JCSE International Journal of Computer Science and Engineering Open Access
Research Paper Volume-2, Issue-4 E-ISSN: 2347-2693

Graphical Password for Authentication

Nirmal Patil[1*], Gaurav Patil[2], Swapnil Patil[3], Chaitali Jadhav[4] and Santosh Durugkar[5]

[1*,2,3,4,5]*Department of Computer Engg, University of Pune, India*

www.ijcaonline.org

Received: 09/03/2014 Revised: 23/03/2014 Accepted: 21/04/2014 Published: 30/04/2014

Abstract— The main issues of knowledge-based authentication, generally text-based passwords, are well identified. A Password authentication system is a need of any application or any web service. Password authentication system is responsible for authentication of user for making entrance into a system. Users tend to choose memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. So that a password authentication should be stronger as compare to current authentication system. We are proposing a graphical password authentication system instead of only text authentication. Whole system is developed using PCCP (Persuasive Cued Click Point) technique. We use persuasion to influence user choice is used in click-based graphical passwords, encouraging users to select more random click-points**.** Using this application system becomes totally secured because it uses various samples of images for authentication. By selecting points of various images as a password we can provide maximum security for authentication. Attackers will not able to attack on a system which uses this system because of only strong authentication.

***Index Term*—**PCCP(*Persuasive Cued Click-Points*); Strong Authentication; *Graphical Passwords*; Guessing Attacks ;*Usable Security*

I. INTRODUCTION

There is critical problem of security since in last two decades due to a result of getting attack by various hackers or unauthorized user, because old methods are not stronger as required for authentication, because any one can get access through it easily. As a staring we focus on common computer authentication method which is text based authentication method. So by examining all security issues in all previous methods need arises to build such a authentication system which provides high amount of security. Using graphical password authentication system user has ability to select multiple points as a password from various images [3]. These multiple points are stored in database. And next time allows user to select these points as a password. As we know that human being can able to remember images much easily as compare to text. Using this system we can avoid each kind of attack like social engineering attack as well. Idea about graphical password authentication is first proposed by Greg Blonder in 1996 but still it is not implemented completely [2]. A system stores predefined images in database as well as points on particular images and provides same for authentication to user at the time of authentication. The major aim behind developing this system is to eliminate the guessing attacks and all kind of vulnerable activity.

II. RELATED WORKS

Currently there are three methods for user authentication these are: 1) Text based authentication, 2) Biometric based authentication and 3) Graphical method. In Text based authentication system password is built by making combination of symbols, characters and number. Such a kind of password is so difficult to remember for user because of large and complex password length. And this system is not much secure as attacker gets access easily by identifying text password.

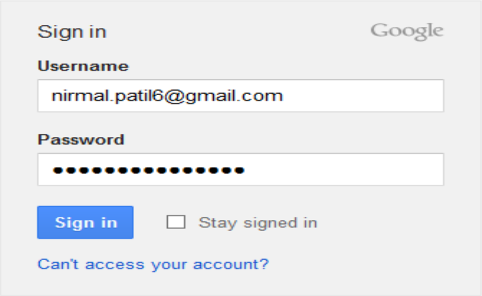

Sign in
Google
Username
nirmal.patil6@gmail.com
Password
•••••••••••••••
Sign in
□ Stay signed in
Can't access your account?

Figure: Text based authentication

Biometrical password authentication is totally based on human facial expresssion, finger prints , hand geometry and retinal patterns.The major disadvantage of this method is that this system is more expensive, and the identification process is very slow and often is unreliable.
E.g. Fingerprint

Figure: Biometric based authentication

Corresponding Author: Nirmal Patil
Department of Computer Engg, University of Pune, India

A graphical based password is one promising alternatives of text based authentication and biometric authentication. Recognize based system is the current system for the graphical authentication. In this system the user is asked to select a certain number of images from set of random pictures generated by a program later the user will be required to identify the pre-selected images in order to be authenticated. A disadvantage of this system is that the server requires storing the main source of the images of each user in the plain text [6].

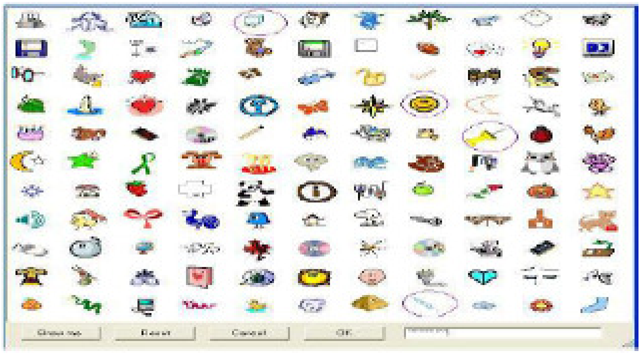


Figure: Graphical based authentication

III. Solution and Need

SOLUTION: To recover from problems occurring in previous system need arises to develop such a system which provides maximum security to user and also user friendly nature to user for strong authentication.

NEED: As we know that in last two decades attackers are continuously getting access of users profile and it is so vulnerable. To avoid all unauthorized activity need arises to develop such strong authentication system.

IMPORTANCE: Such a system is easier for user to remember the password while it is difficult for attacker to identify the password. A graphical password is one another alternative for these problems. This proposed system also provides protection against key logger, spyware. Since, computer mouse is used rather than the keyboard to enter our graphical password this protects the password from key loggers.

IV. Hypothesis

By evaluating all previous authentication method we examined that they are not much strong for authentication. So here we need a strong authentication system which provides high security to user at the time of authentication. Graphical password authentication system is a kind of system which recovers all the problems that are occurred in all previous methods.

V. Methodology

Persuasive Cued Click Point

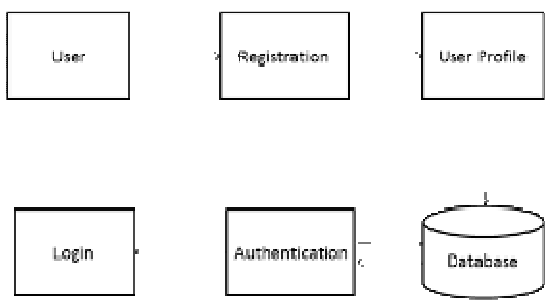
Persuasive Technology it is not a method to implement instead it is a technology which inspire to the people to behave in a desired manner. An authentication system which implements Persuasive Technology should continuous monitor the system and creates inspiration for users to select strong password for authentication, but not execute system generated password. For making this system more effective, the user must not have to ignore the persuasive elements and resulted password must be memorable. Persuasive cued click point (PCCP) makes possible this task of selecting a weak password boring and time consuming [1].

Idea behind Persuasive cued click point (PCCP) is to select random points from provided images. And PCCP provides a strong way to communicate or select a strong password between provided images and it also gives suggestion for selecting random images. Previous work on Persuasive cued click point (PCCP) shows that it is more secure method for authentication and select random points on images by using higher priority and also avoid guessing attacks [7]. Visual attention research shows that dissimilar people are involved to the same expectable area on the images. This advises that if user selects their own click-based graphical password without direction, hotspots will create question.

Encourages users to select less predictable passwords, and makes it more difficult to select passwords where all click-points are hotspots. Specifically, when users create a password, the images are slightly shaded except for a viewport [9].

The viewport is provided in this system, initially it set at any random location instead of any specific location and it is in a hidden state to avoid known hotspots. When we select points on images and if selected point is inside the viewport it will directly store that point instead of decline.

Proposed System Architecture



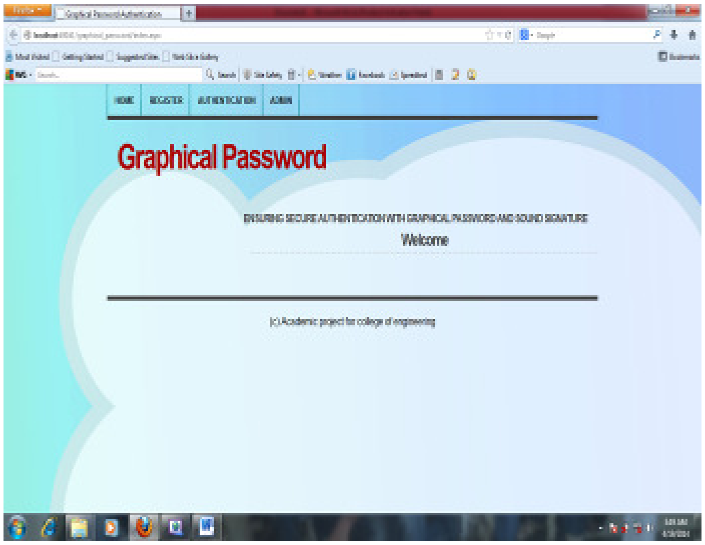
VI. Result and Discussion

Advantages

1. Human friendly password.
2. Easy for password remembrance.
3. Numbers of images are used for authentication.
4. Multiple click points for every image.
5. Two step authentications is provided.
6. Reduce the guessing attacks.

Snapshots

1)Index page



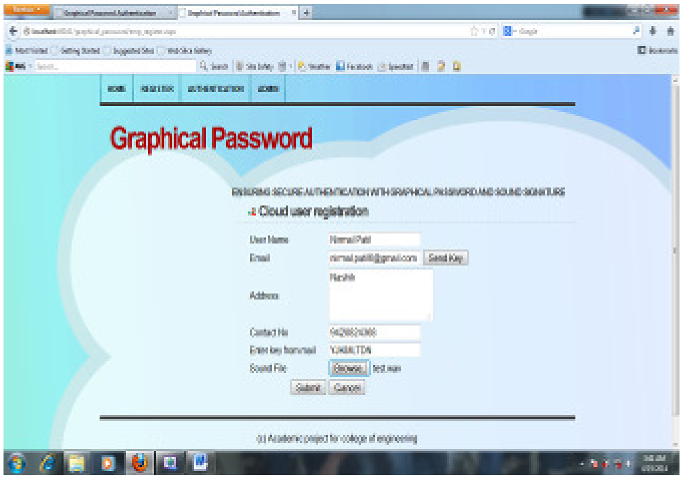
Graphical Password

ENSURING SECURE AUTHENTICATION WITH GRAPHICAL PASSWORD AND SOUND SIGNATURE

Welcome

(c) Academic project for college of engineering

2) Registration form



Graphical Password

ENSURING SECURE AUTHENTICATION WITH GRAPHICAL PASSWORD AND SOUND SIGNATURE

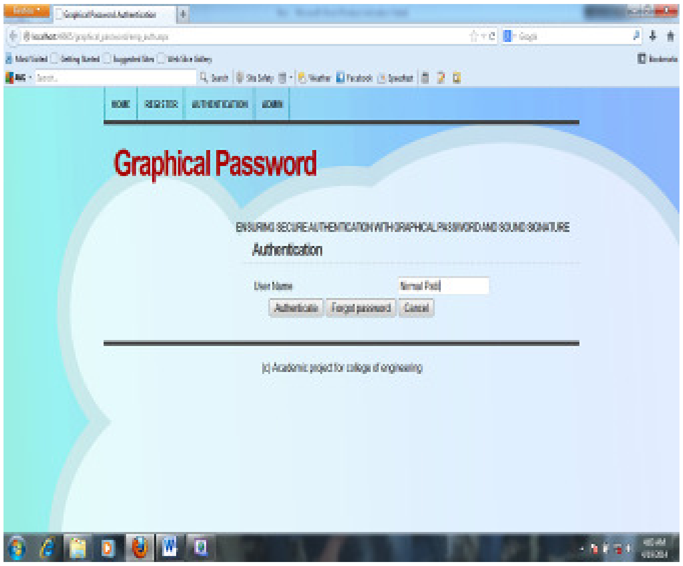
Cloud user registration

User Name	Nirmal Patil
Email	nirmal.patil8@gmail.com Send Key
Address	Nashik
Contact No	9420821088
Enter key from mail	YJAMLTDN
Sound File	Browse... test.wav

Submit Cancel

(c) Academic project for college of engineering

3) Authentication



Graphical Password

ENSURING SECURE AUTHENTICATION WITH GRAPHICAL PASSWORD AND SOUND SIGNATURE

Authentication

User Name Nirmal Patil

Authenticate Forgot password Cancel

(c) Academic project for college of engineering

4) Image authentication

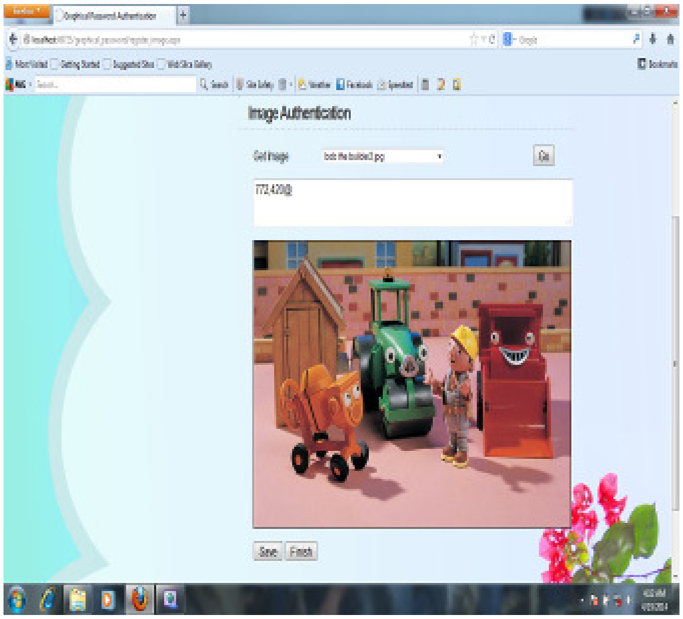


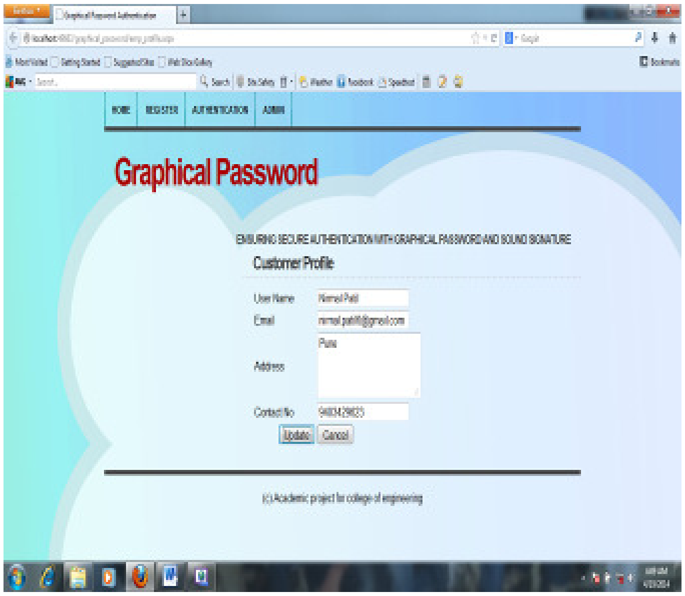
Image Authentication

Get Image bob the builder3.jpg Go

772,420@

Save Finish

5) After login



Graphical Password

ENSURING SECURE AUTHENTICATION WITH GRAPHICAL PASSWORD AND SOUND SIGNATURE

Customer Profile

User Name	Nirmal Patil
Email	nirmal.patil8@gmail.com
Address	Pune
Contact No	9403429823

Update Cancel

(c) Academic project for college of engineering

VII. Conclusion

The goal of good authentication system is to provide effective and more secure password. The graphical click point passwords are more random and strong, so that no hacker can guess it, but easy to remember. The security strength is decided by the user himself, depending upon the requirement. A major advantage of Persuasive cued click point scheme is more secure than textual passwords. There is a growing interest for graphical passwords since they are better than text based passwords, although the main argument for graphical passwords is that people can easily memorizing graphical passwords than text-based passwords. This paper gives an idea of having a effective authentication system, which provides strong and easily remembered graphical passwords with dynamic security.

VIII. Scope for Further Research

In future we add scope to this system by providing messaging on mobile devices if any kind of attacks is going on. By making this we can again recover from unauthorized activity and makes secure to user profile.

References

[1] S. Chiasson, E. Stobert, A. Forget, R. Biddle, P. Oorschot, "Persuasive Cued Click-Point: Design, Implementation, and Evaluation of a knowledge-based authentication mechanism", IEEE Transaction on Dependable and Secure Computing, Volume 09 No 2, Issue: March-April 2012.

[2] M. Patel, Y. Kadam, R. Thombare, H. Patil, "Defences against large scale online password guessing attacks by using persuasive click points", International Journal of Communication and Engineering, Volume 3 No 3, Issue 1, March 2012.

[3] Iranna A M, Pankaja Patil, "Graphical password authentication using persuasive cued click point", IJAREEIE Volume 2, Issue 7, July 2013.

[4] K. Hari Krishna, "Persuasive click points based large scale online password guessing attacks", CSEA Volume 04, Issue: 01-2013

[5] T. Chippy, R. Nagendran, "Defences against large scale online password guessing attacks by using persuasive click points", IJCE Volume 03, Issue:01 March 2012

[6] F. Towhidi, M. Masrom, "A Servey on recognition based graphical user authentication algorithms", IJCSIS, Volume 6, No 2, 2009.

[7] Devi Srinivas, M.L.Prasanthi, "Implementation of knowledge based authentication system using persuasive cued click points", IOSRJCE, volume 12, Issue 2, May-June 2013.

[8] Saurabh Sing, Gaurav Agarwal, "Integration of sound signature in graphical password authentication system", IJCA, volume 12, No 9, Jan 2011.

[9] D. Anu Radha, "A persuasive cued click point based authentication mechanism with dynamic user blocks", IJREAT, Volume 1, Issue 1, March 2013.

Authors Profile

Nirmal Patil is a student of BE Computer in Late G. N. Sapkal C. O. E. Nasik.

Gaurav Patil is a student of BE Computer in Late G. N. Sapkal C. O. E. Nasik.

Swapnil Patil is a student of BE Computer in Late G. N. Sapkal C. O. E. Nasik.

Mr. Santosh Durugkar is a professor in computer department of Late G. N. Sapkal C. O. E. Nasik.

Chaitali Jadhav is a student of BE Computer in Late G. N. Sapkal C. O. E. Nasik.