*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 3 (Jul. - Aug. 2013), PP 20-24*
*www.iosrjournals.org*

# Enhancing a Dynamic user Authentication scheme over Brute Force and Dictionary attacks

[1]A. Sai Kumar, [2]P. Subhadra
[1]*M.Tech (C.S.E), VCE, ligh-79, new santosh nagar colony, Hyderabad.*
[2]*Associate Professor in CSE Dept, VCE, Hyderabad.*

***Abstract:*** *The most universal computer authentication method is to use alpha numerical user names and passwords. This technique has been shown to have significant drawbacks. For example, users tend to pick passwords that can be simply guessed. Conversely, if a password is stiff to guess, then it is often tough to memorize. To tackle this setback, some researchers have urbanized authentication methods that use pictures as passwords. In this paper, we accomplish complete assessment of the obtainable graphical password techniques. We classify these techniques into two categories: recognition-based and recall based approaches. We discuss the strengths and boundaries of every scheme and mention the future study directions in this area. In this paper, we are conducting widespread assessment of existing graphical image password authentication technique. Also we are here proposing a new technique for graphical authentication moving towards rather advance we have been added some features like sending text to registered number and as well as registered email ids. so, in this way security is going to be increase more and more. For generating sms we are going to use some embedded devices like gsm modem. In this way we are going to increase the authentication of our application.*

***Index terms*** *: Online password secure attacks , brute force and dictionary attacks, password collections, ATTs.*

**Submitted date 20 June 2013** **Accepted Date: 25 June 2013**

## I. Introduction

Studies show that while user preserve barely memorize a partial amount of passwords, they lean to write them down or else employ the unchanged passwords for different accounts. To tackle the troubles among conventional user name password authentication, unconventional authentication methods, for instance bio-metrics, have been used. In this paper, conversely we will focus on one more option via pictures as passwords. Graphical password scheme have been projected as a probable option to text- based schemes, motivated moderately by the reality that human be capable of memorize pictures better than text; psychosomatic studies ropes such statement. Pictures are normally easier to be remembered or else recognized than text .In adding up if the amount of feasible pictures is adequately large, the possible password space of a graphical password method might exceed that of text based scheme and thus apparently offer better conflict to dictionary attacks. Owing to these advantages, there is a rising interest in graphical password .In addition to work station and mesh log-in applications, graphical passwords have also been applied to ATM machines and mobile accessories. In this paper, we carry out an inclusive study of the existing graphical password technique.

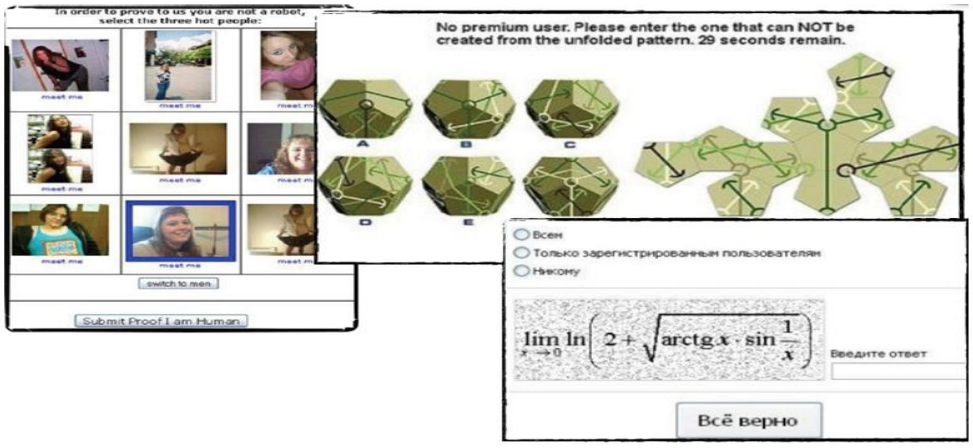


**Fig 1 : "Proof I am a Human".**

## II. Authentication Schemes

***2.1 Distinct feature/Comprehension Based Authentication*:** This kind of authentication technique consists of text base that uses passwords or Personal Identification Numbers (PINs) and graphic based authentication that uses graphics for authentication. Comprehension based authentication uses clandestine information. When user provides some information to authenticate himself as a legitimate user the system processes this information and suggest whether the user is genuine or not. comprehension based authentication is based on "Something You Know" theory in which the user types a password to login to a computer or enters his/her Personal Identification Number (PIN) to access his/her bank account from an ATM . The classic form of Distinct feature authentication is user ID and Password where the user claims his/her identity by presenting a user ID to the IT access control system. The system then checks the password for the claimed identity against its protected list of known identities and passwords. If the user ID and Password pair entered by the user match the User Id and passwords to red in the IT access control system then the user is judged to be authentic and given access to the system.

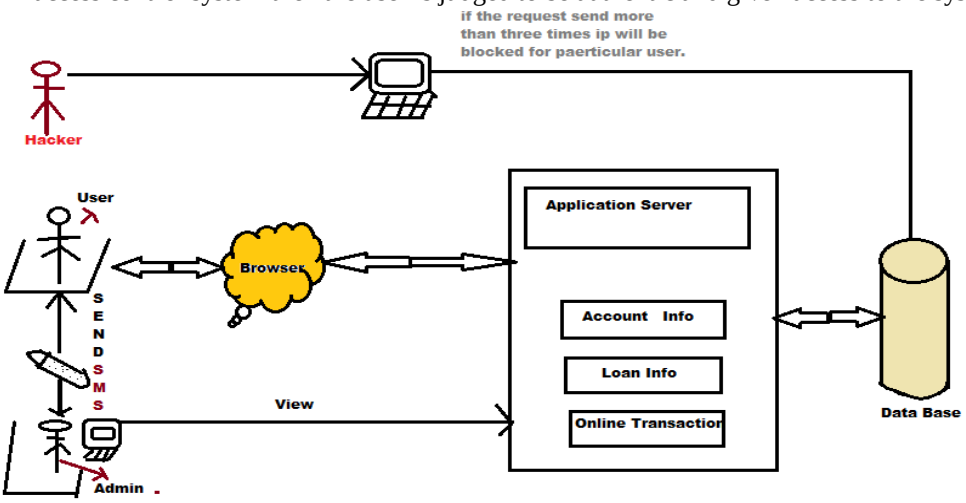


**Fig 2: DESIGN OF ARCHITECUTRE.**

***2.2 Dual Feature/Token Based Authentication***: In this method it uses a few substantial items called tokens such as smartcards, passports and physical keys. Authentication token or simply a token may be a physical device that an official user of computer is given to a id in authentication. Such a token may be physically linked or plugged into the client system. The word may refer to software token as well. Hardware tokens are typically tiny enough to be carried out in a pocket or purse and often are designed to attach to the user's keychain as well.

## III. Identifiaction and Based Techniques

***3.1. Dhamija and Perrig method*:** Dhamija and Perrig proposed a graphical authentication method based on the Hash Visualization technique. In their system, the user is asked to select a firm amount of images from a set of random pictures generated by a program. Later on the user has to identify the preselected images in order to be authenticated. The results show that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average login time, however, is longer than the traditional approach. A weak point of this system is that the server wants to store up the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be monotonous and time consuming for the user. Devisetty's algorithm is similar to the technique proposed by Dhamija and Perrig. The variation is that by using hash function SHA-1, which produces a 20byte output, the authentication is secure and need less memory. The authors recommended a probable prospect enhancement by providing persistent storage and this could be deployed on the Internet, cell phones and PDA's. Kirk Patrick sketched several authentication methods, such as picture identification objects identification and fake word identification and conducted a number of user studies. In the picture identification study, a user is trained to identify a large set of images (100-200images) selected from a data base of 20,000images. After one to three months, users in their study were able to identify over 90% of the images in the training set as per the survey.

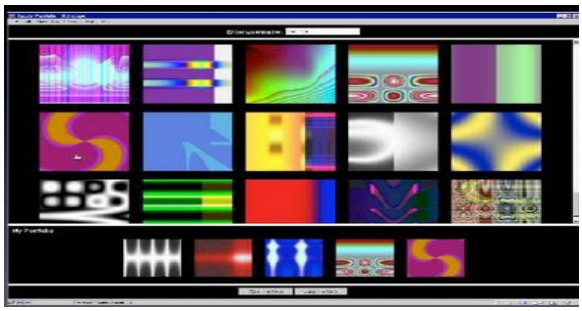

**Fig 3: Hash Visualization Techniques**.

## IV. Sample Work

Account locking is a customary device to avoid an antagonist from attempting numerous passwords for a scrupulous user name. Even though locking is generally temporary, the antagonist can mount a DoS attack by making enough failed login attempts to lock a scrupulous account. Delaying server response after receiving user credentials, whether the password is correct or incorrect, prevents the antagonist from attempting a large number of passwords in a reasonable amount of time for a particular user name. However, for adversaries with access to a large number of machines (e.g. Botnet), this mechanism is unproductive. Correspondingly deterrence techniques that rely on requesting the user machine to perform additional nontrivial computation prior to replying to the entered credentials are not effective with such adversaries.

## V. Tracing The Hacker

When a user tries to login in the company of a fictional username (e.g., typing errors), an ATT confront is set Irrespective of the password or ATT answer, the login fails. This aspect restricts attacker from learning legitimate usernames (apart from the usernames obtained by means of brute force attacks as explained and improves etiquette performance in terms of memory usage. Nevertheless from a usability approach, this is not idyllic. We anticipate that this sort of mistake would be partial in practice in part because usernames, in contrast to passwords, are echoed on a display). Tracing the hacker is done. In this the main objective is to give a lot of ATT confront to the hacker and diminish the ATT to 1 for the genuine user, which is implemented in our paper and the other quality that we have added is to chunk the hacker for that account in that machine. The hacker wouldn't be clever to try more than 3 times. But a scatty user is given an further opportunity to login after the user gets the password in his/her mobile or his/her email. According to a user from an Ip there are more than 3 login attempts an ATT is challenged if it is an hacker the ATT confront is given a lot number of times but to the legitimate user the ATT is reduced to the count of 1. In our paper we have added some extra features like,

i. Jamming the Ip for the fastidious account number
ii. Identifying the Tracker's IP and overcrowding it.
iii. ATT confront minimized to one for a legitimate user.


**Fig4: ATT Challenge.**

## VI. Cued Click Point

CCP was developed as an alternative for click based graphical password system. Where users select solitary point per image for five images the interface displays merely one image at a time the image is replaced by the next image the moment a user selects a click-point .The system determines the next image to display based on the user's click point on the current image. The next image displayed to users is based on a deterministic function of the point which is presently selected. And now it presents a one to one cued evoke scenario where each image triggers the user's memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Genuine users who see an unrecognized image know that they made a blunder with their previous click-point. On the contrary this hidden feedback is not obliging to an attacker who does not know the expected sequence of images.

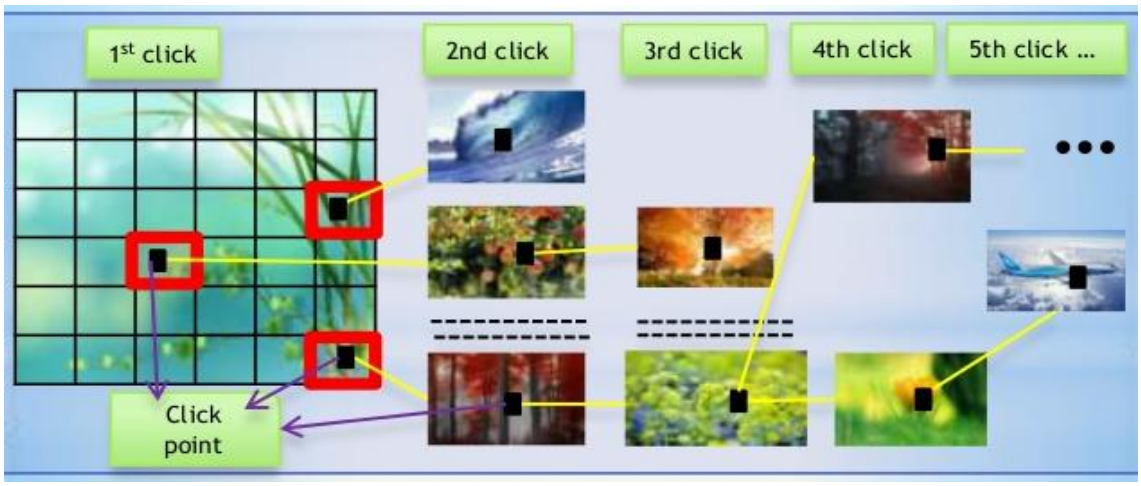


**Fig 5. Click Points as password.**

Now, Let us know how to use this Cued Click Point as Password through these simple steps below:

Step 1: Firstly, User has to enter the User name and click on NRB.

Step 2: Now, Click on PICTURE button for selecting a picture as password.

Step 3: And now, User has to select a point on the Picture and click to next picture.

Step 4: At last, the point on the last picture will be calculated as the last point for opening the desired system.

This study shows that pictures are most effectual among the schemes tested. Pseudo codes can also be used, but need appropriate setting and click inside the convex hull formed by all the pass-objects. During authentication, the user is challenged with quite a few scenes. Every scene contains more than a few pass-objects (each in the form of a randomly chosen variant)and many decoy-objects. The user has to type in a string with the unique codes matching to the pass-object variants present in the scene as well as a code demonstrating the relative location of the pass objects in reference to a pair of eyes. The quarrel is that it is very tough to crack this kind of password even if the entire authentication procedure is recorded on video because there is no mouse click to give away the pass-object information training. So this kind of click point could be useful for the legitimate users.

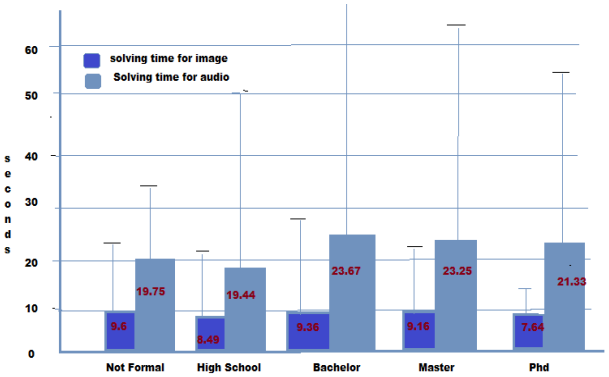


**Fig 6. Chart of image and audio solving time.**

## VII. Conclusion

We conclude this by saying that over the last decade many attempts were made by many other authors to prevent Brute force and dictionary attacks. The past decade have seen a emergent curiosity in using graphical passwords as an substitute to the usual text- based passwords. In this paper, we have conducted a wide-ranging review of existing graphical password techniques. Even though the most important quarrel for graphical passwords is that people are superior at memorizing graphical passwords than text-based passwords, the existing user studies are extremely inadequate and there is not yet credible substantiation to sustain this argument. Our preface study suggests that it is trickier to split graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. Conversely in view of the fact that there is not yet wide exploitation of graphical password systems, the vulnerabilities of graphical passwords are still not completely understood. But definitely it will comparatively decrease the Brute force attacks and helps in tracing the hacker.

## References

[1] B. Pinkas and T. Sander, "*Securing Passwords against Dictionary Attacks*," Proc. ACM Conf. Computer and Comm. Security (CCS '02), pp. 161-170, Nov. 2002.
[2] SANS.org, "*Important Information Distributed SSH Brute Force Attacks*," SANS Internet Storm Center Handler's Diary, June 2010,pp250-254.
[3] Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot, "*Revisiting Defenses against Large-Scale Online Password Guessing Attack",* feb.2012,pp.140-154
[4] M. Naor, Verification of a human in the loop, or Identification via the Turing test, Manuscript (1996). http://www.wisdom.weizmann.ac.il/~naor/PAPERS/ human_abs.html
[5] The CAPTCHA Project. http://www.captcha.net/.
[6] http://ieeexplore.ieee.org.
[7] www.wikipedia.org.