Minimizing Shoulder Surfing Attack using Text and Color Based Graphical Password Scheme

[1]Prof. S. K. Sonkar, [2]Prof. R. L. Paikrao
Computer Engineering Dept.
Amrutvahini College of engineering
Sangamner, India.

[3]Prof. Awadesh Kumar, [4]Mr. S. B. Deshmukh,
Computer Engineering Dept.
Amrutvahini College of engineering
Sangamner, India.

Abstract **- In current days very popular method for Authentication of User is Textual Password. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. Again this Textual Password is also vulnerable to many Attacks like Brute Force Attack, Dictionary Attack, Guessing and Shoulder Surfing. From all of this attack shoulder surfing Attack is most happening. The shoulder surfing attack in an attack that can be performed by the adversary to obtain the users password by watching over the user's shoulder as he enters his password. As we know most users are more familiar with textual passwords than pure graphical passwords, text based graphical password schemes have been proposed. But none of existing graphical password and text based graphical password schemes is both secure and efficient enough to reduce the Shoulder surfing Attack.**

So to Overcome the Problem of Existing Graphical Password Scheme, Textual Password Scheme and text based shoulder surfing resistant graphical password Scheme, the Improved Text and Color Based Graphical Password Scheme to reduce Shoulder Surfing Attack is Proposed. Using this Scheme user can efficiently login the system. The proposed scheme is used to reduce the Shoulder surfing attack and it will improve the security of existing Applications.

Index Terms — Textual Password, Graphical password, Shoulder Surfing.

I. INTRODUCTION

The shoulder surfing is a attack which can be can be performed by unauthorized user to obtain the authorized user's password by watching over the user's shoulder when he enters his password. Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone as they fill out a form, enter their PIN at an automated teller machine, enter a password at a cyber cafe, public and university libraries, or airport kiosks Shoulder surfing can also be done at a distance using binoculars or other vision-enhancing devices. Inexpensive, miniature closed-circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. To prevent shoulder surfing, it is advised to shield paperwork or the keypad from view by using one's body or cupping one's hand.

The conventional password schemes which was used previously are vulnerable to shoulder surfing, so to reduce the effect of Shoulder Surfing attack, Sobrado and Birget [2] proposed three shoulder surfing resistant graphical password schemes. Since then, many graphical password schemes with different degrees of resistance to shoulder surfing have been proposed, e.g., [3][4][5][6][7][8][9][10], and but each scheme has some advantages and Disadvantages. It seems that most users are more familiar with textual passwords than pure graphical passwords, Zhao et al. [11] proposed a text-based shoulder surfing resistant graphical password scheme, S3APS. In S3PAS, the user has to mix his textual password on the login screen to get the session password. However, the login process of Zhao et al.'s scheme is complex and tedious. And then, several text based shoulder surfing resistant graphical password schemes have been proposed, e.g. [12][13][14][15],[16].

Unfortunately, existing text-based shoulder surfing resistant graphical password schemes are not secure and efficient enough. In this paper, we will propose an Graphical Password scheme which uses color and is based on text and it provides resistant to Shoulder Surfing. The working of proposed system is very simple and the proposed system is user friendly. The system is easy and simple for the users which are already familiar with existing Textual password scheme. Using this system the system or any user can login the system easily and efficiently without using any physical keyboard or on-screen keyboard.

Objective:-

1. Usability, the proposed scheme will be usable anywhere and at any time with a low error rate as well as a faster authentication result.
2. Training, the system will provide users a simple and interesting training. They should not spend much time on training.
3. The best use of human memory, the proposed scheme will benefit from the argument that people are better in recognizing images. Therefore, pass images should be easy to remember.
4. Secure, the system will provide a strong line of defense against shoulder surfing brute force, intersection and educated guess attacks

II.LITERATURE SURVEY

In 2002, to reduce the shoulder surfing attack, Sobrado and Birget [2] proposed three shoulder surfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Triangle scheme. But from all this schemes, the Movable Frame scheme and the Intersection scheme fail frequently in the process of Authentication. In the

Triangle scheme, the user has to select and memorize several pass icons as his password. To login the system, the user has to correctly pass the predetermined number of challenges and in every challenge, the user has to find three pass-icons from a set of randomly chosen icons displayed on the login screen, and then click inside the invisible triangle created by those three pass-icons.

In 2006, to overcome the drawbacks of Sobrado and Birgets Scheme, the Convex Hull Click Scheme (CHC) is proposed by Wiedenbeck et al. [4]. It is an improved version of the Triangle scheme with great security and usability. To login the system, the user has to correctly follow several challenges and in each challenge, the user has to find any three pass-icons displayed on the login screen, and then click inside the invisible convex hull formed by all the displayed pass-icons. But this scheme Convex-Hull Click has long login time.

In 2009, To overcome the shoulder surfing attack, a graphical password scheme which uses color login and provide resistant to the shoulder surfing attack is proposed by Gao et al. [5]. In this scheme the background color is a usable factor for reducing the login time.. this Scheme has drawback like, the probability of accidental login of Color Login is too high and the password space is too small.

In 2009, a shoulder surfing resistant graphical password scheme, TI-IBA, in which icons are presented not only spatially but also temporally. TI-IBA is less constrained by the screen size and easier for the user to find his pass-icons is proposed by Yamamoto et al. [10] . Unfortunately, TI-IBA's resistance to accidental login is not strong. And, it may be difficult for some users to find his pass-icons temporally displayed on the login screen. As most users are familiar with textual passwords and conventional textual password authentication schemes have no shoulder surfing resistance.

In 2007, a text-based shoulder surfing resistant graphical password scheme, S3PAS, in which the user has to find his textual password and then follow a special rule to mix his textual password to get a session password to login the system is proposed by Zhao et al.[11]. However, the login process of Zhao et al.'s scheme is complex and tedious.

In 2011,a text-based shoulder surfing resistant graphical password scheme by using colors is proposed by Sreelatha et al. [13]. Clearly, as the user has to additionally memorize the order of several colors, the memory burden of the user is high.

In 2011, after Sreelatha, a text based shoulder surfing resistant graphical password scheme, and employed an analysis method for accidental login resistance and shoulder surfing resistance to analyze the security of their scheme is proposed by Kim et al. [14]. Unfortunately, the resistance of Kim et al.'s scheme to accidental login is not satisfactory.

In 2012, a text based shoulder surfing resistant graphical password scheme, PPC is proposed by Rao et al. [16]. To login the system, the user has to mix his textual password to produce several pass-pairs, and then follow four predefined rules to get his session password on the login screen. However, the login process of PPC is too complicated and tedious.

III.IMPLEMENTATION DETAIL

In this Proposed Scheme, we will describe a simple and efficient Method to avoid the shoulder surfing Attack using Texts and color based graphical Password Scheme. The Proposed Scheme Contains alphabets i.e 64 characters (26 Capitalc Letter, 26 Small case letters, 0-9 i.e. 10 decimal digits, two symbols"." and "/". This proposed system involves registration and the login phase. The System will work in two steps,

1. *Password Registration :*
   In the proposed scheme user has to set textual password K of length L.

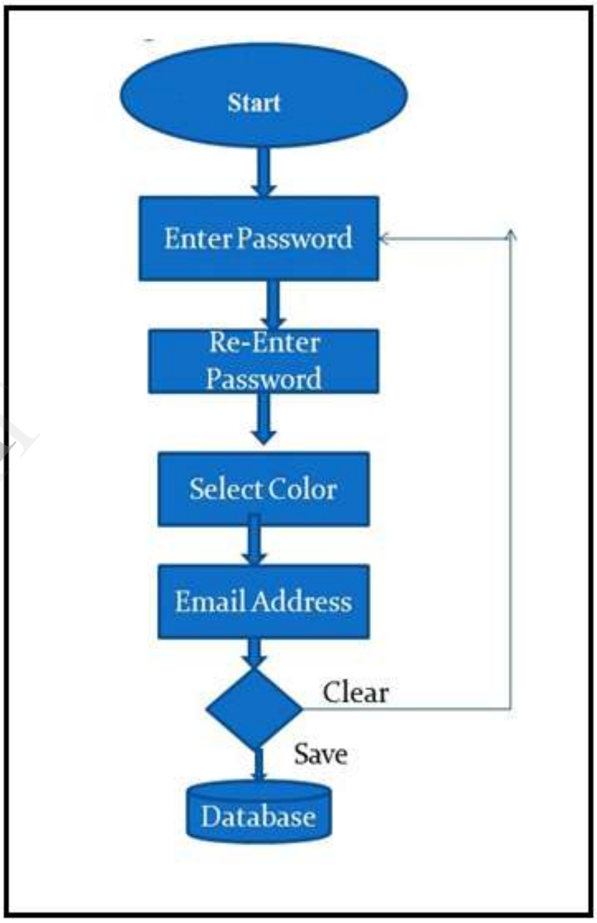
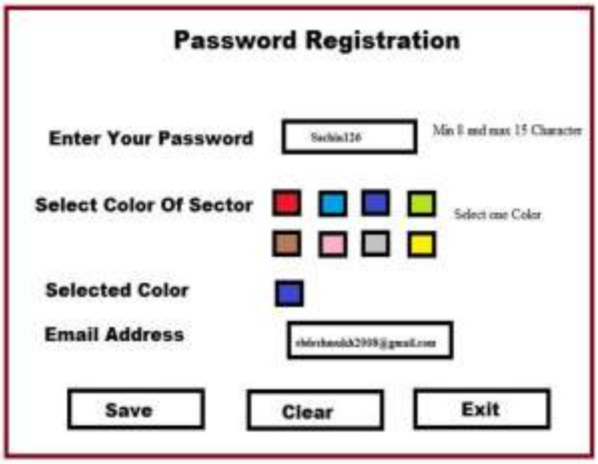


Fig.1 Flowchart of Registration Process

The minimum length of Password is 8 Characters and the maximum length of password is 15 characters i.e password length is between 8 to 15 Characters, and choose one colour as his pass colour from 8 colours assigned by the system.



Password Registration

Enter Your Password: Sachin126 — Min 8 and max 15 Character

Select Color Of Sector: 🟥 🟦 🟦 🟩 🟫 🟪 ⬜ 🟨 — Select one Color

Selected Color: 🟦

Email Address: [illegible]

Fig.2. Password Registration

The remaining 7 colours not chosen by the user are his decoy colours. And, the user has to register an e-mail address for re-enabling his account when he enters a wrong password. In this scheme, registration process should carried out in an environment free of shoulder surfing. In addition, a secure channel should be established between the system and the user during the registration phase by using SSL/TLS or any other secure transmission mechanism. The system stores the user's textual password in the users entry in the password table, which should be encrypted by the system key. So in short in registration phase the user set is textual password and select 1 Colour from 8 Colours.

2. Login:

In the login phase when an user sends an login request to the system, the system displays a circle which is composed of 8 sectors of equal Size. The colors of the arcs of each sectors is different, and every sector is identified by the color of its arc, e.g., the red sector is the sector of red arc. In this Step 64 characters are placed averagely and randomly among these sectors.

All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector counter clockwise by clicking the "counter clockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel. The login screen of the proposed scheme can be illustrated by an example shown in Figure. To login the system, the user has to finish the following steps:

Step 1: The Login Screen is shown to user.

Step 2: After the display of login Screen, The System displays a Circle Composed of 8 sectors of equal size and each sector contain 64 characters randomly and averagely distributed among the sectors. The 64 characters are in three typefaces in that the 26 upper case letters are in bold typeface, the 26 lower case letters and the two symbols "." and "/" are in regular typeface, and the 10 decimal digits are in italic typeface.
Again there is a button for rotating the circle clockwise, the button for rotating the Circle anti clockwise, the "Confirm" button, and the "Login" button are also displayed on the login screen. All the characters in sectors are rotated clockwise and anticlockwise by pressing the button clockwise and anticlockwise. The mouse wheel can also be used to move the characters from one sector to another sector. Suppose that, at the start of login session we assume one variable i , and Let i = 1.

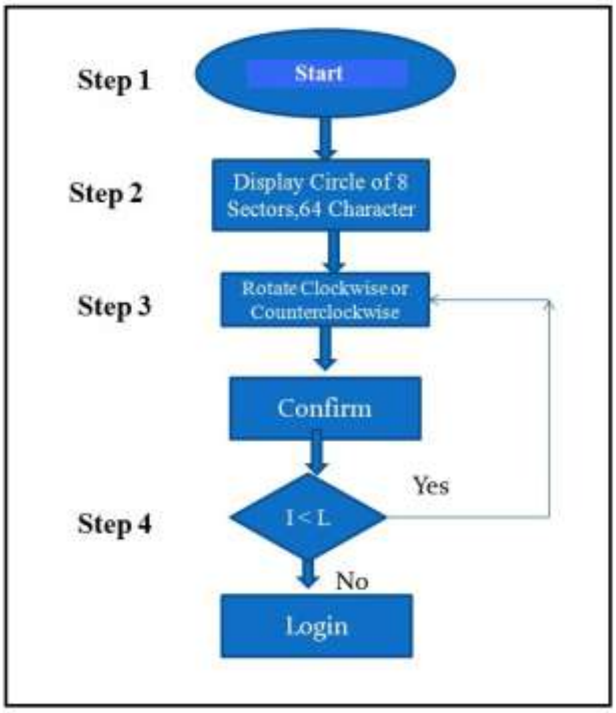

Step 1
Step 2
Step 3
Step 4
Start
Display Circle of 8 Sectors,64 Character
Rotate Clockwise or Counterclockwise
Confirm
I<L
Yes
No
Login

Fig.3. Flow Chart Of Login Process

Step 3: After step to, in step 3 user has to rotate the sector which contains the Characters of password , and has to move that character in the sector whose color is selected by user, for that purpose many rotate clockwise or anticlockwise operation are performed. After the rotation and click on the confirm button, and after the confirmation increase the value of i by 1.

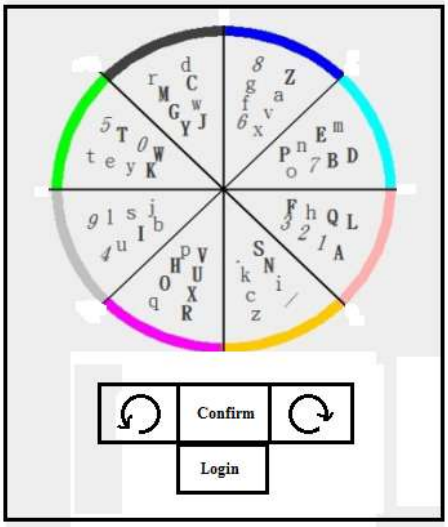


Fig.4. Login Screen

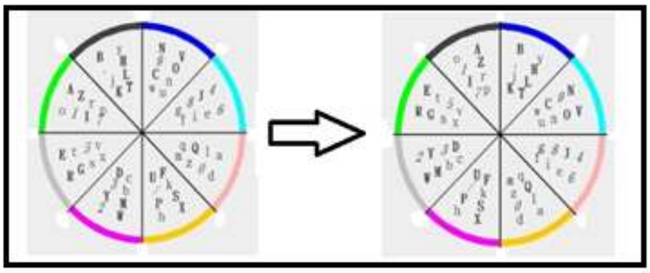


Fig. 5. Rotation Operation

Step 4: If the value of I is less than L, where L is the length of password, then perform step 3 repeatedly until the value of i becomes L , After that click on Login Button and then login process gets complete. To provide the security the user can enters the wrong password only 3 Consecutive times, If the account is not successfully authenticated for three consecutive times, this account will be disabled and the system send the link to the registered email address which can be used by authorized and correct persons to login and re-enable the disabled account. The operation of the system is shown in the figure.

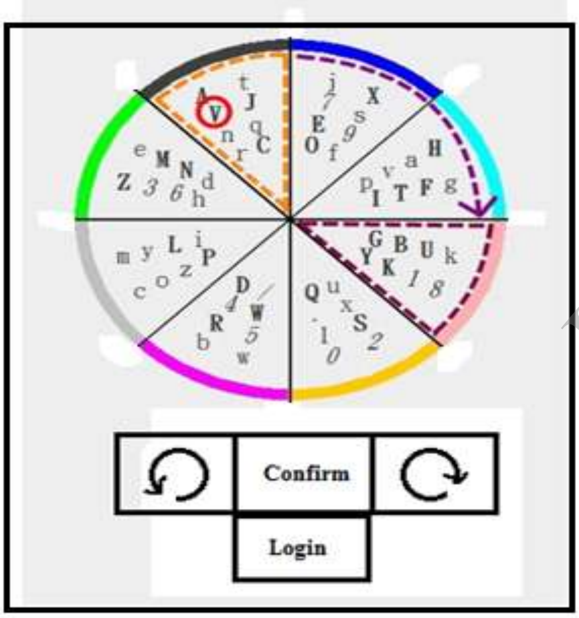


Fig.6. Example Of Rotation Operation in Login Process

IV Results

A. *Result Analysis*

The security and the usability of the proposed system will be as follows,

A. Password space

Suppose that the length password is L, i.e. 8 < L < 15 so now there are $8*64^L$ password available for use, Therefore, the password space of the proposed scheme is

$$\sum_{L=8}^{15} 8 * 64^L \approx 1.006*10^{28}$$

B. Resistance to accidental login

Accidental Login means chance of entering password accidently. The probability of entering password is 8/64, i.e., 1/8, so the probability of accidental login is , $(1/8)^{L.}$
Now consider the different values of L as shown in graph,

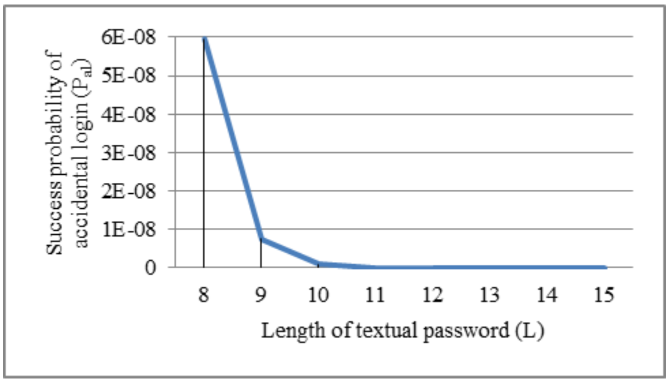


Fig. 7. Probability of Accidental Login

To provide the security the user can enters the wrong password only 3 Consecutive times, If the account is not successfully authenticated for three consecutive times, this account will be disabled and and the system send the link to the registered email address which can be used by authorized and correct persons to login and re-enable the disabled account. So the chance of Accidental login is to low.

C. Resistance to shoulder surfing

As the user has given only three chance to enter the password and if he enters wrong password account will get disabled, and to login the account user has to Select specific Color and after that user has to move the all characters of password to that sector of specific color. So the resistance to Shoulder Surfing is provided.

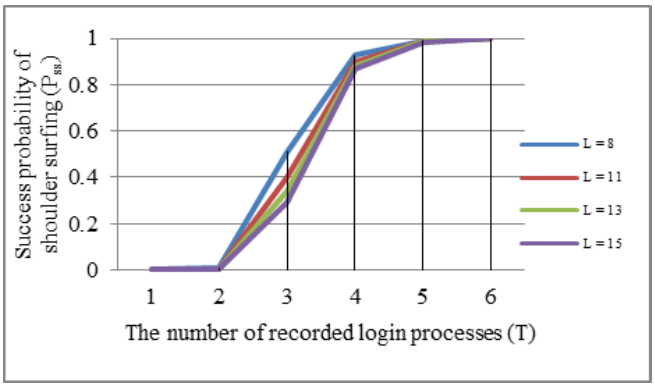


Fig.8. Probability of Shoulder Surfing

D. Usability

As we know that users The user chooses traditional textual passwords and one color as his password in the proposed scheme. As most users are familiar with textual passwords, it is usually easier for the user to find characters than icons on the login screen. In addition, since the system displays the upper case letters, the lower case letters, the symbols "." and "/", and the 10 decimal digits in three different typefaces on the login screen, the user can easily and efficiently find his pass-characters. And, the operation of the proposed scheme is simple and easy to learn, the user only has to rotate the sectors to login the system.

V. CONCLUSION & FUTURE SCOPE

In this paper we had proposed a system which uses text and color based graphical password which is useful to reduce shoulder surfing attack. Using this authentication method user can login the system without caring about shoulder surfing and he can enter the password without using physical keyboard. This method uses both textual password and color based graphical password and as the user are familiar with both this password scheme user can easily and efficiently login the system. In future we can use this system in an applications which requires high security.

REFERENCES:

1. Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh," A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme," IEEE 2nd International Symposium on Next-Generation Electronics (ISNE),February 2013 , Kaohsiung, Taiwan.
2. L. Sobrado "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4,2002
3. J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005.
4. S. Wiedenbeck and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme,"Proc. of Working Conf. on Advanced Visual Interfaces,May. 2006, pp. 177-184.
5. H. Gao, X. Liu and R. Dai, "Design and analysis of a graphical password scheme," Proc. of 4th Int. Conf. on\ Innovative Computing, Information and Control, Dec. 2009, pp. 675-678.
6. B. Hartanto and S. Welly, "The usage of graphical password as a replacement to the alphanumerical password," Informatika, vol. 7, no. 2, 2006, pp. 91-97.
7. S. Man, and M. Mathews, "A shoulder surfing resistant graphical password scheme," Proc. of the 2003 Int. Conf. on Security and Management, June 2003, pp. 105- 111 .
8. T. Perkovic, "SSSL: shoulder surfing safe login," Proc. Of the 17th Int. Conf. on Software, Telecommunications & Computer Networks, Sept. 2009, pp. 270-275.
9. Z. Zheng, and Z. Liu, "A stroke-based textual password authentication scheme," Proc. of the First Int. Workshop. on Education Technology and Computer Science, Mar. 2009, pp. 90-95.
10. T. Yamamoto, and M. Nishigaki, "A shouldersurfingresistant image-based authentication system with temporal indirect image selection," Proc. of the 2009 Int. Conf. on Security and Management, July 2009, pp. 188- 194.
11. H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," Proc. of 21st Int. Conf. on Advanced Information Networking and Applications Workshops, vol. 2, May 2007, pp. 467-472.
12. B. R. Cheng, and W. P. Chen, "An efficient login recording attack resistant graphical password scheme Sector Login," Proc. of 2010 Conf. on Innovative Applications of Information Security Technology, Dec. 2010, pp. 204-210.
13. M. Sreelatha, M. Anirudh, Md. Sultan Ahamer, and V. Manoj Kumar. "Authentication schemes for session passwords using color and images," International Journal of Network Security & Its Applications, vol. 3, no. 3, May 2011.
14. S. H. Kim, S. Y. Kim, and H.G. Cho. "A new shoulder surfing resistant password for mobile environments," Proc.of 5th Int. Conf. on Ubiquitous Information Management and Communication, Feb. 2011.
15. Z. Imran and R. Nizami, "Advance secure login," International Journal of Scientific and Research Publications, vol. 1, Dec. 2011. M. K. Rao, "Novel shoulder-surfing resistant authentication
16. schemes using text-graphical passwords," International Journal of Information & Network Security, vol. 1, no. 3, pp. 163-170, Aug. 2012 .
17. Network Working Group of the IETF, "The Secure Sockets Layer (SSL) Protocol Version 3.0," RFC 6101,2011.
18. Network Working Group of the IETF, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246,2008