word. Password that are based on image rather than alphanumeric string. The basic idea of password that it is easy to remember and decrease the latency to choose assure password. 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 to dictionary attack. Because of this reason there is growing interest in graphical password. The Graphical Password is also applied to ATM machine & mobile device for security purpose.

There are three types of authentication method:-

1] Token base authentication:

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

2] Biometric Base Authentication:

There are many asset of Bio-metrics authentication method as compare to other authentication methods, there has been several consequence in the use of bio-metrics for authentication in recently. Biometric –based authentication system is design to overcome the different attacks when employed in security critical application, 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.

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 distinguishing 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 candidate's .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.

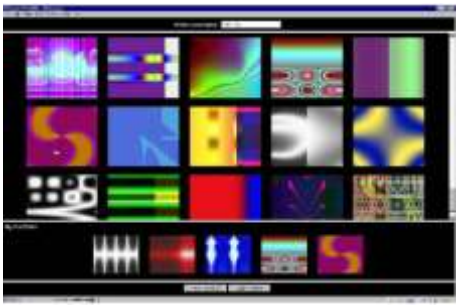


Fig 1: Set of Random Images

2.2 Pure Recall-base Techniques:

In this method 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 follows many algorithms, which include:

A] Pass doodle: -

This method is introduced in 1999. Pass doodle method is introduce by Christopher [2]. This is a graphical password which is made up of handwritten designs.

B] Syukri algorithm (pure recall):-

This method 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 introducing.

D] Draw a Secret:

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

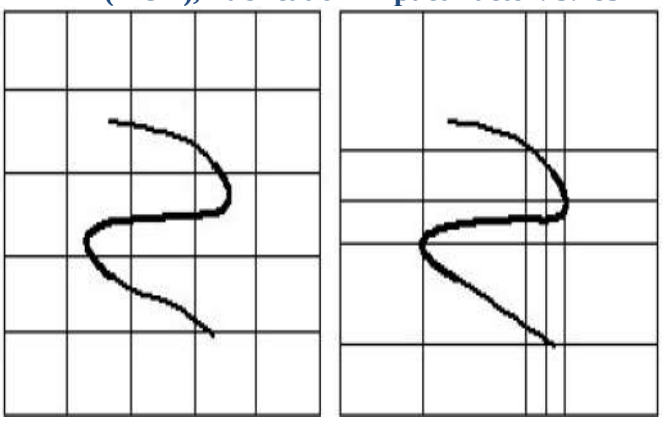


Fig. 2: A sample of qualitative DSA algorithm

2.3 Cued Recall Based Techniques:

In this technique framework of reminder, gesture and hints are consider. Using this technique user reproduces their password or reproduction becomes more accurate. It follows many algorithms, 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 determined image is presented to the user on a visual display and then the user have tap regions by pointing to one or more predefined locations on the image as a way of pointing out his or her authorization to access the resource. 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.

EXISTING SYSTEM

A] Image based scheme: - in this scheme we are using a different kinds of images as background .Including multiple photos, 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 point. The pass point scheme by Wiedenbecket, al 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 3:BlonderScheme

2] Multiple Images Based:

In this user provide multiple images to select any one of them.Pass face 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 password images are unique and do not existing more than once .In the story scheme , a password is a sequence of k different images selected by the user to make a story from a single set of n>k images, each derived from a different category of image types .

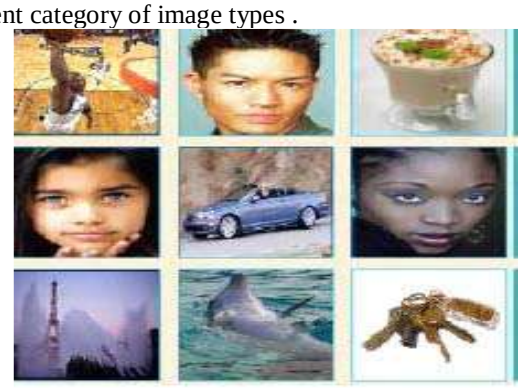


Fig 4: Story Scheme

Advantages:

User easily remembers the password.

Disadvantages:

It is a very long process of selection of images.

B] 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.

Advantages:

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

Disadvantages:

Convex surface assigning process takes longer time.

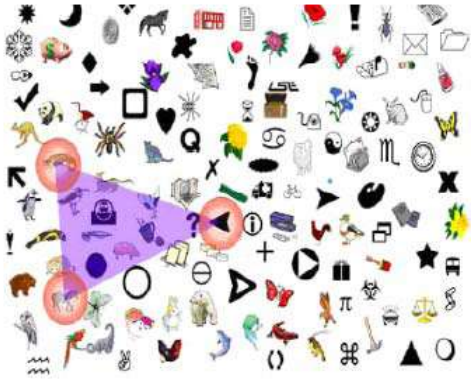


Fig 5: Triangle Based Scheme

PROPOSED SYSTEM

Proposed system of our project will be explained in detail with the help of following few steps. Following steps gives us the information about the password selection:

A. How to start

When one starts the cloud service they will be provided with multiple options to select. For registration user have to pass through authentication process. Depending on the 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: EFGH

B. Calculations on the basis of username (Sever Side)

On the server-side, position of username's alphabet in alphabet series will be calculated. Depending on alphabet position addition is done. First digit of that sum will be considered for further calculations.

Table 1.Alphabet's position

Alphabet	E	F	G	H
Position	05	06	07	08

Finding the set to be assigned:

Calculation of result: A+B+C+D=5+6+7+8=26

This first digit is 2, forwarded for further calculation.

C. How to assign image

In this step finally the images are assigning 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 concludes 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'. Two images are provided by server & two are provided by user. This create complete password & stored into the server database. GPA that will be introduced for security in cloud environment deals with the development of a web application

that allows authorized users to access the information in the cloud environment. In this system the password is provided as an image. When one starts the cloud service they will be provided with multiple options to select. To register user has to pass through authentication process. Depending on the username, process will be started at the server-side. Set of images which will be provided to user are based on result of calculation.

Table2.Assigned sets

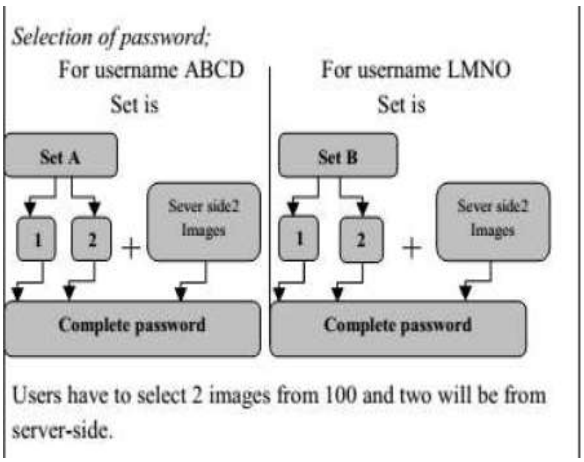
SET A	SET B	SET C	SET D	SET E	SET F	SET G	SET H	SET I
100	100	100	100	100	100	100	100	100

Every set contain the 100 images. That set of an image is assign according the calculation to the user. And finally password is set for cloud.

If the username is KLMN =11+12+ 13+ 14

= 50

5 is considered for further calculation so the set of E is assign for username KLMN.



BLOCK DIAGRAM OF PROPOSED SYSTEM

From the above block diagram it is clear that, when any user try to Access the cloud services they will be provided with two options sign in and sign up. Sign up registration is made for user at server side and calculation is done. User enters the username based on that particular image set which will be provided to them on the basis of algorithm. Then user name is checked. After calculation set of images will be provided to user. Users have to select two images as any other two will be given from server side as server side selection. Then the complete password will be stored in server database. In sign in the user have to give username which he or she has given during sign in and has to select the password from given set of images. After Validation of user is done then cloud account with uploading and downloading facility. access is given to particular user. Then they can access their

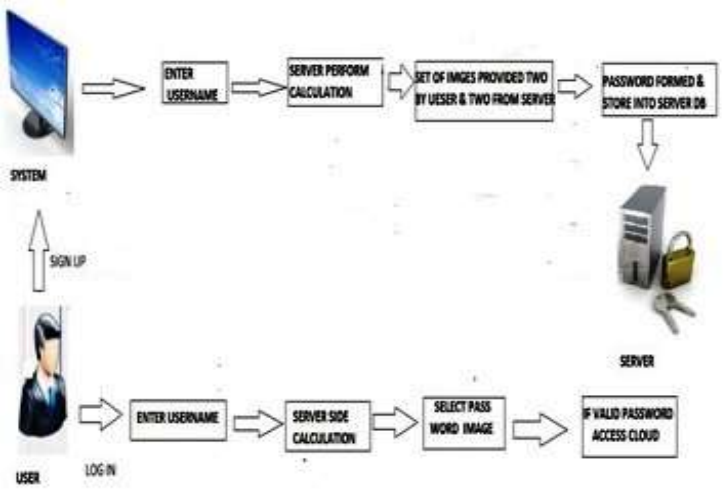


Fig.6 .Block Diagram of Proposed System

Use of Graphical Password for Cloud Security*:*

Graphical passwords 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.

FLOW OF GRAPHICAL PASSWORD AUTHENTICATION SCHEME

The flow chart describes the procedure of Graphical password authentication:

The user enters the username. Server checks whether the user name is present in database. If it is not present, then it displays the message as invalid username. If username is present it will display the screen of image password. Then user clicks the image password which is matched with images stored in database. If this is true it will display full image otherwise error message is displayed. Finally password is match and user is authenticated.

Here we describe the authentication steps:-

1.Cloud user request login page.
2.The server displays login screen.
3.Cloud user login with username and password.
4.The server checks if it is valid username and password by searching in database.
5.If user information not valid it displays error message.
6.Server displays graphical login screen, in which multiple images are showed.
7.The cloud user clicks his password image from multiple images.

8.Server checks whether image is valid by searching in database. If it is not valid, it displays error message else it displays the full image.
9.If user password is valid you will get successfully authenticated with cloud server. Otherwise display error message.

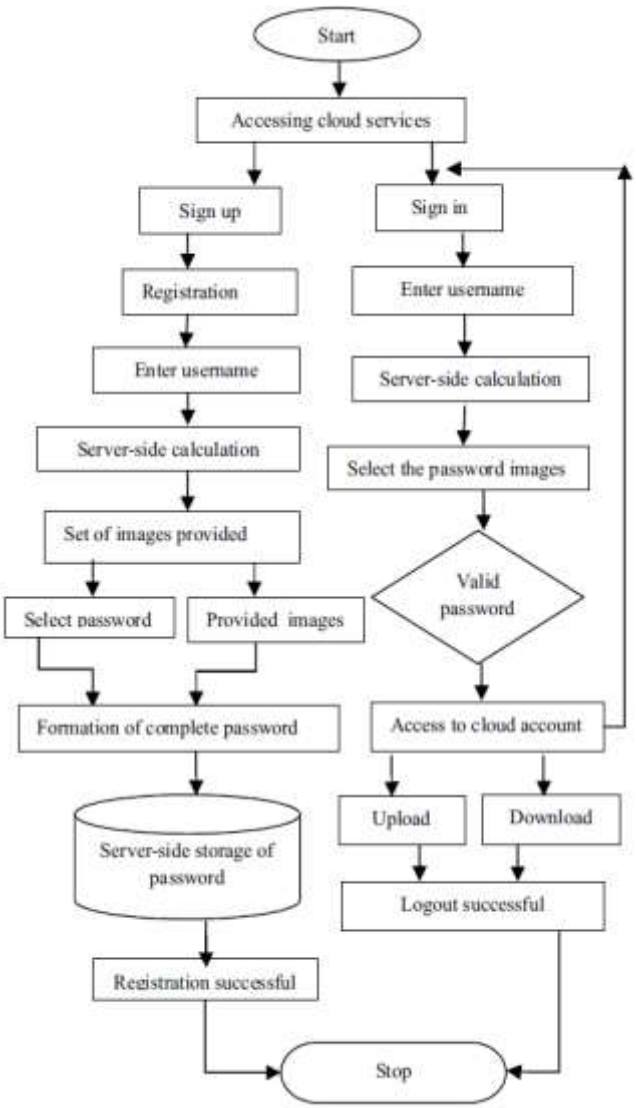


Fig 7: Flow chart of Graphical password authentication scheme

FUTURE SCOPE

Providing static time security is less secure than dynamic security mechanism. Our system is dynamically secure but in future we will need is more dynamic mechanism to secure our data. During graphical password processing speed is a biggest concern. So in future mechanism can be analyzed & faster scheme can be implemented with highly security.

CONCLUSION

Thus we can use graphical password authentication for cloud platform. This new scheme solves the many problems of existing system. The Shoulder surfing attack is also reduced using Graphical Password Authentication. It will certainly be a tremendous enhancement especially in the areas where high security is the main issue and time complexity is secondary. It can be used for applications like, in a firm or industry or institute where it will be accessible only to higher designation people, who need to store and maintain the important and confidential data secure. This will significantly reduce the hacking chances of password by attacker.

ACKNOWLEDGEMENT:

We would like to acknowledge and extend our heartfelt Gratitude to our guide prof. Suchita Wankhade and Prof. Rakhi Bhardwaj for encouragement and support.

REFERENCES

[1] Authentication Using Grid-Based Authentication Scheme and Graphical Password by Vijayshri D. Vaidya1 Department of Computer engineering SND COE & RC Yeola, India Imaran R. Shaikh2 Department of Computer engineering SND COE & RC Yeola, India, Volume 4, Issue 7, July 2015. [1]Authentication Using Grid-Based Authentication Scheme and Graphical Password by Vijayshri D. Vaidya1 Department of Computer engineering SND COE & RC Yeola, India Imaran R. Shaikh2 Department of Computer engineering SND COE & RC Yeola, India, Volume 4, Issue 7, July 2015.

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

[3] An Optimized Approach to Secure Password Graphical Images in Cloud Computing by Teshu Gaurav Singh1, Mr. Somesh Dewangan, Dhairya Kumar,10-11 April 2015

[4] A Survey n Recognition-Based Graphical User Authentication Algorithms by Farnaz Towhidi, Imaran R. Shaikh, Vol. 6, No. 2, 2009

[5] A Survey on Recall-Based Graphical User Authentic- ations Algorithms by D.Aarthi, r.K.Elangovan, Vol.2 Issue. 2, February- 2014

[6] A Survey on Different Graphical Password Authentication Techniques by Saranya Ramanan, Bindhu J S, Vol. 2, Issue 12, December 2014

[7] Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice, by Susan Wiedenbeck,Jean-Camille Birget, July 68, 2005.

[8] Graphical Passwords as Browser Extension: Implementation and Usability Study by Kemal Bicakci, Mustafa Yuceel, Burak Erdeniz, Hakan Gurbaslar, Nart Bedin Atalay

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

[9] Pass-Go, a New Graphical Password Scheme Hai Tao, Ottawa, Canada, June, 2006
[10] Enhancing Mixing Recognition-Based and Recall-Based Approach Graphical password Scheme by mar Zakaria, Toomaj Zangooei, Mohd Afizi Mohd Shukran, Volume4, Number15, September2012
[11] Authentication Using Grid-Based Authentication Scheme and Graphical Password Vijayshri D. Vaidya, Imaran R. Shaikh, Volume 4, Issue 7, July 2015
[12] Shoulder Surfing Resistant Password Authentication Mechanism (Using Convex hull Click Scheme) by Professor Sandeep Samleti, Chandan Kumar, Vijay Prakash, Nitin Kumar, Sunil Kumar,Vol. 3, Issue 3, March 2014

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785