Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

User Authentication Using Text And Color based Graphical Password

Deshmukh S.B[1], Ssonkar S.K[2], Arote S.V[3]

[1,3]Student, Computer Dept.
[2]Computer Engg, AVCOE,Sangamner,

Abstract— In today's life user authentication is most important point in information security. Text based password provide security up to certain constrains. To provide high security we can use strong password but that password will become difficult to remember so we write that password on paper or write it somewhere else in computer. To avoid this user can select the password which is easy to remember. This textual password is vulnerable to many attacks like brute force attack, dictionary attack, guessing, shoulder surfing attack. From all this attack should surfing attack mostly happened. Graphical password with textual password can become alternative to avoid the all type of attack.

Keywords- Textual Password, Graphical password, Shoulder Surfing Attack, Authentication, Security

I. INTRODUCTION

People wants secure his own private data from unauthorized access for that purpose user uses some type of password which limits access to third party. Authentication is process which identifies authorized user who can access the data. For the purpose of authentication user can use a textual password. This password is vulnerable to attack like shoulder surfing, brute force attack etc. Out of this shoulder surfing attack is most happening. The shoulder surfing attack is attack in which unauthorized user can obtain user password by watching towards shoulder when he enters his password. The shoulder surfing attack will occurred in crowded place when someone fills form, enter pin at ATM machine. It can also be done from distance using binoculars, close circuit television camera. To prevent shoulder surfing we shield paper work or keypad from third party by cupping our hand. To reduced the effect of shoulder surfing attack on conventional password scheme sobrado and birget proposed three shoulder surfing resistant graphical password scheme. But each scheme has some advantages and some disadvantages. It looks that mostly user are familiar with textual password and graphical password, Zhao et al. proposed text base shoulder surfing resistance 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.

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.

All this existing text base shoulder surfing resistance graphical password scheme are not secure and efficient in this project I had purposed graphical password scheme which uses combination of textual password and color. The working of this system is very simple and user friendly. It is easy to use as user familiar with textual and graphical password.

II. RELATED WORK

In 2002, Sobrado and Birget proposed three shoulder surfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Triangle scheme. However, both the Movable Frame scheme and the Intersection scheme have high failure rate.In 2006, Wiedenbeck et al. proposed the Convex Hull Click Scheme (CHC) as an improved version of the Triangle scheme with superior security and usability. In 2006, Wiedenbeck et al. proposed the Convex Hull Click Scheme (CHC) as an improved version of the Triangle scheme with superior security and usability. In 2009, Gao et al. proposed a shoulder sur_ng resistant graphical password scheme, ColorLogin, in which the background color is a usable factor for reducing the login time. However, the probability of accidental login of ColorLogin is too high and the password space is too small. In 2012, Rao et al. proposed textbased shoulder suffering resistant graphical password scheme, PPC. To login the system, the user has to mix his textual password to produce several pass-pairs, and then follow four prede_ned rules to get his session password on the login screen. However, the login process of PPC is too complicated and tedious.

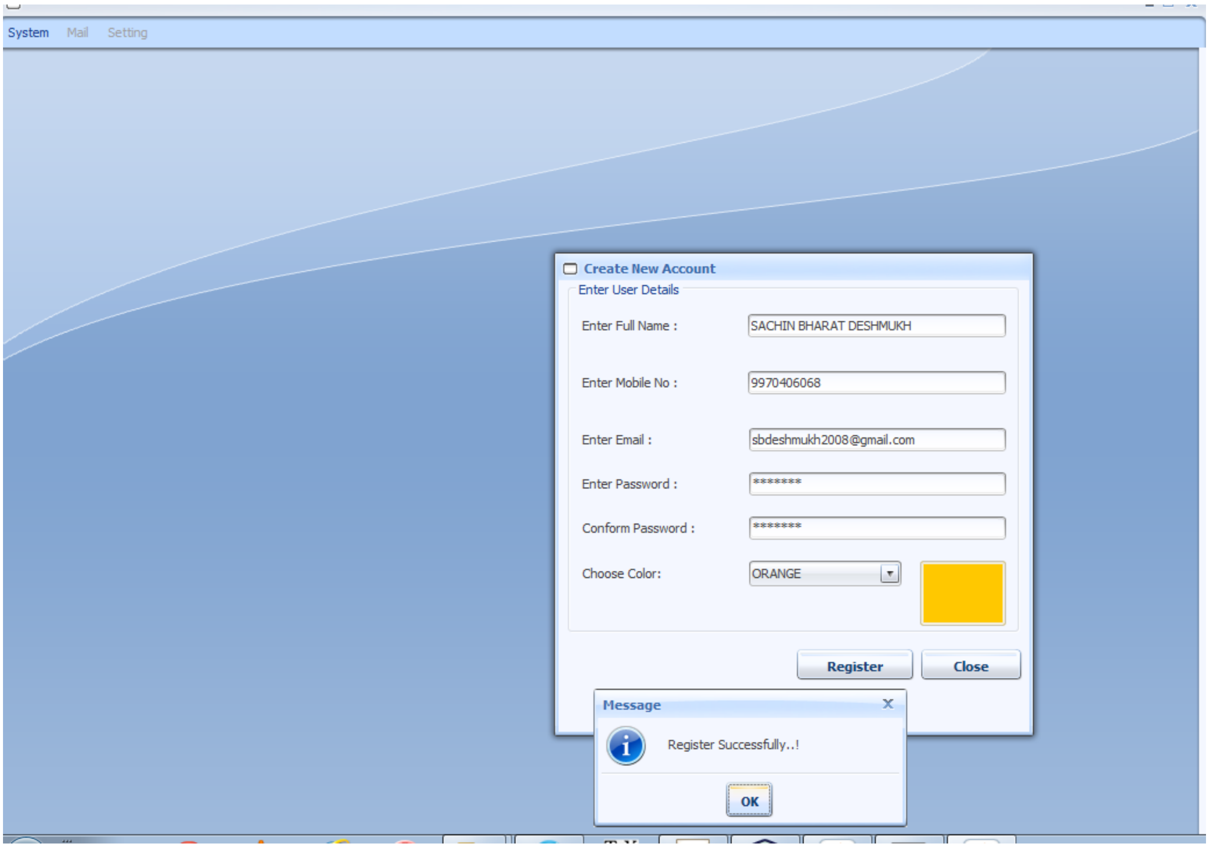
III. PROPOSED SYSTEM

In this we will see our proposed work system which uses combination of textual and Color based password to avoid the shoulder surfing Attack. We had developed a application mail server which will open when we enters the text and color based graphical password. Our projects has two phases First is for new user registration and Second is for Login in to system In this Proposed Scheme, we will describe a simple and efficient Method to avoid the shoulder surng Attack using Texts and color based graphical Password Scheme. The Scheme Contains alphabets i.e 64 characters (26 Capital Letter, 26 Small case letters, 0-9 i.e. 10 decimal digits,two symbols . and /.

The system functions in following steps,
1. Start The Server **2**. Start Client **3**. Registration
4. User log In **5**. Verication By One Time Password (which we receive by Registered E mail Id) **6**. System Starts

3.1. Registration Phase

The password registration is a simple step in which new user make his own registration. In this phase user enters his name, email ID, mobile number,password and selects one color from available 8 Colors. Here user set his textual password of length of minimum 8 character and maximum 15 character. Along with this user selects a color from available colors as his pass color. The remaining 7 colors not chosen by the user are his decoy colors. The email id chosen by user is used by system to send a one time password to user. After entering this all and selecting Register user easily gets registered for his own login. The registration phase should proceed 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.



Create New Account

Enter User Details

Enter Full Name : SACHIN BHARAT DESHMUKH

Enter Mobile No : 9970406068

Enter Email : sbdeshmukh2008@gmail.com

Enter Password : *******

Conform Password : *******

Choose Color: ORANGE

Message

Register Successfully..!

Fig 1. Password Registration

The system stores the users textual password in the users entry in the password table, which should be encrypted by the system key.

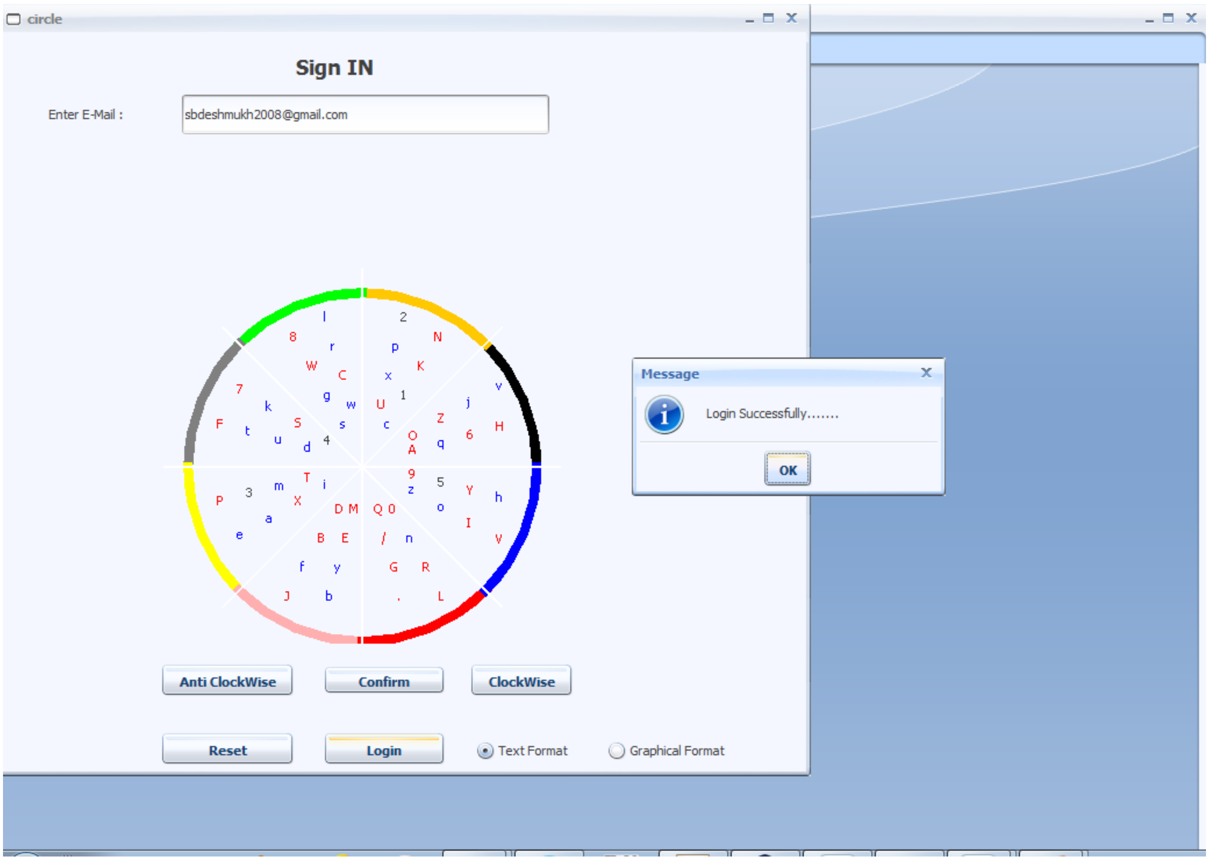
Registration Process is Carried Out in Following Steps,

1. Click On Register
2. Enter Full Name
3. Enter E mail Address
4. Enter mobile number
4. Enter Password
5. Confirm password
6. Select Color
7. Register or Cancel

3.2 User Login

In this phase system displays a circle which compose of 64 character and eight sectors. Each sector is used for representing a color. Initially, 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 counterclockwise by clicking the “counterclockwise” button once,

Here user has to move the characters in such a way that each character retains in selected color. For rotating a Circle we have button like rotate clockwise, rotate anticlockwise. Also we have button for resetting a password when user enters a wrong character. After selecting a character and moving it in specific color sector user has to click on confirm button to confirm his character entry. After entering all character user has to click on login button.



Enter E-Mail : sbdeshmukh2008@gmail.com

● Text Format ○ Graphical Format

Login Successfully.......

Fig 2. User login

Here to provide high level of security we have implemented a two way security mechanism. Hence after successful login user must have to enter a one time password which has be send to his registered email id. User can enter his one time password by directly using textual box or user can again enter his otp by using a circle which we had used in previous step. We had used two level security by using one time password. User can enter his OTP by entering it directly using text box or he may use graphical password. Making selection we had used option box.

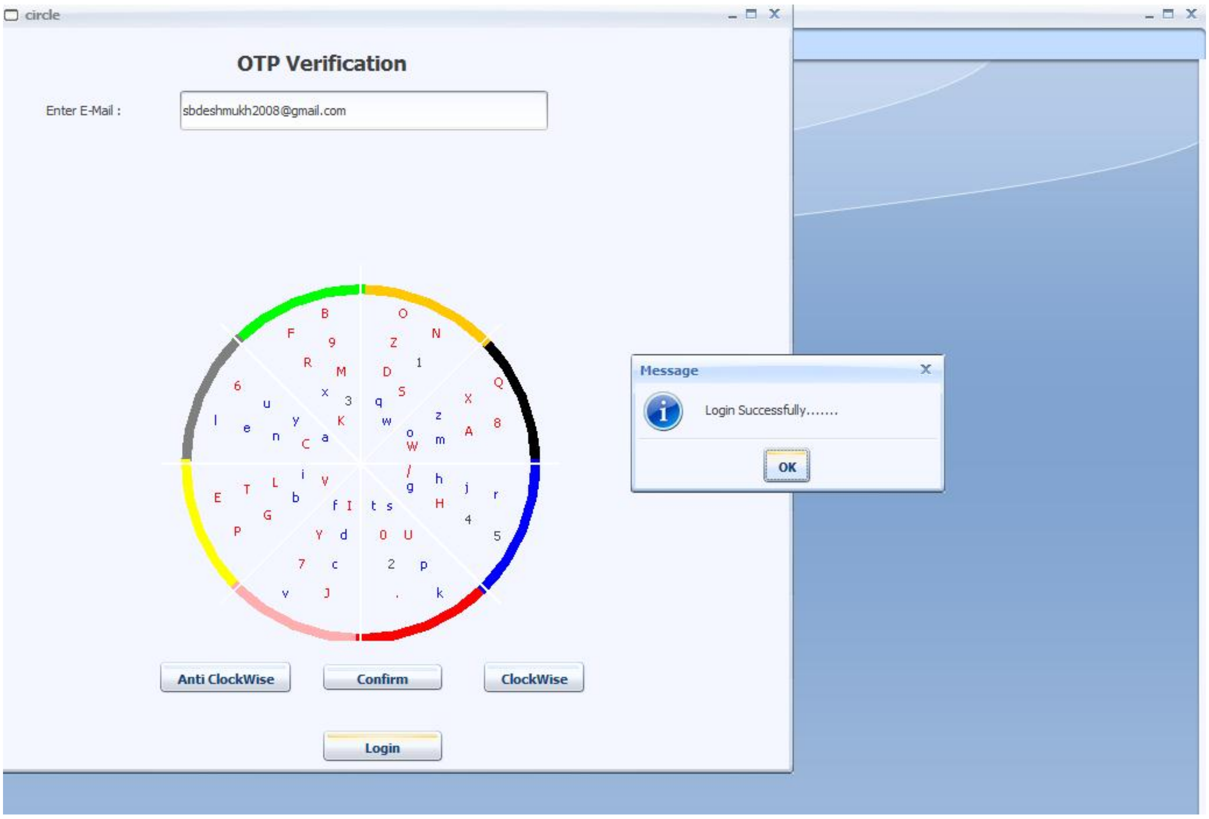
To login the system, the user has to finish the following steps:

Step 1: The Login Screen is shown to user.

Step 2: In The Login screen user has to enter his E mail Id. After Enter e mail id user have to select his textual password step by step and have to put in selected Circle.

Step 3: In this step 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.

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.


circle

OTP Verification

Enter E-Mail : sbdeshmukh2008@gmail.com

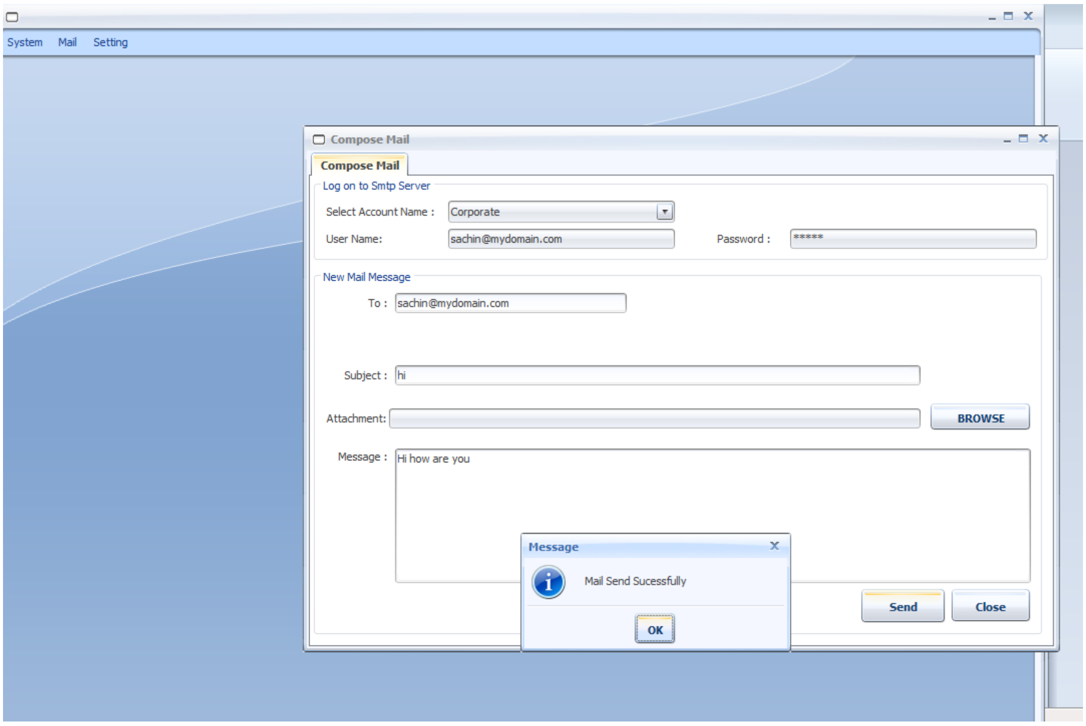
Message

Login Successfully.......

Fig 3. OTP Verification

3.3 Example System

.


Compose Mail

Log on to Smtp Server

Select Account Name : Corporate

User Name: sachin@mydomain.com

Password : *****

New Mail Message

To : sachin@mydomain.com

Subject : hi

Attachment:

Message : Hi how are you

Message

Mail Send Sucessfully

Fig 4. Example System

After successful login user enter into Corporate E-mail system. In which user can perform some basic operations like-send mail, receive mail, view mails in inbox etc. By using this corporate email system user can send mail to his members by using system

IV. ANALYSIS

The main Advantage of Our Project over other system is that we had used two steps security. So even after entering his text and color based password user again have to enter One time password which is send to his registered e mail id. To provide better security we had provided options to enter OTP, user can directly enter his OTP or he may use text and color for entering OTP. To break the system user hacker must have to know E mail Address of the user, Then his textual password, then color of sector, then OTP password, then Password of Registered e mail address. So here 5 steps Security is provided. So The chance of Accidental login, shoulder surfing attack etc is very less.

1. Login time :-

In our Password Scheme we used to methods for entering One time Password. First is using simple text box and second is using graphical password. The Time required for Login is directly Proportional to Length Of Password. As the length of Password Increases the Time required to login gets increased. Again The length of Password is also directly Proportional to Security. Maximum Length password has maximum Security. We had drawn a graph of length versus time. We had carried out experiment of Entering Password by batch of 20 students. and From Them we had taken the average result.

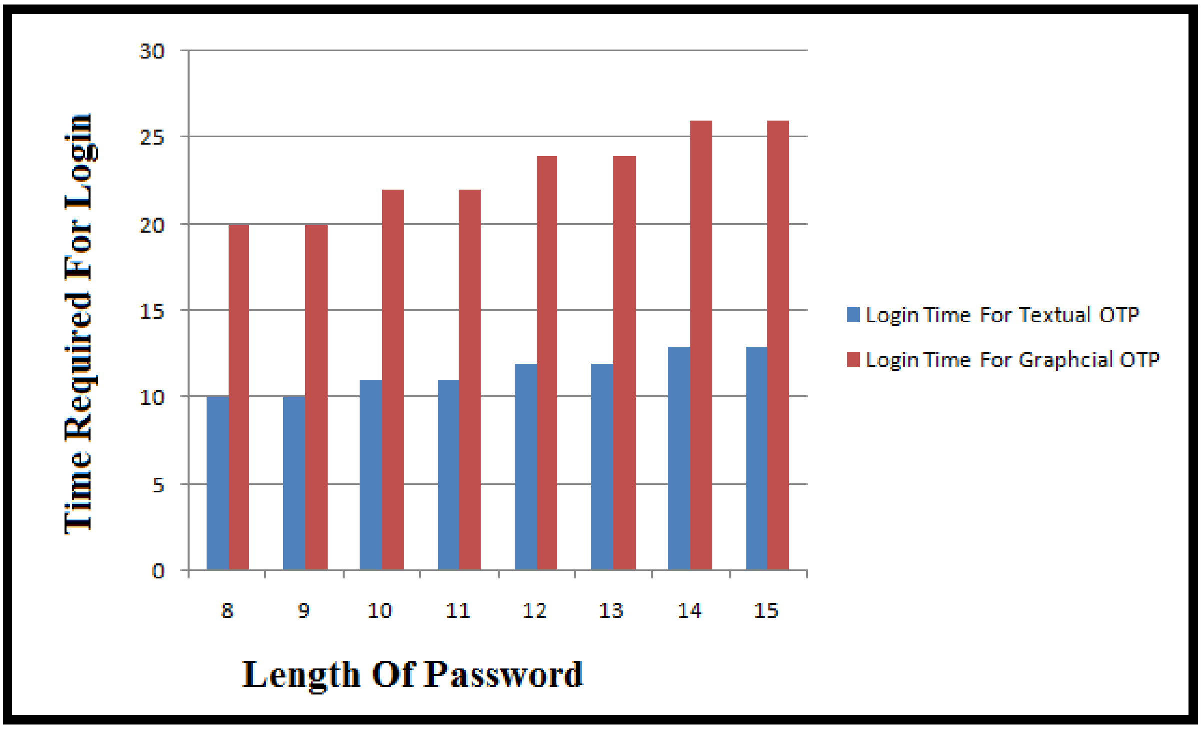


Fig 5. Graph Of Time Versus length for Novice User

We had carried same experiment of Entering Password by batch of 20 trained students. We found that as the students are trained the time required to enter password gets reduced. From this we had taken the average result.

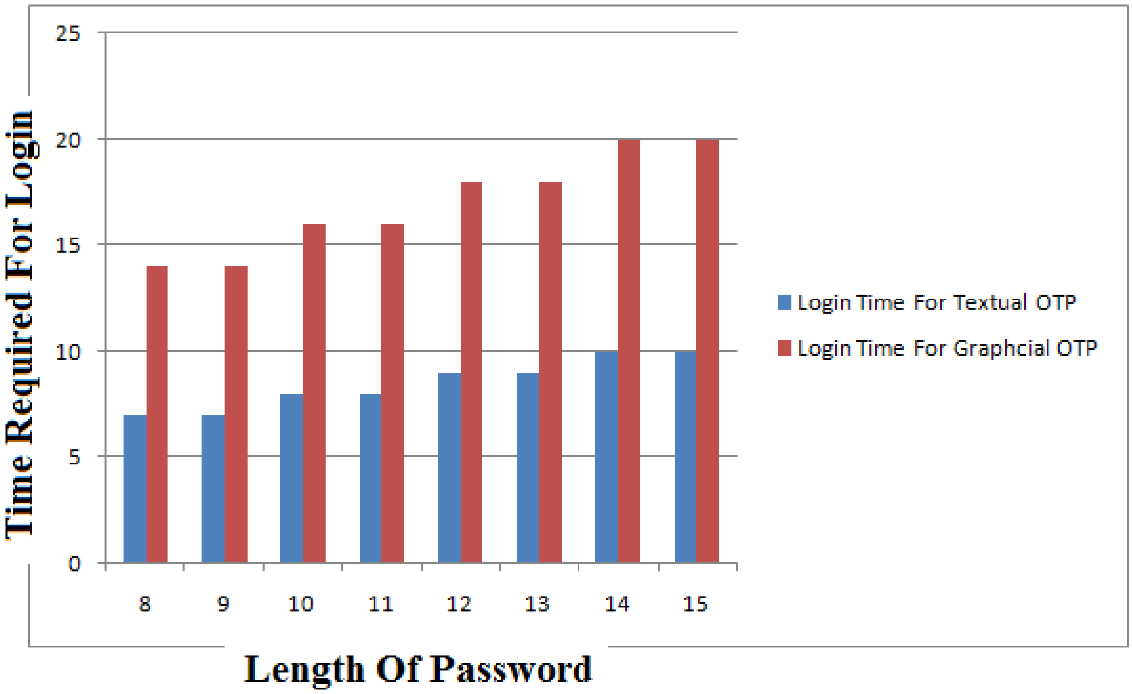


Fig 6. Graph Of Time Versus length for Trained User

2. Resistance to Accidental Login :-

Accidental Login means chance of entering password accidently.We had used two level security. So Even if user enters password accidently in next step user again have to enter the password which is his One time Password. Probability of Accidental Login Is calculated by Formula,

PL=(1/8)^L,
Where 8<L<15

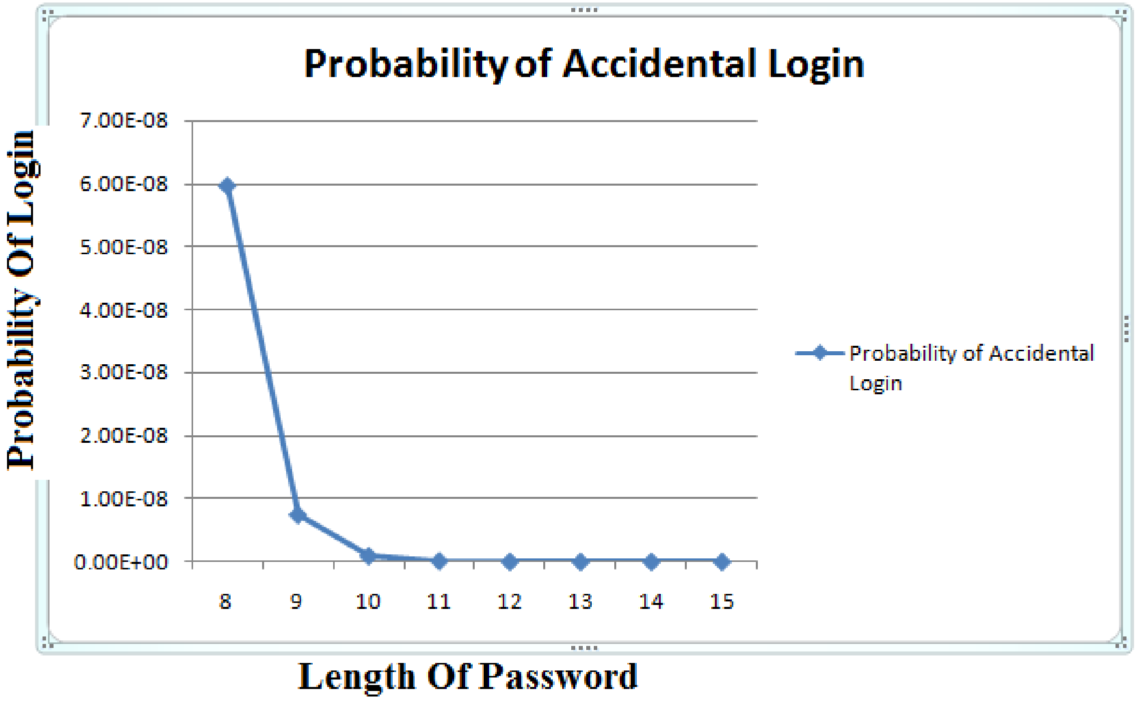


Fig 7. Accidental Login Probability

3. Password space

The password Space of our scheme is calculated by formula,

P= 8 * (64)^L

Where 8<L<15

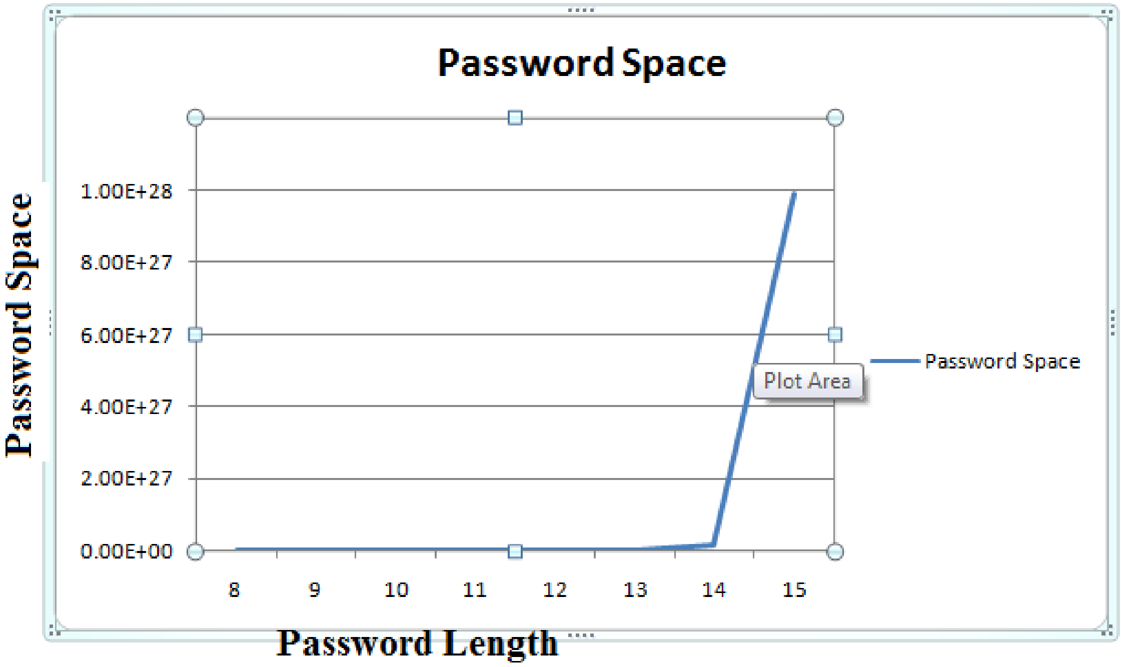


Fig 8. Password Space

4. Resistance to Shoulder Surfing :-

Shoulder surfing is a attack in which hacker sees the action of Shoulder and guess the password. In our password scheme we had used two step authentication.

Again in First step authentication user rotates the character from sector to sector. For hacker it is not possible to see what user enters. So even if user sees password he must have to know his e mail address, password of email address, one time password. So shoulder surfing also never happens.

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.