ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1-6), Month:April - June 2015, Available at: www.researchpublish.com

Authentication Schemas Using Color Password

Alfiya Sayed[1], Afrin Khan[2], Afrin Sayed[3]

[1,2,3]Student (Information Technology), MHSSCOE, Mumbai, India

Abstract: **Authentication is a process that ensures and confirms user's identity. Studies have shown that user tend to pick short passwords or passwords that are not easily forgotten. But both Textual, graphical password have issues of hacking and cloning. Hence we propose a technique, where text can be combined with images or colors to generate passwords for authentication. This paper provides authentication using different color codes rankings based on the current time of the system. Also the chances of hacking are very less as the color password changes after every one minute. It is a two step authentication process as it uses color codes as well as unique PIN number for each user.**

Keywords: **Authentication, brute force attack, color password, dictionary attack, hacking, PIN number, shoulder surfing.**

I. INTRODUCTION

Authentication schemas using color password is a website which enables the user to authenticate himself using color passwords. The main goal of this system is to enhance security. Security of personal as well as account details is the need of the hour. Any account on the internet is vulnerable to hacking, cloning, shoulder surfing, eaves dropping, dictionary attack, etc. Also it becomes really difficult for any user to trust and use the websites which are vulnerable to hacking. Sometimes, the entire process of registering on a website is very difficult. After the survey done with the users, who tend to login to a website on a regular basis, the concluded result was that a more user-friendly and secure system can be implemented for increasing the security. Authentication schemas using color passwords, provides a two-step authentication wherein the PIN number is at the first step which is very difficult to hack. It is difficult for a hacker to break the security level at the first level itself, because PHP provides the an inbuilt functionality called MD5 to store this PIN number in the encrypted manner. If the intruder is an expertise person gets the entry in the database then it's of no use because PIN number is not exist in database. Further the color password implementation is a tricky concept for the intruder to understand since the sequence can follow any pattern (regular, circular or reverse). This system can be implemented to any website which wants to secure the user's important credentials and personal data. The list of users can range from students, teachers, professionals or any common man who wishes to secure his credentials in the outside world of web. In the long run, it can be implemented to any social networking sites, company's personal website or CRM Company, online shopping site etc.

II. EXISTING SYSTEM

A. Textual Password:

Textual password scheme or Alphanumeric password scheme are the most common method used for authentication. It prompts the user to choose text, numbers and special character as a password. It can be his name, favorite team's name, favorite date, etc. The simple and straightforward alphanumeric passwords are very easy to remember but Studies have shown that, these passwords can be easily guessed or cracked. Whereas the complex and difficult password makes the system more secure, resisting the brute force attack, dictionary attack.[1].

B. *Graphical password*:

Consequently, Graphical login scheme has been introduced by Dhamija and Perrig as a substitute for alphanumeric scheme .Since in the alphanumeric scheme, User pick the short password that are easy to remember. Unfortunately, these passwords can be easily hacked. User chooses the set of the images instead of entering the alphanumeric password shown on the interface .User passes the authentication by selecting the images in sequence, as he had selected during registration. Moreover, the password space of graphical login extends that of the alphanumeric based schemes and hence providing the higher level of the security [2] . But this scheme is prone to shoulder surfing, a known hazard where hacker can scrutinize the graphical password by recording, watching or through direct surveillance and also it's costlier than the alphanumeric scheme [3].

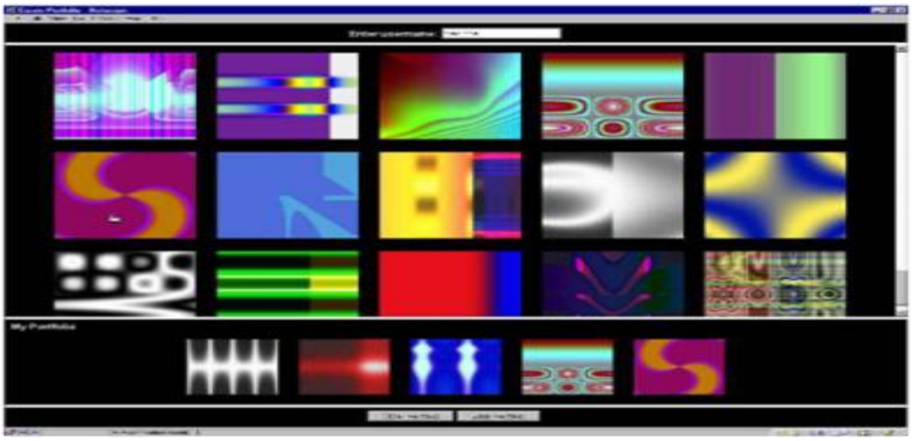


Fig.1: Set of images used by Dhamija and Perrig

C. *Pass face*:

Pass face technique , First of all shows the nine faces on the interface from where user have to selects only one face previously chosen as shown in figure 2. The User chooses four images of human faces as their password and the users have to select their pass image from eight other images. Since there are four user selected images it is done for four times [4].

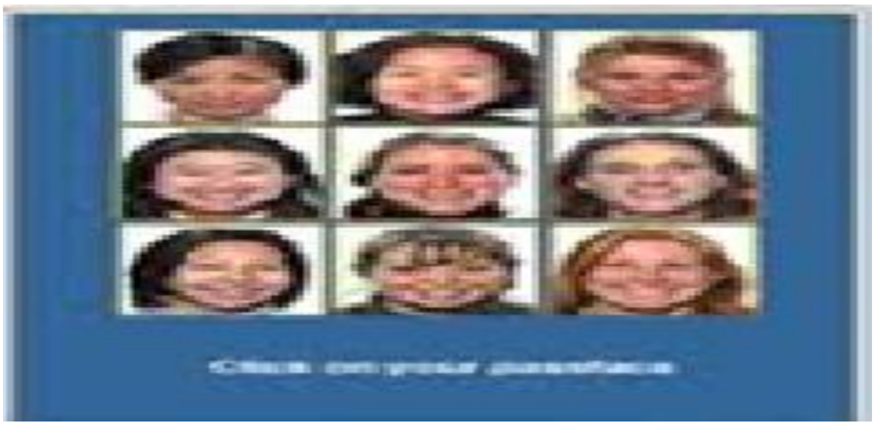


Fig.2: Passface

D. *Biometrics*:

Biometric is a growing technology used for authentication .There distinctive and measurable characteristics are used to describe individuals [5] In biometric, user is authenticated by his different logical feature namely Physiological and Behaviometric. Physiological feature is related to shape or structure of the body .Finger print, Retina scan, Face recognition, Hand geometry, DNA, palm vein and scent and voice recognition and so on.[6]. Some researchers have coined the term behaviometrics to describe the latter class of biometrics [7] .But the main disadvantage of this Authentication schema is that, if the user's eye,Voice or hand get changes due to any accident injury or simply aging ,he will not longer be an authenticated user. Also it's very costlier security solution.

Fig.3: Iris Scanning

III. DRAWBACK OF EXISTING SYSTEM

- Textual passwords are prone to hacking and cloning.
- In Graphical password intruders seem to identify the selected images hence they are vulnerable to Shoulder surfing.
- Graphical systems are costlier than Textual password.
- Biometrics is an expensive technique.

IV. PROPOSED SYSTEM

Authentication Schemas Using Color Password aids in enhancing the security Concerns on various online website. The unique concept of PIN number and color password will provide the two level authentication. In the first level it is very difficult for the intruder to cracked the PIN number which is a combination of the Text & Number & special character. This is so because the system is programmed in PHP language wherein the PIN number doesn't stored in the database & hence it is not subjected to dictionary attack, shoulder surfing , brute force, eves dropping attack. PHP offers an inbuilt function called MD5 to store this PIN number in the encrypted manner. If the intruder is an expertise person gets the entry in the database then it's of no use because PIN number is not exist in database . Even in the worst case scenario , if the intruder breaks the first level it's difficult for him to guess the color sequence selected by the user. This color password at the login time is based on the current time of the system. At the time of registration user can choose the order of choosing the color sequence like regular (For e.g. if the time is 08:43 am then the user will enter the color denoting the digit '0', '8' , '4' , '3') or reverse(for e.g. if the time is 02:16 pm then the user has to select the color denoting the digit '1','4','1','6') and so on for the circular same technique is applied .24 hour format is used to keep a check that no user have the same color sequence & the color password in Am and Pm mode.

V. IMPLEMENTATION

The Phases of the Block Diagram fig.4 are explained below:

***1) REGISTRATION PHASE*:**

The registration phase Consist of two steps.

STEP1: when the user wishes to register him, he must enter his personal detail. Each and every personal detail have some criteria's to be fulfilled. Some fields are mandatory while some are not. After filling the personal detail the user is directed to the next page after clicking the 'PROCEED' button. If the user wants to alter his personal details, he should click on 'CLEAR' button before proceeding.

STEP 2: After clicking on 'PROCEED' button and filling the personal detail, the user is redirected to the "Accounts detail'' page. Here, the user should select an appropriate user id (Containing of text and number only). The system notifies the user if the user id is available or not. Next he must enter his valid e-mail id and PIN number (Consisting of text, numbers and special characters). The most important part of this step is the sequencing of the colors (from 0-9) according to the user's preference. User should also select the pattern of putting the color password (regular, reverse or circular) and a security question and answer. The user can reset his color sequence by clicking 'RESET COLOR CODES'. After clicking on 'REGISTER' button, and validations of all the fields, the user is registered on the website. A link of the USER ID, Color sequence will be sent to the user on his e-mail id for further reference. CAPTCHA functionality is called to make sure that the user is a genuine or not or a robot on this page.

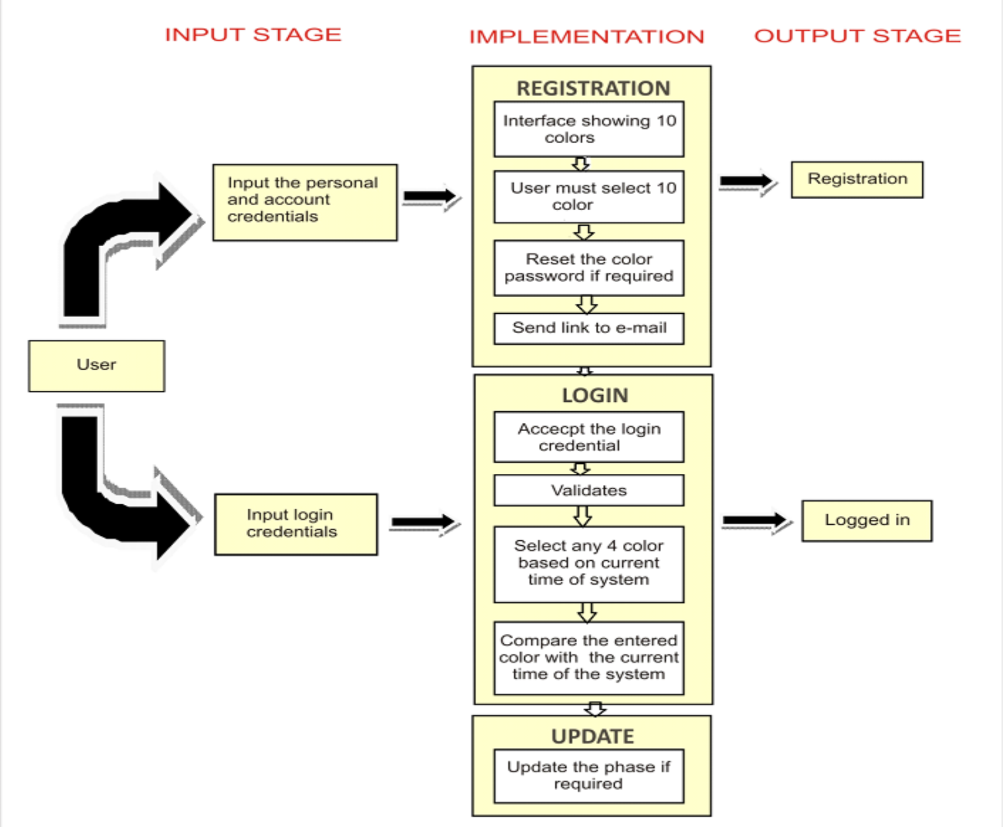
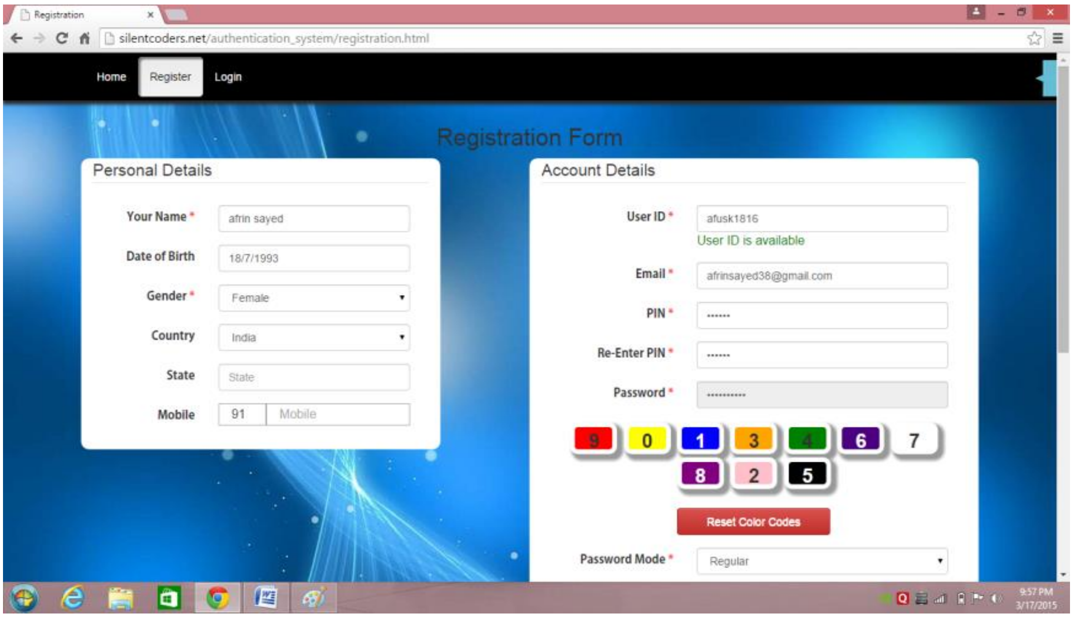

INPUT STAGE
IMPLEMENTATION
OUTPUT STAGE
User
Input the personal and account credentials
Input login credentials
REGISTRATION
Interface showing 10 colors
User must select 10 color
Reset the color password if required
Send link to e-mail
LOGIN
Accecpt the login credential
Validates
Select any 4 color based on current time of system
Compare the entered color with the current time of the system
UPDATE
Update the phase if required
Registration
Logged in

Fig.4: Block Diagram of Authentication Schemas using color Password



Registration Form

Personal Details

Your Name *	afrin sayed
Date of Birth	18/7/1993
Gender *	Female
Country	India
State	State
Mobile	91 Mobile

Account Details

User ID *	afusk1816 User ID is available
Email *	afrinsayed38@gmail.com
PIN *	******
Re-Enter PIN *	******
Password *	**********

9 0 1 3 4 6 7
8 2 5

Reset Color Codes

Password Mode *	Regular

Fig.5: Registration Form

2) *LOGIN PHASE:*

This phase is consists of two steps:

STEP 1: When the user has registered successfully, he can login to the website. Here a screen appears where the user is promoted to enter his user id and PIN number. After clicking the ‘PROCEED BUTTON’, the user is directed to the next page. If the user has forgotten his PIN number or wishes to reset the PIN number , he can reset the same by clicking on the “FORGOT PASSWORD” button.

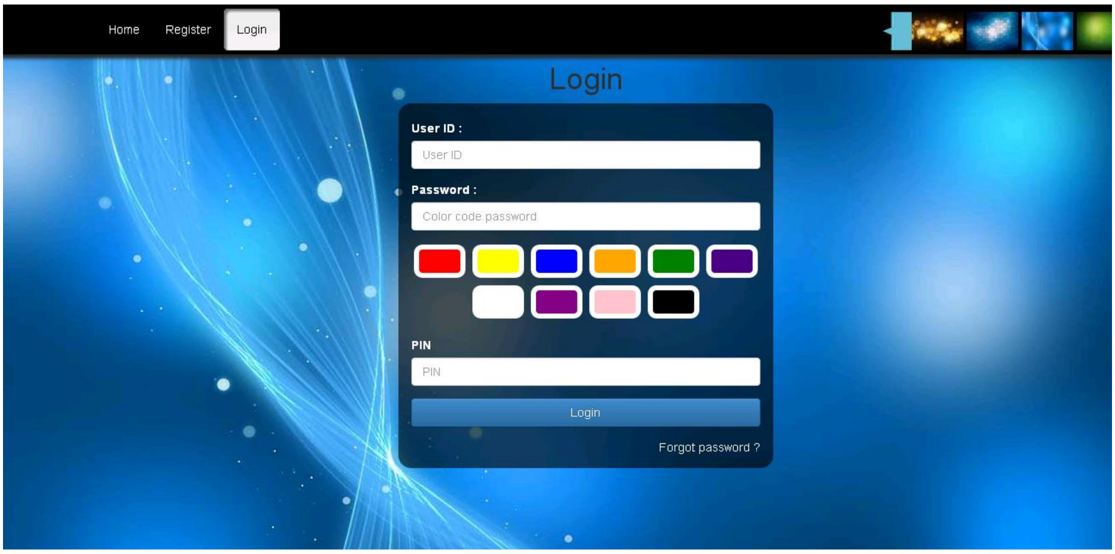


Fig. 6: Login form

STEP 2: After filling the user id and PIN number, the user is supposed to enter his color password based on the current time of the system, ‘for example: if the current time is 07:29 PM, the user will have to enter the first letters of the colors(for example: RED-r, white-w, pink-p, etc)denoting the digit ‘1’,’ 9’,’ ‘2’, ‘9’ the order of the entering the password can be regular, circular or reverse as mentioned in the registration phase. If the credential are correct, the user is logged in after pressing the LOGIN button, a message starting successfully login is displayed on the screen ‘ . If the user forgotten his color sequence, he can map the digits from the link given in his e-mail id given during the registration. Also if the has forgotten his color password or PIN number, he can reset the same by clicking on the “FORGOT PASSWORD” button.

3) RESET PHASE:

When the user clicks on ‘FORGOT PASSWORD’ he can reset his password or PIN number by both the ways either,

1: Answering the security question, OR

2: clicking in the link sent to the users e-mail id.

In both the case, user can reset his password and PIN which is sent on his e-mail id for further reference.

4) UPDATE PHASE:

After successfully login, the user is authenticated to the home page of the website. Here, if required the user can update his password or PIN number.

VI. COMPARISON

TABLE I: COMPARISON CHART

Authentication Schemes	**Textual Passwords**	**Graphical password**	**Biometric Passwords**	**Color Password**
Implementation	Easy	Complicated	Highly Complicated	Easy
Attacks	Brute force attack, Dictionary attack, Guessing.	Shoulder surfing, Guessing	Forgery.	Brute force attack

Cost Of Attacks	Low	Moderate	Very High	Moderate
Time To Login	Low	Moderate	High	Low
Flexibility	Moderate	High	Very Low	High
Hardware	Not Required	Not Required	Required	Not Required
Recovery	Easy	Easy	Difficult	Easy
Password Varies according to Time	No	No	No	Yes

VII. CONCLUSION

Authentication is an act of confirming the truth of an attribute of a datum or entity. [8] This might involve confirming the identity of a person . Our System will make the user's experience more friendly & secure on the web .The system is definitely more secure since the system is implemented in PHP because of this we are inbuilt getting the MD5 feature. , Intruder can't hacked the system and also if the user forgot his password or PIN number , it can be retrieved from user's E-mail. The system is reliable and scalable providing the better performance. In present scenario, the system can be applied to the authentication of user on online website. In future it can be implemented in java & .Net for personalized desktop application.

REFERENCES

[1] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[2] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium,2000.

[3] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder surfing.

[4] Real User Corporation: Passfaces. www.passfaces.com.Jain, A., Hong, L., & Pankanti, S. (2000). "Biometric Identification". Communications of the ACM, 43(2), p. 91-98. DOI 10.1145/328236.32811.

[5] Jump up to:a b c d Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2.

[6] Jump up^ "Biometrics for Secure Authentication" (PDF). Retrieved 2012-07-29.

[7] T. Pavan Kumar, Nagesh Vadaparthi, A.Manvi, A.Alekhya(Secure Session based Authentication Schemes).

[8] ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 2, March -April 2013, pp.1749-1751.