ISSN (e): 2250 – 3005 || Vol, 04 || Issue, 11 || November – 2014 ||
International Journal of Computational Engineering Research (IJCER)

Authentication Using Graphical Password

Mayur Patel[1], Nimit Modi[2]
[1]Department of CE Sigma Institute of Engineering, Baroda, India
[2] Assistant Professor Department of CE Sigma Institute of Engineering, Baroda, India

ABSTRACT:
This paper introduces image based captcha to protect user data or unauthorized access of information. In that password is created from images and text password. Current system is based on only text password but it has disadvantages small password mostly used and easy to remember. This type of password is easy to guess through different attack i.e. dictionary attack and brute force attack. In this paper we have proposed a new image password scheme. In this Recognition based technique is used with numerical password which provide more security and easy to remember text and graphical password.

KEYWORDS: *Captcha, brute force attack, Authentication, Graphical Password, images, security, dictionary attack.*

I. INTRODUCTION

Security is most important in our daily life. CAPTCHA standing for "Completely Automated Public Turing test to tell Computers and Humans Apart", is an automatic challenge-response test to distinguish between humans and machines [2].Captcha is used for protection against different attack i.e. bot.In image based captcha is click based graphical passwords, where sequence of clicks on an image is used to derive a password. It provides protection against online dictionary attacks on password. In this for login every time click on images. Captcha can be applied on touch screen devices where on typing passwords is not more secure, especially for secure internet applications such as e-banks. For example ICBC (www.icbc.com.cn) used captcha. This bank is largest bank in world for every login user has to solve Captcha challenges. Captcha helps to reduce spam emails [1].In early system only text password is used which is very difficult to remember if enter a long password. If we use smaller password then it can be easily identify and we also use common password for many accounts so for that Image based captcha provide more security during authentication.

Literature Survey : Bin B. Zhu [1] implemented the Captcha as Graphical Passwords-A New Security rimitive Based on Hard AI Problems. This authentication system is based on Animal Grid and Click text which can be used in smartphone as well as desktop computers. Hossein Nejati [2] implemented the DeepCAPTCHA: An Image CAPTCHA Based on Depth Perception. In this system 6 images of different objects and different sizes of images is used and user task is to order these images in terms of their relative size. Hadyn Ellis [3] implemented the Science behind Passfaces. In this system 3x3 grid is used. User also uses the human faces or a numerical keypad value this value is corresponds to the faces on the grid. In that at least 3 to 7 faces user have to select for login process. But in this system required login time can be increased if user selects more passfaces.

P. R. Devale [4] implemented Cued Click Points with Click Draw Based Graphical Password. In this system increasing security using secret drawing in particular image during authentication process. Correct password or incorrect password is displayed after final click.Pankaja Patil [5] implemented Graphical password authentication using persuasive cued click point. In this system after filling the form user can select user define picture or system define picture after that user have to click any pixels in the images as click point to create graphical password. During creation of password one view port that is randomly positioned on the image User also change this view port if user does not want that view port. View port can be changed using Shuffle. During registration phase user has to click 5 point within that view port and at a login time sequence must be in correct order.Nilesh Kawale [6] implemented A Recognization Based Graphical Password System. In this system 3x3 grid is used. During registration phase user has to select 3 images from that grid. After completion of registration process one message send to user mobile which contain a password which is entered during login phase. During login phase user have to enter username which is entered during registration phase, text password, and select 3 images from current grid which is selected during registration phase.Darryl D'Souza [7] implemented Avatar Captcha: Telling Computers and humans apart via face classification. In this system based

on combination of human faces and Avatar faces. In that 2 rows are used each row having 6 images total 12 images in that. Each images having checkbox which is used to select only avatar faces for successful login.
Robert Biddle [8] discussed on Graphical Passwords: Learning from the first Twelve Year. A survey and conducted a brief study on existing graphical password techniques.
Mohamed Sylla [9] implemented Combinatoric Drag Pattern Graphical Password. In this System one graphical keyboard is provided to user for selection of a password. During selection of password user has to choose set of characters from the graphical keyboard. These characters shown in textbox. User must follow the sequence for creation of password. After that system check password if it is not strong then system suggests different character between passwords. And for that user has to draw pattern for that to create a password.

II. EXISTING SYSTEM

Graphical Password was originally defined by Blonder (1996).In graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques. In Recognition based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he selected during the registration stage. In recall based graphical password, a user is asked to reproduce something that he/she created or selected earlier during registration phase [5].Existing System is based on recognition techniques in that A. Click Text and Animal Grid two method introduce. A. Click Text In this method 33 Capital Letters except I, J, O, and Z digits except 0 and 1, and three special characters #,@,and &.The last three characters is used to balance the security. Characters were arranged in 5 rows. Each character was randomly rotate from -30 degree to 30 degree and scaled from 60% to 120%.Neighboring characters could overlap up to 3 pixels [1].

"Figure 1. Click Text image with 33 characters [1]."

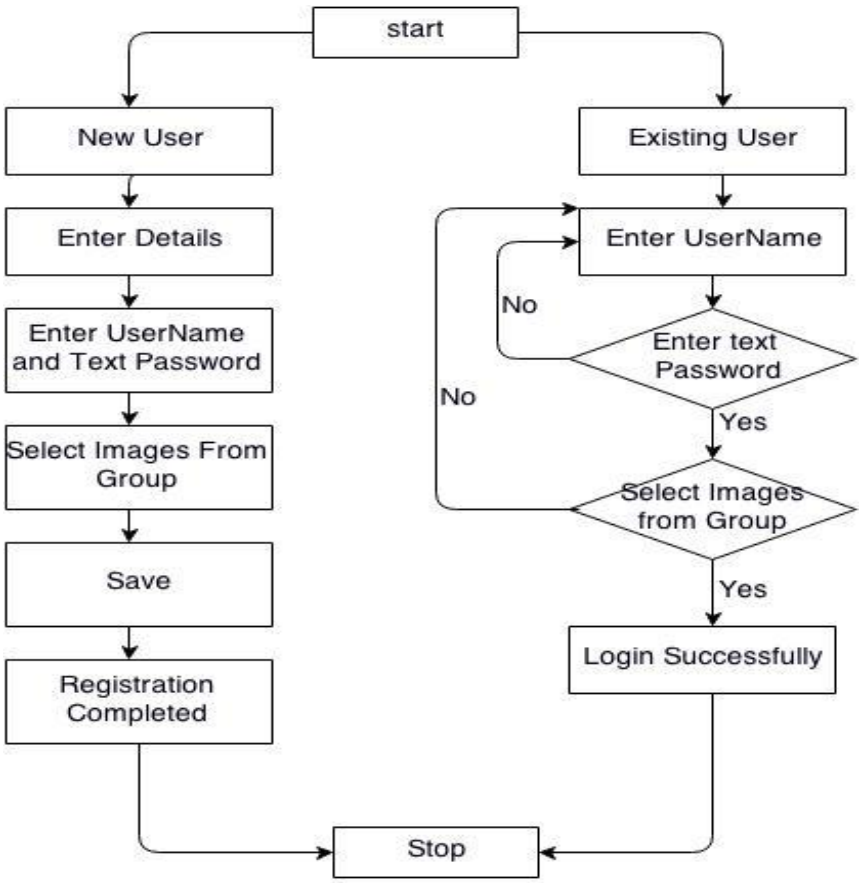
B. Animal Grid : In this method 10 animals used: bird, cow, horse, dog, giraffe, pig, rabbit, camel, element and dinosaur. Each animal had three 3d models.3d animal model was randomly selected and posed at a random view in generating a 2d object. Each click animal image was also set to 400 by 400 pixels. A 6x6 grid was used for CAS. Cells were labeled clockwise starting from cell 0.

"Figure 2. Click Animal images (left) and 6x6 grid (right) [1]."

The main disadvantage of above two methods is increasing load on system. Click text letters overlap with each other so it is time consuming sometimes during login process. In Animal grid 3d model is used and size of each animal is smaller. It does not protect from shoulder surfing attack. There is no theoretical model for this System.

III. PROPOSED SYSTEM

Our system is based on Recognition Technique. In this three different group of image is used in that 1.Famous Places 2. Famous People 3.Reputed Company Name. Each group contains 25 images. User has to select at least one image from each group during registration phase. During login time user has to click on that images which is selected during registration phase. This system provide protection against shoulder surfing attack, dictionary attack, brute force attack using text password as well as graphical password.



"Figure 3. Architecture Diagram of System."

IV. CONCLUSION AND FUTURE WORK

Our graphical password system provides more security to data and protection against different attack. Our graphical password system is based on text password and graphical password. For successful login user has to select correct image which is chosen by user during a registration and this system provide text password which provide more security to data. Future work is based on Pattern.

V. AKNOWLEDGEMENT

The authors wish to thank the Management, Principal, Head of the Department (Computer Engineering) and Guide of Sigma Institute of Engineering for the support and help in completing this work.

REFERENCES

[1] Bin B.Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu. Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems. IEEE TRANSACTIONS ON INFORMATION FORENSIS AND SECURITY, VOL.9, NO 6, June 2014.

[2] Hossein Nejati, Ngai-man Cheung, Ricardo Sosa and Dawn C.I.Koh. DeepCaptcha: An Image CAPTCHA Based on Depth Perception. ACM digital Library, March 2014.

[3] Hadyn Ellis. The Science behind Passfaces. www.realuser.com,Feb 2012.

[4] P.R.Devale Shrikala, M. Deshmukh and Anil B.Pawar. Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme. International Journal of Soft Computing and Engineering, Volume-3, Issue-2 May 2013.
[5] Iranna A M and Pankaja Patil. Graphical Password Authentication using Persuasive Cued Click Point, International Journal of Advanced Research in Electrical,Elecrtorics and Instrumentation Engineering, Vol.2, Issue 7, July 2013.
[6] Nilesh Kawale and Shubhangi Patil. A Recognization Based Graphical Password System. International Journal of Current Engineering and Technology, Vol.4, No.2, Apr 10, 2014
[7] Darryl D'Souza Phani, C.Polina, Roman V and Yampolskiy.Avatar Captcha: Telling Computers and humans apart via face classification.IEEE, 2012.
[8] Robert Biddle, Sonia Chiasson and P.C.van Oorschot. Graphical Passwords: Learning from the First Twelve Year. School of Computer Science, Carleton University, Jan 4, 2012.
[9] Mohamed Sylla, Gul Muhammad, Kaleem Habib and Jamaludin lbrahim.Combinatoric Drag-Pattern Graphical Password. Journal of Emerging Trends in Computing Information Sciences, Vol.4,No.12,Dec 2013.