IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Chromatic Password System – A Novel Method to Avoid Shoulder Surfing Attack

[1]Divya M S, [2]Kiran P S, [3]A Ramadevi, [4]Anu V B, [5]Varun K S

[1] Lecturer, Department of Studies and Research in Computer Science,
[2] Student Department of Studies and Research in Computer Science,
[3] Lecturer Department of Studies and Research in Computer Science,
[4] Lecturer Department of Studies and Research in Computer Science,
[5] Student Department of Studies and Research in Computer Science,
[1] Department of Studies and Research in Computer Science,
[1]Davanagere University, Davanagere, India

Abstract: To keep our bank account details, emails, social media accounts, personal data secure we need a password. The password system plays an important role in keeping the data safe. Protecting the password from the hackers or unauthorized users is the main challenging task. Most of the existing password systems are exposed; they may lead to the chances of hacking. The simple and common way that the hacker can guess the password is by looking over the users shoulder. In this hacker is going to watch the users shoulder when the user enters the password, this leads to the result of shoulder surfing attack. Since to avoid that attack we mentioned here a chromatic password system, it is a novel or new method, which avoids the shoulder surfing attack.

Index Terms **- Chromatic, Shoulder surfing, Password, Hacker.**

I. INTRODUCTION

The most simple and common way that an unauthorized user can access the password is by looking over the users shoulder, it can be done by standing very close to the user or by longer distance. The hacker will guess the password by watching the hand moment, by keystroke, by binoculars, secret microphones, hidden cameras, etc. Securing the password from these issues is becoming one of the challenging task. Therefore, to avoid shoulder surfing attack we can use chromatic password system. This system uses colors as well as characters, special characters and numbers. It is much useful for the system where password security is highly in need.

This system is simple and easy to work on it provides - up and down arrows, conform and login button to operate and it does not require any keyboard or any on-screen keyboard. By this system, the user can secure their account details and other personal data, even we can also implement it in bank ATM's also. All the users are familiar with the text passwords, but in chromatic password system along with the text password, the user has to remember the colour that was send to user registered mail id while account creation or form filling. Generation of password and modification is allow to the user with certain authorization and authentication. These processes carried out through registered mail id, so this system is cost efficient and secured.

II. EXISTING SYSTEM

The only way to authenticate the user while login to the system is by using the password system. The existing password system will results in shoulder surfing attack. By this paper we are going to use the word shoulder surfing in the following sense: A shoulder surfing attack consists of a user being filmed during her/his login.

III. PROPOSED SYSTEM

In this proposed system we improved the earlier text based password system results in shoulder surfing attack by using the colors. That's why we give the name "Chromatic Password System - A Novel Method To avoid Shoulder Surfing Attack". In this scheme the user can login to the system easily and efficiently. Next, we analyse the security and usability of the proposed scheme, and show the resistance of the proposed scheme to shoulder surfing and accidental login. The proposed scheme finds an application in any login system.

Advantages of using a chromatic password system:

- Avoid procedure of login using physical / on-screen keyboard.
- Provides the security from surfing attacks, efficiently authenticate the validity of the users.

IV. SYSTEM DESIGN

4.1 Flow Charts

A. Admin Login Flow Diagram

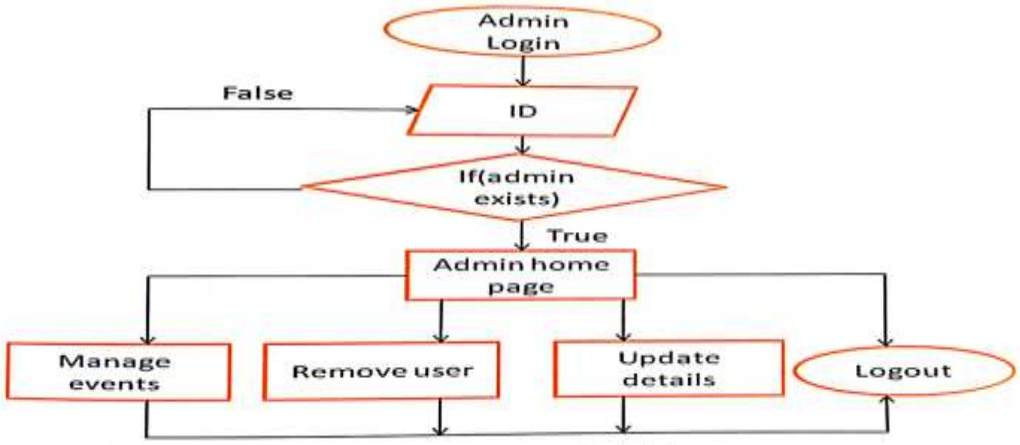

Figure 1: Admin Flow Diagram.

Admin will login to the system by his/her Email – Id, if the Id is exist admin home page will be displayed. If Id not exists, then it will point to re-enter Email – Id.

B. User Login Flow Diagram

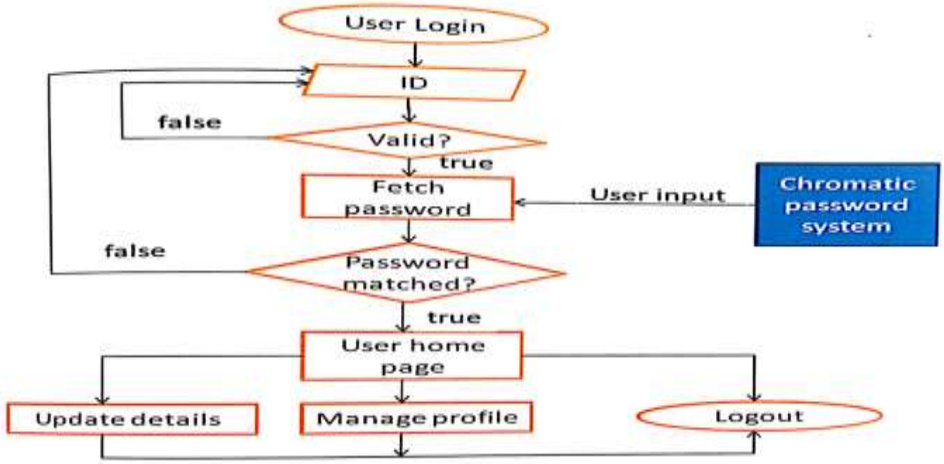

Figure 2: User Flow Diagram.

User will login to the system by providing his Email-Id. If the Id is valid then it fetches the password, if not then it will point to re-enter the Id. The user will matches the password, if the password matched is correct then it displays the user home page, if the matched password is invalid, then it returns to match password.

4.2 Use Case Diagrams

A. User

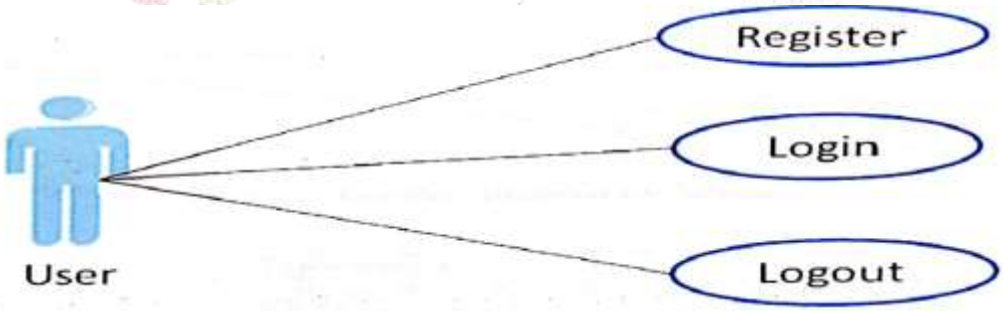

Figure 3: Use Case Diagram for User

Use case	Description
Register	A nonmember has to register to upload his details
Login	User has to login, in order to start his session
Logout	User logs out to end the session

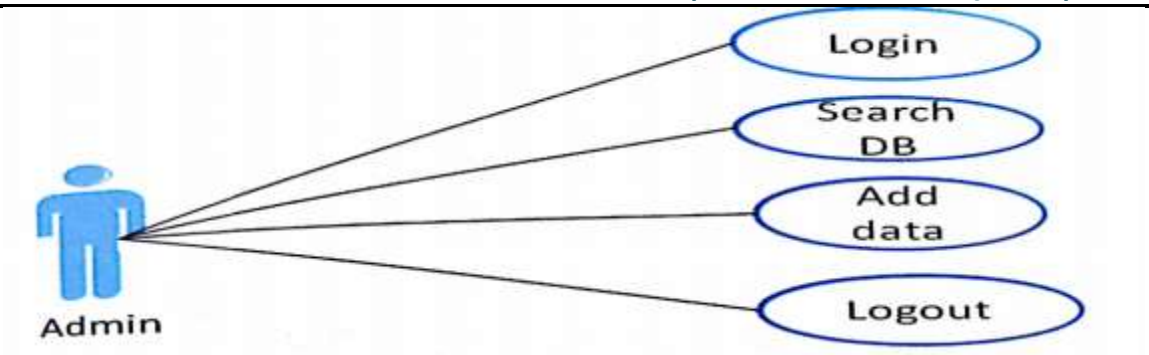

Figure 4: Use Case Diagram for Admin

Use case	Description
Login	Admin has to login in order to start the session.
Search Database	Admin will search the database to check the user details
Add Data	Admin will update the details of user to the database
Logout	Admin logs out

V. METHODOLOGY

5.1 Admin Login

Admin is going to login to the system by providing Admin ID, if the ID entered is valid and present in the database then admin can perform the database insert, delete and update operations. Admin having the control of user in issuing the user kit, activation and all.

Figure 5: Admin login page.

5.2 User Registration

User is going to register to the system by filling registration form; the registration form consists of user name, gender, address, mobile number, email-ID, password, security pin and all. The user has to fill the details to make registration.

Figure 6: User Registration page.

5.3 User Activation

User has to activate the account by entering the kit number provided by the admin through registered email-id, when the user asks the kit by clicking 'Activate now' link. The kit also consists the colour and colour code.

The user enters once the kit number and clicking update button an information will be displayed on the user, which consists of message the kit number along with, that a randomly generated colour code between 1 to 8 was displayed.The colour code between 1 to 8 tell the colour, for example code 1 for red, 2 for blue, 3 for green colour which is sent to the user email-id.

NOTE: A, B, C methods are the one time process…

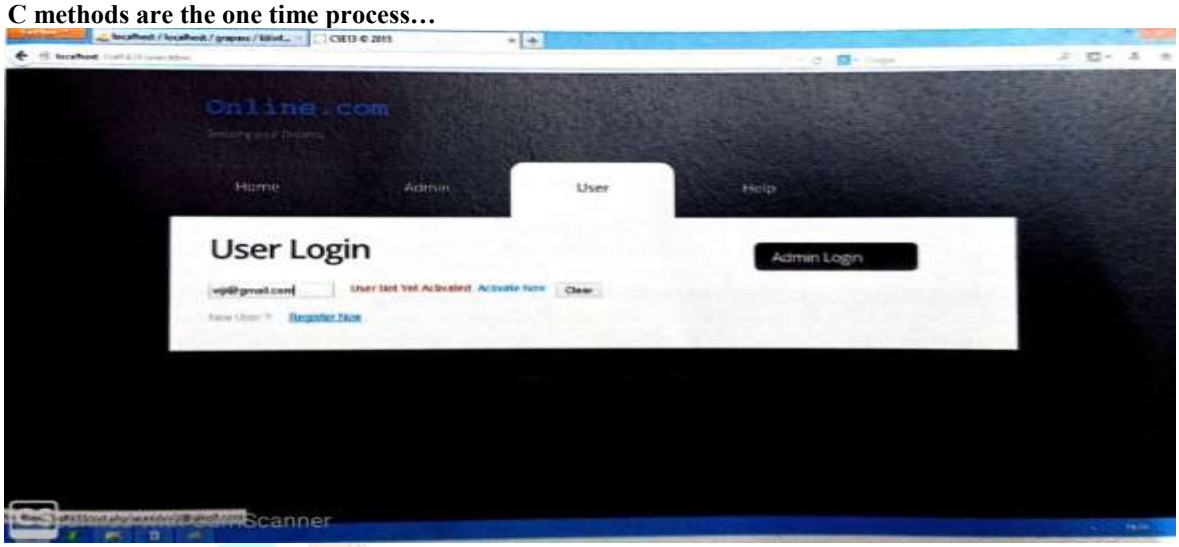

Figure 7: User Activation page.

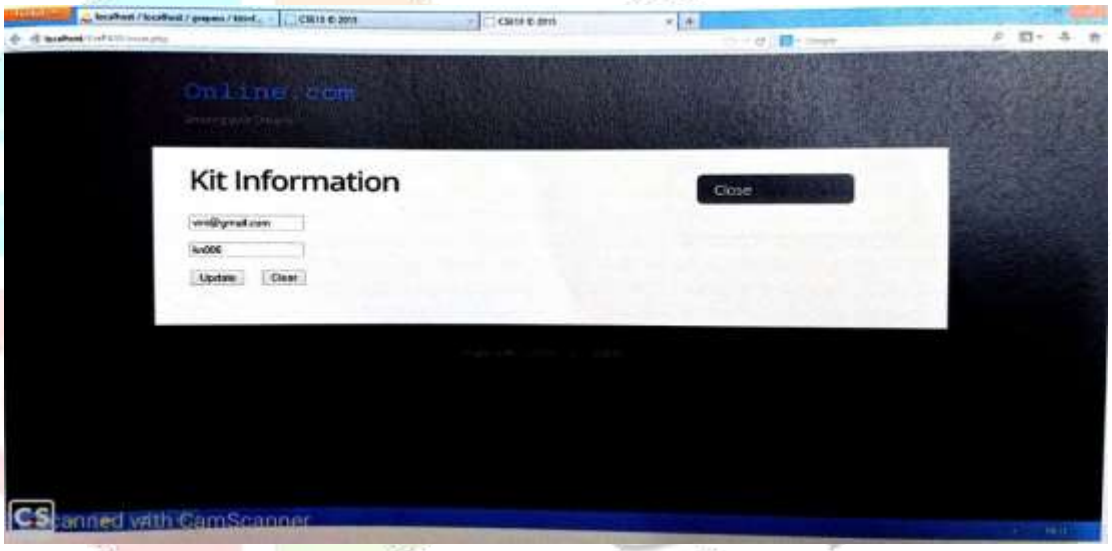

Figure 8: Admin Issuing User Kit.

Figure 9: User Activation by entering Kit number.

Figure 10: Randomly generated color code between 1 to 8

5.4 User Login

Once after completing the registration and activation phases completely. The user can login to the system any time.

Figure 11: User login page.

Here comes the actual steps and login to the chromatic password system. While in the registration, the user has to keep two things in his mind.

1. The password filled while registration phase.
2. The colour sent to the registered email-id.

The password matching page will opens once after all the steps are completed. This page consists of list of colours with their names and randomly shuffled numbers, characters and special characters above the different colours. The user has to match the password characters one by one to the specific colour given.

For example, the password is ‘abc’ and the colour is red. The user has to match the password first letter ‘a’ to red colour with the help of provided keys upwards/ downward arrow keys, once ‘a’ is placed at the red colour then click conform, then the colours are reshuffled once by shuffling the letters, numbers, special characters. The letter ‘b’ is placed to red colour by clicking arrows, if ‘b’ is already exists in the red colour then just press conform button. Likewise, match ‘c’.

Once the user clicks conform button at each single match then it going to entered in the password section. After all the password characters matched then the user has to click the login button.

Figure 12: User Password Matching page.

Figure 13: User matching the password to the assigned color.

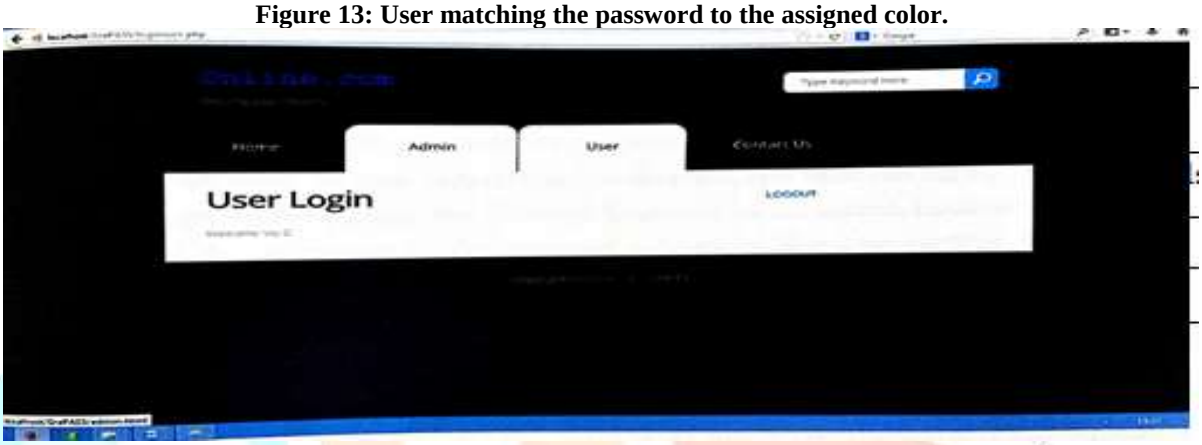

Figure 14: Login Successful and welcome page

If the matched password is correct or valid then the successful login message will display. If not correct, then the error message will display.

VI. Test Cases

6.1 User Registration Module

Name of Activity	Input	Expected Output	Pass/Fail
User Registration.	Submit valid details	Successfully submitted	Passed
	Invalid details	Unsuccessful	Passed
Details updating.	Update changes	Successfully updated	Passed
	Invalid updates	Unsuccessful	Passed

6.2 User Login Module

Name of Activity	Input	Expected Output	Pass/Fail
Login	Valid user ID and password	Success	Passed
	Invalid user ID or password	Unsuccessful	Passed

6.3 Admin Module

Name of Activity	Input	Expected Output	Pass/Fail
Login	User ID	Success	Passed
	Invalid user ID	Unsuccessful	Passed

VII. CONCLUSION AND FUTURE WORK

The Paper "Chromatic Password System – A Novel Method to Avoid Shoulder Surfing Attack" provides a user to easily and efficiently complete the login process without worrying about shoulder surfing attack. The operation of the proposed system is simple and easy to learn for the users familiar with textual passwords. Without using any physical keyboard or on screen keyboard the user can login to the system. Finally we have analysed the resistances of the proposed scheme to shoulder surfing and accidental login. This proposed scheme is very much useful where confidential data needs security.

As a future work mechanisms can be adopted to reduce the time consumption during password matching.

REFERENCES

[1] L. Sobrado and J. C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[2]L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005. (http://clam.rutgers.edu/~birget/grPssw/srgp.pdf)

[3] S. Wiedenbeck, J. Waters, L. Sobrado, 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.

[4] H. Gao, X. Liu, S. Wang, H. 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.

[5] B. Hartanto, B. Santoso, and S. Welly, "The usage of graphical password as a replacement to the alphanumerical password," Informatika, vol. 7, no. 2, 2006, pp. 91-97.

[6] S. Man, D. Hong, 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 .

[7] T. Perkovic, M. Cagalj, and N. Rakic, "SSSL: shoulder surfing safe login," Proc. of the 17th Int. Conf. on Software, Telecommunications & Computer Networks, Sept. 2009, pp. 270-275.

[8] Z. Zheng, X. Liu, L. Yin, 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.

[9] T. Yamamoto, Y. Kojima, and M. Nishigaki, "A shouldersurfing-resistant image-based authentication system with temporal indirect image selection," Proc. of the 2009 Int. Conf. on Security and Management, July 2009, pp. 188- 194.

[10] 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.