RESEARCH ARTICLE OPEN ACCESS

# A Novel Approach to Resist Shoulder Surfing Attack

Smitesh salian[1], Shivani Deosthale [2], Kranti Ghag [3]

(Department of Information Technology, Shah & Anchor College of Engineering, Mumbai) [1]

(Assistant Professor, Department of Information Technology, Shah & Anchor College of Engineering, Mumbai) [2]

(Assistant Professor, Department of Information Technology, Shah & Anchor College of Engineering, Mumbai) [3]

----------------------------------------************************----------------------------------

## Abstract:

In today's technology world one may have been witness password attacks on their applications or even websites. Currently there are many methods that help you provide security as well as prevent various kinds of attacks that your application or website may be vulnerable to. So it has become dire necessity to protect your Applications, Databases and various Projects from these kinds of attacks.

Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text is combined with colors to generate session passwords for authentication.

A usability testing is carried out to measure the satisfactory level of users on the completeness of the system, which include factors such as, total response time to access the system, remembering of password using the system and resistant to shoulder surfing. The testing result shows that the modified colour pass authentication method is resistant to shoulder surfing.

*Keywords* — **Shoulder Surfing Attack, User Interface, Feature tables, Challenge Values.**

----------------------------------------************************----------------------------------

## 1. INTRODUCTION

Today in the world of Internet, a major problem of every online user is information protection. To protect the information the most common and widely used security system is passwords. Unfortunately, the password system in its simplest form, as is implemented on most websites, is very weak, and can be compromised in a variety of ways such as, Shoulder surfing, Key logger, Phishing, Man in the middle, Session hijacking and Brute force. Though conventional PIN entry mechanism is widely famous for ease of usability, but it is prone to shoulder surfing attack [1] in which an attacker can record the login procedure of a user for an entire session and can retrieve the user original PIN.

Based on the information available to the attacker, secure login methods can be classified into two broad categories fully observable and partially observable. In the first one, the attacker can fully observe the entire login procedure for a particular session and in the second one, the attacker can partially observe the login procedure [2]. Our proposed methodology falls into second category and users are required to remember four colours instead of conventional four digit PINs.

The most common method used for authentication is textual password. The vulnerabilities of this method like evesdropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow [3]. There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels.

The rest of the report is organised as follows, the section 2 gives a brief overview of existing methods of authentication and different kinds of attacks. Section 3 presents the proposed method and user interface. Section 4 gives security and usability analysis of the method.

## 2. EXISTING SYSTEM

Authentication is the process to allow users to confirm his or her identity to a Web application. This process usually refers to as login. When the user wants to login to a system, the user enter a username and password to the server and the server will grant access to the user if the provided username and password match the original username and password.

### 2.1 EXISTING METHODS TO MITIGATE PASSWORD ATTACKS

There are some existing methods for resisting shoulder- surfing attack but they do not fulfil all the aspects of security. There are some existing methods available today that do not offer complete security to the passwords from shoulder surfing attack. Here are some methods mentioned below:

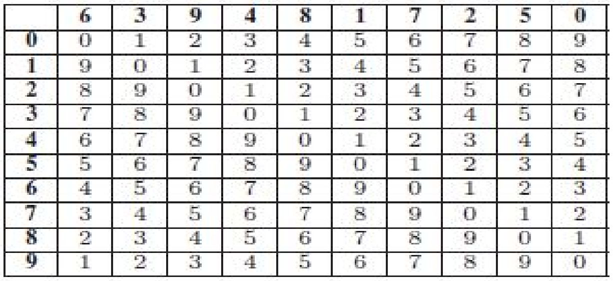
**Mod 10 Method**

In this method user has to perform a simple mathematical operation. User remembers a four digit PIN number from the set {0 to 9}. User receives a challenge from the set {0 to 9}. User will add the challenge digit with the corresponding PIN digit and will perform a modulo 10 operation[4]. Finally he will enter back the obtained digit using a public keyboard. Suppose the first digit of the user chosen PIN is 5. User now securely receives a challenge 7 from the system. So the valid response by user will be (5+7) modulo 10 (which is equal to 2). Though this method is easy to execute for math oriented people and gives good security against guessing the password but for non-math-oriented people this methodology is difficult to adopt.

**Mod 10 Table Method**

In this method a concept of lookup table is used. If user chosen PIN digit is 1 and the system generated challenge is 6 then the user first goes to the row number 1 in the lookup table and subsequently goes to the digit 6 in that row[5]. After that user will see the corresponding column number where 6 is placed (here 9) and enter back 9 as response corresponding to the first challenge.

When the user enters login an interface consisting of a grid is displayed during the login phase. The grid is of size 6 x 6 and it contains of alphabets and numbers. These are randomly placed on the grid and the interface changes every time.



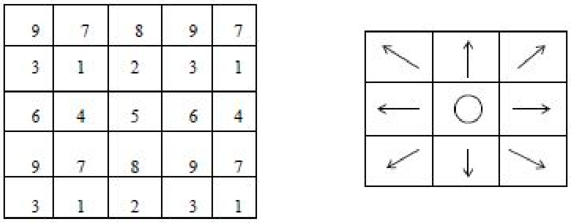
| | 6 | 3 | 9 | 4 | 8 | 1 | 7 | 2 | 5 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 3 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 4 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 |
| 5 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 |
| 6 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 |
| 7 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 |
| 8 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 |
| 9 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |

Fig 1. User Lookup Table

But one of the drawback of this procedure is login time in this method goes high with respect to modulo 10 method. The other drawback we observed that the error rate does not improve much with the number of attempts.

**Shoulder Surfing Safe Login Method**

Unlike the previous two schemes, in SSSL, user does not provide any number as response rather enters some direction to the system[7].



|  |  |  |  |  |
|---|---|---|---|---|
| 9 | 7 | 8 | 9 | 7 |
| 3 | 1 | 2 | 3 | 1 |
| 6 | 4 | 5 | 6 | 4 |
| 9 | 7 | 8 | 9 | 7 |
| 3 | 1 | 2 | 3 | 1 |

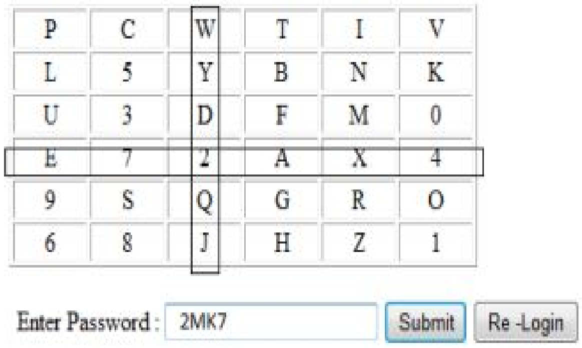
|  |  |  |
|---|---|---|
| ↖ | ↑ | ↗ |
| ← | ○ | → |
| ↙ | ↓ | ↘ |

Fig 2. Keypad structure for SSSL

In this scheme a user remembers a five digits PIN. In terms of authenticate himself the user has to answer to the challenge values throws to him with respect to the table and keypad consist of arrows shown in Fig.2. The table in SSSL method constructed in such a way that every digit i is an immediate neighbour to other 8 digits from the set.

### Pair-based Textual Authentication system

In this scheme, during registration user submits his password. The maximum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters[8]. Session passwords are created based on this secret pass. When the user enters login an interface consisting of a grid is displayed during the login phase. The grid is of size 6 x 6 and it contains of alphabets and numbers. These are randomly placed on the grid and the interface changes every time.



|  |  |  |  |  |  |
|---|---|---|---|---|---|
| P | C | W | T | I | V |
| L | 5 | Y | B | N | K |
| U | 3 | D | F | M | 0 |
| E | 7 | 2 | A | X | 4 |
| 9 | S | Q | G | R | O |
| 6 | 8 | J | H | Z | 1 |

Enter Password : 2MK7

Fig 3. Pair based Authentication System.

The grid will be appeared as shown in below fig 3. Depending upon the password which is submitted during the registration phase, user has to enter the password. Users have to consider his password in terms of pairs. The session password consists of alphabets and digits. Now the user have to enter his authentic password which is the intersection part of that submitted password.

## 3. PROPOSED SYSTEM`

Modified colour pass authentication method consists of 3 phases: registration phase, login phase and verification phase. During registration, users select the colours as the password. During login phase, the user enters password based on the random challenge values and feature tables displayed on the screen. The system verifies the password entered by comparing with content of the password generated during registration.

### Feature Table

Modified Colour Pass interface consists of 10 different Feature Tables which is numbered from 0 to 9. Each cell of a table is represented by a pair < Ci, Vi >. Here Ci denotes the colour of the cell i and Vi indicates special characters corresponding to cell i. Both Ci and Vi is random with respect to a Feature Table generated in each login. Thus no colour occupies in more than one cell. So for a particular table is twelve different colour cells. The positions of colour cells are shown in fig 4. and this is fixed for every table.

|  |  |  |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |
| 10 | 11 | 12 |
| K |  |  |

|  |  |  |
|---|---|---|
| C1,Vi | C2,Vi | C3,Vi |
| C4,Vi | C5,Vi | C6,Vi |
| C7,Vi | C8,Vi | C9,Vi |
| C10,Vi | C11,Vi | C12,Vi |
| K |  |  |

Fig 4. Color Position of Feature Tables.

### Challenge Values

Challenge Values is random number values from 0 to 9 used as a medium for authentication of users in to the system. During the login procedure, when the Feature Tables appear in the screen then the system is throwing some challenge values to the user. The challenge is passed to the user by three modes: Audio, Email, screen. Challenge values via audio requires user to plug in headphones to listen the challenge code. Based on the challenge value the user select the corresponding Feature Table

### 3.1. Characteristics of user chosen pin

In the existing system it is required to remember either few digits or few characters as users PIN. But in our scheme the colour is used to form a PIN. User have to choose 3-6 colours from a set of 12 different colours and have to choose one colour more than once.

### 3.2. STEPS FOR LOGIN PROCEDURE

1. User enters his/her login id.
2. Once system checks that the login id exists then it will generate the color tables.
3. System then generates four random challenge values from 0 to 9.
4. Next user has to give response to those challenge values.
5. Finally system decides whether the user is legitimate or not.

### 3.3. PIN ENTRY MECHANISM IN COLOR PASSSWORD

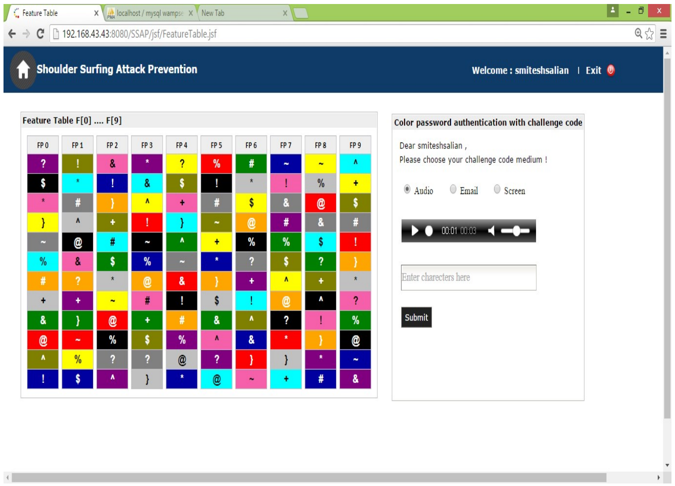
In this scheme, the user chosen PIN is four colours. During login the colour table appears in the screen then the system throws some values through handheld devices. Those values are ranges from 1 to 10. Based on that value the user has to select the corresponding colour table. This values will be randomly generated. Then corresponding to the chosen colour PIN, user locates the colour cell in that table. By locating the digit in that colour cell user enters the digit. similarly user will respond to other values and will finishes the login process. Valid response to the values will authenticate the user.

| Index | Assigned Values | Colour name | Colour |
|---|---|---|---|
| 1 | ! | Yellow | 🟨 |
| 2 | @ | Blue | 🟦 |
| 3 | # | Green | 🟩 |
| 4 | $ | Red | 🟥 |
| 5 | % | Black | ⬛ |
| 6 | & | Grey | 🟫 |
| 7 | * | Orange | 🟧 |
| 8 | ? | Purple | 🟪 |
| 9 | ^ | Cyan | 🟦 |
| 10 | ~ | Olive | 🟫 |
| 11 | + | Silver | ⬜ |
| 12 | } | Pink | 🟪 |

Fig 5. Colors used for implementing features tables

Each colour has been assigned a number from 0 to 9 by the system as shown in Fig.5. The user PIN is stored in an array UCOL (indexed from 0 to 3). The four random numbers (challenge values) generated by system is stored in array RAN (indexed from 0 to 3). User response to the challenge is stored in array CLICK (indexed from 0 to 3).

### 3.4. USER INTERFACE



Shoulder Surfing Attack Prevention

Welcome : smiteshsalian | Exit

Feature Table F[0] .... F[9]

| FP 0 | FP 1 | FP 2 | FP 3 | FP 4 | FP 5 | FP 6 | FP 7 | FP 8 | FP 9 |
|---|---|---|---|---|---|---|---|---|---|
| ? | ! | & | * | ? | % | # | ~ | ~ | ^ |
| $ | * | ! | & | $ | ! | * | ! | % | + |
| * | # | } | ^ | + | # | $ | & | @ | $ |
| } | ^ | + | ! | } | ~ | @ | # | & | # |
| ~ | @ | # | ~ | ^ | + | % | % | $ | ! |
| % | & | $ | % | ~ | * | ? | $ | ? | } |
| # | ? | * | @ | & | } | + | ^ | + | * |
| + | + | ~ | # | ! | $ | ! | @ | ^ | ? |
| & | } | @ | + | # | & | ^ | ? | ! | % |
| @ | ~ | % | $ | % | ^ | & | * | } | @ |
| ^ | % | ? | ? | @ | ? | } | } | * | ~ |
| ! | $ | ^ | } | * | @ | ~ | + | # | & |

Color password authentication with challenge code

Dear smiteshsalian ,
Please choose your challenge code medium !

● Audio ○ Email ○ Screen

Enter charecters here

Submit

Fig 6. User interface on screen

This module accept password from user. Once the user enters password, then the user is allowed to logged in into the system as shown in fig 6.

User have to enter password based on the challenge values generated by the system. Challenge values are random number in range 0 to 9. Each time challenge values would be changing. User can see Challenge values in 3 modes: audio, email, and screen. Through audio mode, user will have to plugin headphone to listen to the audio which contain challenge code. Through email mode, challenge values will be sent to user vai email.

Through screen mode, the challenge values will be displayed on the screen itself.

These page also contain 10 feature tables, named from 0 to 9. Each Feature tables contain 12 different colour cells and ecah cell has some special characters written on it. For each login, this features tables would be changing, i.e., colour cells and characters will be different every time.

Based on the challenge code, user will select corresponding numbered feature table and then user have to select colour cell which he has selected at the time of registration. The special characters written on that cell is the first character of the password.

## 4. SECURITY AND USABILITY ASCEPTS

### 4.1. SECURITY ANALYSIS

As the scheme is partially observable so the attacker cannot see the colour pin and entered password by the user. Only the challenge values in case of display on screen are visible to the attacker. Thus to ensure security, the attacker should not able to guess the PIN just by seeing the responses. Suppose user has chosen color yellow as one of his secret PIN and he gets a challenge 4 corresponding to that PIN digit. Let a valid response from user will be $ as per the random Feature Tables. Now as attacker does not know the colour pin 4 and as digit $ is printed upon all 12 colors of all ten tables so attacker will not be able to retrieve the original colours chosen by user. This makes modified Color Pass method robust against shoulder surfing attack.

In case of guessing attack, attacker cannot guess the user pin as there are total 12 colours and password length range is from 3-6. So there would be many combination, which is not easy for attacker to guess.

Side channel attack is another possible attack where human users are involved. Some variation of this attack is found in. In this attack, the attacker tries to guess from the time the user takes to execute a particular operation. In the modified Color Pass scheme, the user response time is expected to improve with each login session. So with each session user gradually gets familiar with the system and thus response time also improves. This makes side channel attack quite challenging for the modified Color Pass scheme.

### 4.2. USABILITY EVALUATION

System implemented for use in public domain requires user friendliness along with mechanism to protect sensitive details of the users. In our proposed methodology, it has been found that this method is efficient against attack like Shoulder Surfing or guessing the password. Evaluation of usability and feedback from users also appears satisfactory. The experiment has been performed using the following work station with configuration 2 GB RAM, quad core processor and processing speed of 2.42 GHz. The experiment is conducted with the help of 5 users. The average time taken by users to understand our methodology is about 10 minutes (mins). And the feedback got from most of the users is that the methodology is very easy to understand. The users has been given lesson about how to use the system. Each lesson period is about 5 mins. The users selected are from the students (2 students) and other persons from the society (3 people).

Compatibility of modified Color Pass in terms of use- After a discussion with users we give users about 30 mins to choose their password and for memorizing it. Then we asked the users to login with their password. The login time is the duration of time taken by user to listen to challenge values and give response to the challenge values during a session. Login time obtained from our experiment is shown in Fig 7. The percentage of error during login time is significantly low (less than 4 percentage) as the users get habituated (after 5, 10 trails) with the system. The error rate for our experiment is shown in Figure 8.

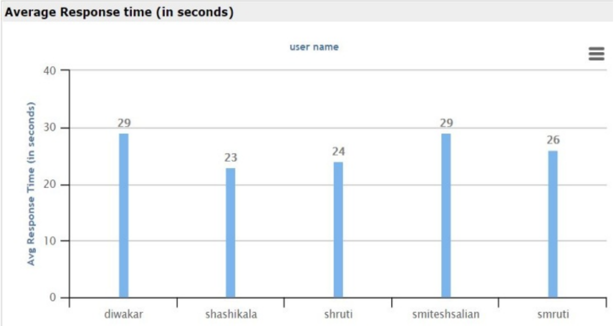


Fig 7. Average Login Time

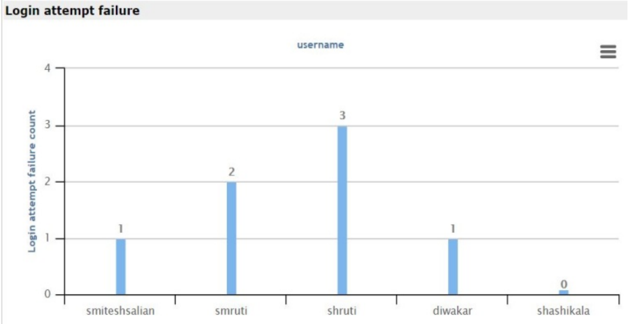


Fig 8. login attempt failure

No special mathematical knowledge is required to use our scheme. Thus the scheme can be easily used by any type of users which widens the scope of applicability of our scheme. However one problem associated with our scheme is that scheme cannot be used by color blind people. As the scheme is based on colors only, Except this limitation our methodology is quite powerful against attacks such as guessing PIN, shoulder surfing attack, side channel attack and yet provides a simple to use interface which consumes a very low login time.

## 5. CONCLUSIONS

Passwords provide security mechanism for authentication and protection services against unwanted access to resources. But passwords are more prone to attacks like shoulder surfing attack, brute force attacks. The modified Colour Pass scheme provides an intelligent interface for users to login into system in a public domain. In this scheme, the user remembers colours as his PIN.

The scheme works on the framework of partially observable attacker model. From security point of view the scheme is quite robust against some possible attacks such as shoulder surfing, guessing password, side channel attack, etc. And from usability point of view the scheme is user friendly and takes very less time for login. Also the scheme can be used by both math and non-math oriented people. The methodology shows significant low error rate during login procedure.

In future we will explore how to extend this scheme for fully observable attacker model and to develop system which can be used by colour blind people also.

## REFERENCES

[1] Chakraborty, Nilesh, and Samrat Mondal, "Color Pass: An intelligent interface to resist shoulder surfing attack”, IEEE Transaction on Technology Symposium, Vol. 2, No. 7, 2014.

[2] Lee, Mun-Kyu, "Security and advanced method for human shoulder-surfing resistant pin-entry", IEEE Transaction on Information Forensics and Security, Vol. 1, No.2, 2014.

[3] Aratani, Akira, and Atsushi Kanai, “Authentication method against shoulder-surfing attacks using secondary channel", IEEE Conference on Consumer Electronics (ICCE), 2015.

[4] Shi, Peipei, Bo Zhu, and Amr Youssef, "A PIN entry scheme resistant to recording-based shoulder-surfing", IEEE Conference on Emerging Security Information Systems and Technologies, 2009.

[5] Afzal, Samiullah, "Operation Code Authentication preventing shoulder surfing attacks." IEEE Conference on Computer Science and Information Technology, 2010.

[6] Kwon, Taekyoung, and Jin Hong, "Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks", IEEE Transactions on Information Forensics and Security, Vol. 14, No.5, 2015.

[7] Zhao, Huanyu, and Xiaolin Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme", IEEE Conference on Advanced Information Networking and Applications Workshop , 2007.

[8] Nand, Pradyumn, et al, "Prevention of shoulder surfing attack using randomized square matrix virtual keyboard."IEEE Conference on Computer Engineering and Applications, 2015.

[9] Shin, Hyungjun, Daeyoung Kim, and Junbeom Hur. "Secure pattern-based authentication against shoulder surfing attack in smart devices." IEEE Conference on Ubiquitous and Future Networks, 2015.

[10] Sreelatha, M., et al, "Authentication schemes for session passwords using color and images", International Journal of Network Security & Its Applications, Vol. 7, No.2, 2011.