A High Secure Shoulder Surfing Resistant Text Based Graphical Password Authentication System

Ms. Krishna Amin[1], Ms.Simriti Koul [2],Ms .Priyanka Khade[3],Ms.Swaleha Shaikh[4] ,Ms.Swati Sagar[5]
Department of Information Technology Bharati Vidypeeth's College of Engineering for Womens,Pune
Savitribai Phule Pune University[1,2,3,4,5]

Abstract-

Shoulder-surfing is a known risk where an attacker can capture a password by direct observation or by recording the authentication session. Due to the visual interface, this problem has become exacerbated in graphical passwords. usability. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system Pass Matrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. By this paper we are trying to give set of images on the basis of alphabet series position of characters in username. Finally cloud is provided with this graphical password authentication.

Index Terms: Graphical Passwords, Authentication, Shoulder Surfing Attack, cloud security.

I .INTRODUCTION

EXTUAL passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect [1]. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is not a rare case that users may use only one username and password for multiple accounts [2]. According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds [3]. Textual passwords are often insecure due to the difficulty of maintaining strong ones.

Various graphical password authentication schemes [4], [5], [6], [7] were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in [8], [9], humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies [10], [11], [12]. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information [13], [14], [15].

The human actions such as choosing bad passwords for new accounts and inputting passwords in an insecure way for later logins are regarded as the weakest link in the authentication chain [16]. Therefore, an authentication scheme should be designed to overcome these vulnerabilities.

In this paper, we present a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time login indicators. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly.

II. LITERATURE SURVEY

1. **Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng,**Textual passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect.
2. **Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu**, AFUNDAMENTAL task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. For

example, the problem of integer factorization is fundamental to the RSA public-key cryptosystem and the Rabin encryption. The discrete logarithm problem is fundamental to the ElGamal encryption, the Diffie-Hellman key exchange, the Digital Signature Algorithm, the elliptic curve cryptography and so on.

3. **ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare,**When anyone wants to access the network, for security purposes every web application provides user authentication. From ancient day's secret data or code is used for hiding and giving security to information. In user authentication the process which we have to pass through is username and password. Authentication process divided into Token based authentication,

III. PROPOSED SYSTEM

They A large number of graphical password schemes have been proposed. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. Each type will be briefly described here. More can be found in a recent review of graphical passwords. As name indicates in this, various types of images or shapes are used as password. Also psychological study says that images can be easily remembered by human than text [4 -7]. Human brains can process images easily. Because of this human characteristic, graphical passwords are superior to textual passwords. As images are used it is resistant to dictionary attack, key logger, social engineering etc.

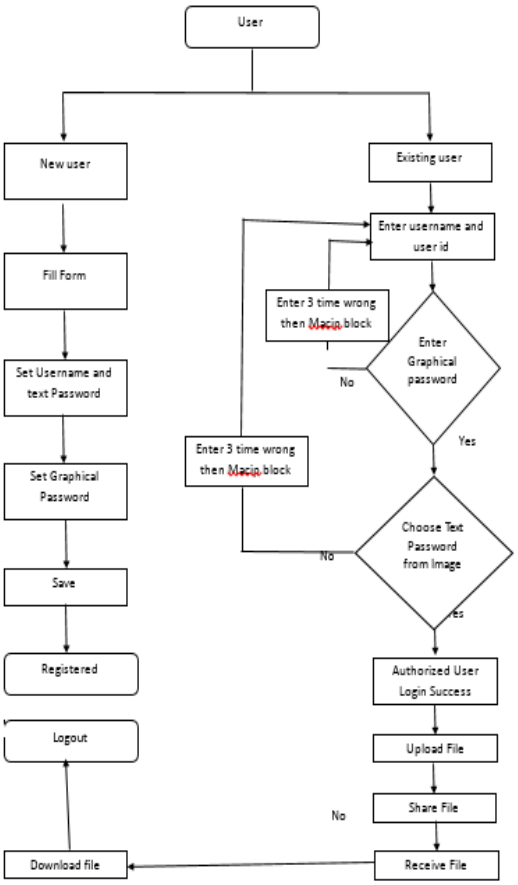

Fig. 1 Proposed System

So, as images are used in graphical password it is easy to remember and difficult to guess and it is best alternative for textual password. But it is observed that there are also some limitations of graphical password techniques and the major limitation observed is that, it is vulnerable to shoulder surfing attack as images are used as a password. Shoulder surfing means watching over the person's shoulder to get the password. When user enters password using keyboard, mouse, touch screen or any other traditional input device, a malicious observer may be able to acquire the user's password credentials.

IV. SCHEME

Input:64 character a to z=26, A to Z=26, 0 to 9=10, and ". /"=2

Output: Random Printing Algorithm:

1. To generate the matrix wit row and column 4*4.
2. Put 0 to 63 numbers into matrix.
3. Select one random number from 0 to 63.
4. For putting number into matrix system check number is already parent or not.
5. If number present then perform Setp3.If not present then put into a matrix and go to setp3.
6. Do step 5 repeatedly up to 0 to 63 inserted into matrix.
7. Print The Matrix.
8. Now Get string which have 64 character " a to z=26, A to Z=26, 0 to 9=10, and. /=2".
9. Get number present into matrix sequentially [0][0] to [4][4] i.e., total 64 character .
10. Select index of string from 64 char. put into that Current location.
11. Do step 9 and 10 repeatedly up to [4][4] number.
12. Print Current Matrix With String Char.
13. Display a matrix With Random Printing
14. Stop

V. CONCLUSIONS AND FUTURE WORK

In this paper, a new text based graphical shoulder-surfing resistant scheme was proposed. It adopts a visual login technique that matches the capabilities and limitations of most handheld devices and provides a simple and intuitive way for users to authenticate. As such, it is an example of "usable security". CaRP is both a Captcha and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new CaRP image, which is also a Captcha challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. A password of CaRP can be found only probabilistically by automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent vulnerability in many graphical password systems. Thus graphical password authentication can be given by taking cloud as a platform. The new scheme provides solves

the many problems of existing system. It can also be useful for user in security point of view.

REFERENCES

[1] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A CAPTCHA that exploits interest-aligned manual image categorization," in Proc.

[2]ACM CCS, 2007, pp. 366–374. S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[3]G. Mori and J. Malik, "Recognizing objects in adversarial clutter," in Proc. IEEE Comput. Society Conf. Comput. Vis. Pattern Recognit.,

[4]Jun. 2003, pp. 134–141. R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4./.

[5]I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.

[6]S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

[7]A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.