

THREE WAY GRAPHICAL PASSWORD AUTHENTICATION

Prof. R. S. Yenape¹, Ashwini Waghmare², Diksha Madhave³, Jayashree Rokade⁴,
Shamali Thorve⁵

¹Asst. Professor, Department of Computer Engineering, SAOE, Maharashtra, India

²Student, Department of Computer Engineering [B.E], SAOE, Maharashtra, India

³Student, Department of Computer Engineering [B.E], SAOE, Maharashtra, India

⁴Student, Department of Computer Engineering [B.E], SAOE, Maharashtra, India

⁵Student, Department of Computer Engineering [B.E], SAOE, Maharashtra, India

ABSTRACT

When it comes to security it becomes very difficult to remember password which is in alphanumeric form. According to psychological studies it is very easy for human to remember images rather than numbers or words. When any application is having user friendly authentication, it becomes very easy to use that application. In this paper we are giving three way graphical password authentications by providing set of images. Authentication deals with the identification of the user and in this paper we are identifying user by checking an image which is selected as password. Text based scheme is more prone to dictionary attacks as cracking the password in the text based scheme is very easy. If the number of possible images are large enough then it provides better resistance to dictionary attacks. By using this system we can provide security to different types of application in an user friendly manner. We can provide security to cloud also. In this system selectable images are used and users have to select one image from the given set of images. This image will be set as password for login purpose. In alphanumeric password at least eight characters are used to set a password which is very easy to crack whereas in three way graphical authentication image is selected which is providing memorable password and more security. Graphical password provides better security, easy to remember, very difficult to crack and also user friendly choice. Therefore three way graphical password authentication is a best alternative solution to the alphanumeric password.

Keyword:- Authentication, graphical password, security.

1. INTRODUCTION-

In real world we are dealing with the number of different applications that contain sensitive information. To provide good authentication to that applications different approaches are used such as token based authentication, biometric authentication, knowledge based authentication. Most of the applications use knowledge based authentication. In knowledge based authentication alphanumeric password are used which contain combination of words, numbers. Alphanumeric password is very difficult to remember for human being. Alphanumeric password is not much secure. Human can easily remember images rather than numbers or digits. Graphical password means we are providing image as password. We are giving different set of images to user from that user have to select one image as his password. When he will login then that image will be checked three times. Therefore strong authentication is provided to the system. We can use this system for cloud also which will provide more security to cloud.

2. LITERATURE SURVEY

Authentication deals with security that means “to authenticate” or means “to authorize”. Now a days various authentication techniques are available. But are these actually secured and safe? We can deal with graphical password as they are better alternative to text based scheme, motivated partially by the fact that human can remember pictures better than text. Humans are prone to easily remember or recognize pictures or images. In addition it increases the possibility of password to be secured than text based scheme as they can offer better resistance to dictionary attacks[1].

For information security authentication is first step. In that user have to remember their password for login time. Traditionally we are using textual password which are used for providing security. But sometimes it is vulnerable to shoulder surfing attack so it's better to use graphical password to overcome this attack. Session password is the new technique introduced which is the combination of text and images to solve the security issues. Whenever password is created for authentication, we can use session password for security purpose[2][3].

3. EXISTING SYSTEM

A. Image based scheme : Image-based schemes use images including photo graphics, artificial pictures, or other kind of images as background. Based on the number of images displayed, we further divide image-based schemes into two subclasses: single-image schemes and multiple-image schemes.

1) Single-image based :- Single-image based schemes, Single image is provided to user, they have to select particular points.



Fig -1. Single imaged Based

2) Multiple-image based :- In this scheme number of images will provided to user they have to select one or more of them.



Fig -2. Multiple-image Based

Advantages :-

- User can easily remember the password as it given in images.

Disadvantages :-

- Image based password is very long process user have to pass through selection of number of images.
- It consumes user's time also.

B. Triangle Schema : In this scheme user is provided with convex surface. Users have to select the points from that forming particular triangle.

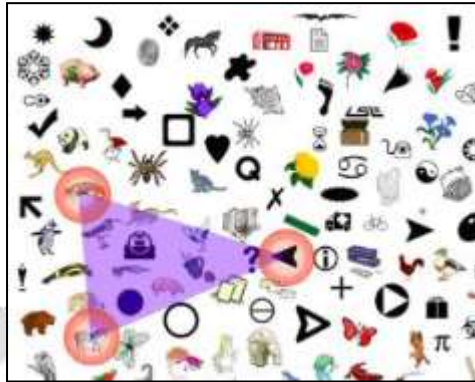


Fig -3. Triangle schema

Advantages :-

- In this scheme the display is very crowded so not able to guess the password.
- Numbers of images shown are almost same, it is difficult to distinguish.

Disadvantages :-

- As it has convex surface assigning process takes longer time and number of attempts.

C. Hybrid textual authentication : In this scheme user have to rate the number so as to find the particular color Sequence and have to remember that.

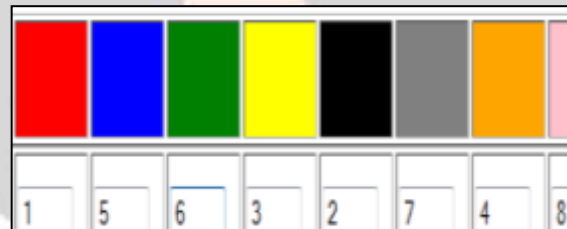


Fig -4. Hybrid Textual Authentication

Advantages:-

- In this method colors are already given user only have to remember the rating.
- Very easy to assign no special algorithm is used.

Disadvantages:-

- It is somewhat difficult to remember colors with sequence.

4. PROPOSED SYSTEM ARCHITECTURE

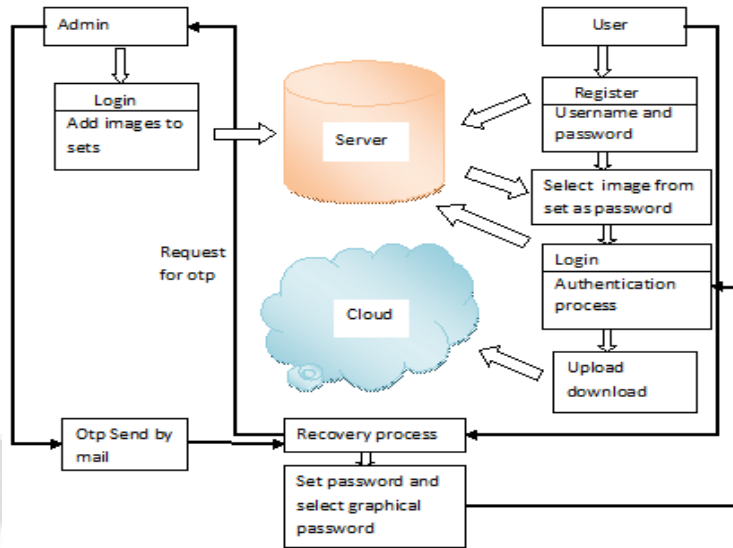


Fig -5. Proposed system architecture

5. PROPOSED SYSTEM FLOWCHART

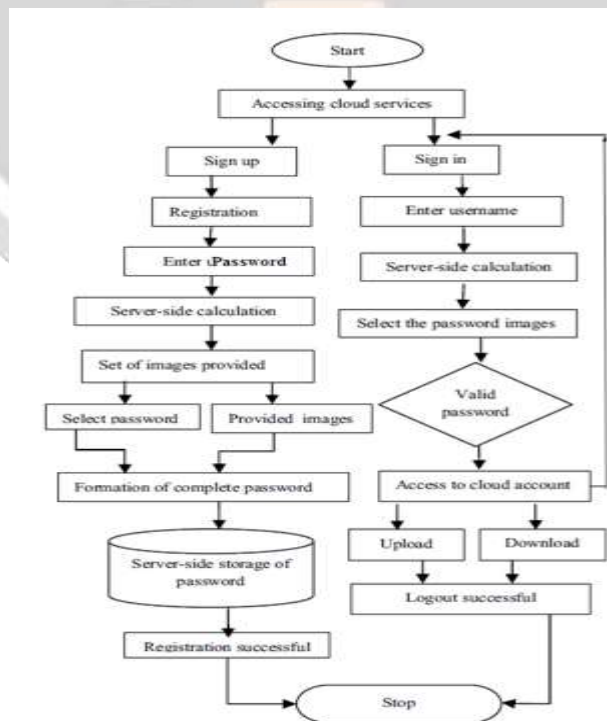


Fig-6. Proposed System flowchart

6. PROPOSED WORK

A. Start

In this system we are giving username and password. On the basis of password the process will be started at server side. In that we are providing different sets and in that different images are added by the server. On the basis of the password calculation particular set will be given to user from that set user will be select one image as password for future login.

Password: ABCD

B. Calculation on the basis of password

At the server side we are assigning position to the alphabet and according to that number we will perform addition. After that we will consider first digit of that result.

Alphabets	A	B	C	D
position	1	2	3	4

Finding set to be assigned

Calculation of result : $A+B+C+D=10$

In these we will consider first digit 1 and forwarded for further calculation.

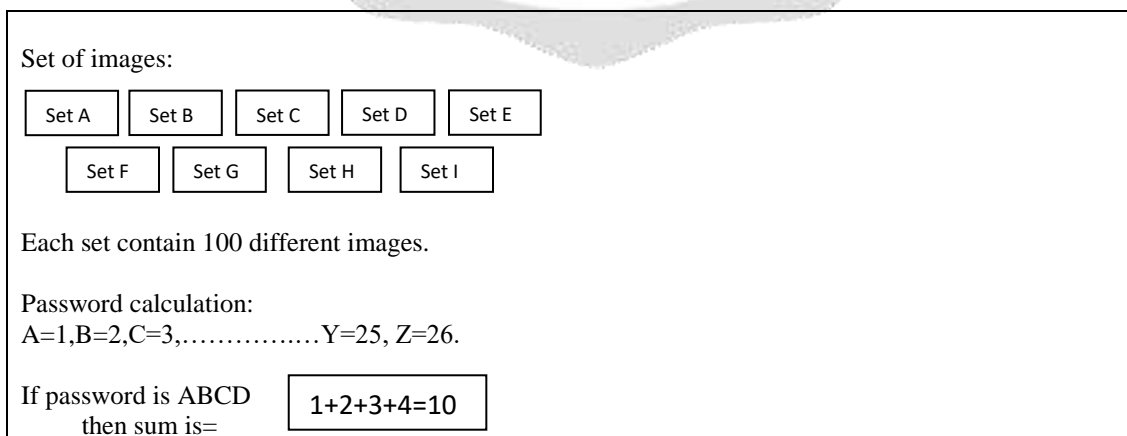
C. Assigning set of images

In the alphabet series there are 26 alphabets. All the numbers start with 1- 9. Asset of images has been made by server which will assign the resulted image to the set that we got in the second step. 1-9 numbers will be assign to that sets like

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

So if first digit is 1 then it will be assigned to set A. If first digit is 2 then it will be assigned to set B.

D. Flow of proposed system



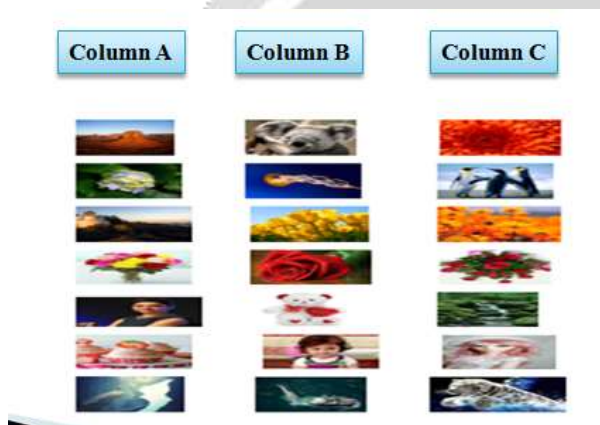
Set of images will be assigned from Set A

Select image that is to be set as the password image

Print "image successfully assigned for password for particular user".

Login steps for user:

1. Enter user ID and textual password.
2. Display 21 random images including the actual password image from the particular assigned set in 7*3 tabular format



3. Select the column that contains the password image.
4. Repeat step 3 for three times.
5. Compare the actual password image from the database with the user selected image.
If(selected image= = password image)
then
 Print "login successful"
Else
 Print "unauthenticated user".
- 6.End.

7. CONCLUSION AND FUTURE WORK

The preliminary analysis suggests that graphical password technique achieve better security than conventional textual password. In the future we can use many more than one algorithm in the system. So it will confuse the user to identify which algorithm is applied. It can also be useful for user in security point of view. Images are different for case, so if hacker try to match each combination to find the correct password it will take lots of time. The Proposed scheme provides Strong Authentication as well as it provides user friendly system.

8 . REFERENCES:

- 1) 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
- 2) Authentication for Session Password Using Colour and Images by jai patel,SNJB's COE Computer Engineering
Department, University Of Pune.Ganeshkhind,Pune. December 2013
- 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 as Browser Extension: Implementation and Usability Study1,Kemal Bicakci1, Mustafa
Yuceel1, Burak Erdeniz2, Hakan Gurbaslar2, NartBedin Atalay3
- 5) Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice Susan Wiedenbeck Jim
Waters College of IST Drexel University Philadelphia
- 6) Design and Evaluation of a Shoulder-Surfin Resistant Graphical Password Scheme Susan Wiedenbeck and Jim
Waters College of IST Drexel University Philadelphia, PA 19104 USA
- 7) 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
- 8) Authentication Using Graphical Passwords: Basic Results Susan Wiedenbeck Jim Waters ,College of IST Drexel
University Philadelphia, PA, 19104 U