Password Authentication Using Colour Matrix & Persuasive Click Points

Priyanka Srivatsa[1], Poojitha Ramachandra[2], Mashitha.A[3], Srilekha.G[4], Shikha[5]

Department of Computer Science & Engineering, M.S.Ramaiah Institute of Technology, Bangalore- 560054.

[1]priyanka.srivatsa@live.com, [2]poojitha.ramachandra@gmail.com, [3]mashitha42@gmail.com, [4]lekha.sri.g@gmail.com, [5]shikha@msrit.edu

Abstract- **The growth of technology in computer science & the popularity of information technology among the common people; changed the means of information exchange from letters to electronic messages. Security became a major concern with the advent of electronic messages as it led to higher possibilities of information vulnerability. One of the proposed solutions to this problem is the usage of passwords to protect authenticity of the information. PASSWORD is a word or a string of characters used for user authentication to prove identity or approval to gain access to a resource, which should be kept secretive from unauthorized users. The most common type of passwords is TEXTUAL PASSWORDS, NUMERIC PASSCODES or ALPHANUMERIC PASSCODES. These are vulnerable to various kinds of attacks such as shoulder surfing, eaves dropping, dictionary attack, spyware attack etc. This paper proposes a unique idea of AUTHENTICATING PASSWORDS USING COLOUR MATRICES & PERSUASIVE CLICK POINTS. These authentication mechanisms generate stronger passwords & thereby present a more feasible way of varying the security level of an application or a file depending upon the user's requirement.**

Keywords:-* password, authentication, colour-matrices, click-points, encryption, decryption, shoulder-surfing, eavesdropping, dictionary attack

I. INTRODUCTION

The problems of knowledge based authentication – typicallytext based passwords, are well known. Users often create memorable passwords that are easy for the hackers to guess, but strong, system-assigned passwords are difficult for the users to remember. A password authentication system should encourage strong passwords while maintaining ease of usage & memorability. The proposed authentication schemes allow users, their choice,while influencing users to choose stronger passwords. The proposed system makes the task of selecting weak passwords more tedious, discouraging users from making such choices. In effect, this approach makes choosing a more secure password the path-of-least-resistance. Rather than increasing the burden on users, it is easier to follow the application for the creation of a secure password - afeature lacking in most systems.

This paper proposes a unique idea of using colour matrices and images in various authentication schemes. Colours are allocated priority and the user is expected to input the right priority during authentication. A combination of alphabets and numbers has been used to increase the strength of the password. Images play a major role in creating strong passwords. This system proposes the concept of persuasive cued click points implemented on images such that the co-ordinates of the clicked points are mapped onto the database and later, verified to confirm the user's identity.These schemes are resistant to shoulder surfing. This system can be used with various file uploading, hard-disk locking, folder locking and web-login applications.This authentication system can be integrated with social networking applications,cloud applications, system specific applications and used mainly in Defence, Airline, IT, Fashion, Manufacturing, Research, Banking & Nuclear sectors.

II. RELATED WORK

M Sreelathaet al. [1] proposed two authentication techniques based on text and colours for PDAs (Personnel Digital Assistants). These techniques generate session passwords and are resistant to dictionary attack, brute forceattack and shoulder-surfing. Both the techniques use grid for session passwords generation. Pair-based technique requires no special type of registration; during login time based on the griddisplayed a session password is generated. For hybrid textual scheme, ratings should be given to colours, based on these ratings and the grid displayed during login, session passwords aregenerated. However, these schemes are completely new to users and the proposedauthentication techniques should be verified extensively for usability and effectiveness.

Shruti Bhavsaret al. [2] developed authentication schemes for PDAs (Personnel Digital Assistants). These schemes authenticate the user by assigning session passwords. For every login process, users have to enter different passwords. Session passwords provide higher security against various attacks such as dictionary attack, brute force attacks, as password changes for every session. However, this scheme is completely new to the user, but if practiced, then the user will find it easy to generate session password. Thus, it reduces the complexity and increases the usability.

D Anu Radha et al. [3] gives an idea of having an effective authentication system, which provides strong and easily remembered graphical passwords with dynamic security level.

III. AUTHENTICATION SCHEMES

This paper proposes an implementation that permits the user to choose the level of security he desires for the application. Accordingly there are three levels of security: Easy, Intermediate & Expert, which are proposed. Easy & Intermediate levels have 3 unique authentication schemes each, (E1, E2, E3) & (M1, M2, M3) respectively, that appear in random for the user. Expert level offers a 2 step authentication process utilising the schemes H1 & H2 respectively. The authentication technique consists of 3 phases: signup phase, sign-in phase and verification phase. During signup, user clicks images or rates the colours. During sign-in phase, the user has to enter the password based on the interface displayed on the screen. The system verifies the password entered by comparing with content of the password generated during signup.

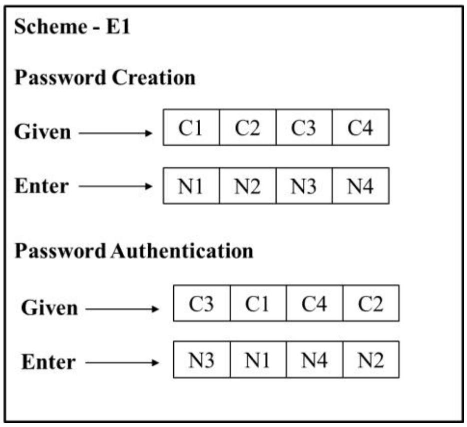

Figure 1: Scheme-E1

With reference to Figure 1, during signup, the user enters numeric priority for each colour displayed in the form of matrix and has to remember the priority he has entered for each colour. During sign-in, the colours are displayed in random order in the form of a matrix. The user has to enter the right priority for every colour.

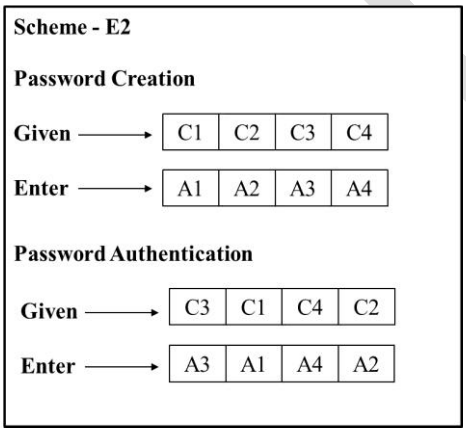

Figure 2. Scheme-E2

With reference to Figure 2, during signup, the user enters alphabetic priority for each colour displayed in the form of matrix and has to remember the priority he has entered for each colour. During sign-in, the colours are displayed in random order in the form of a matrix. The user has to enter the right priority for every colour.

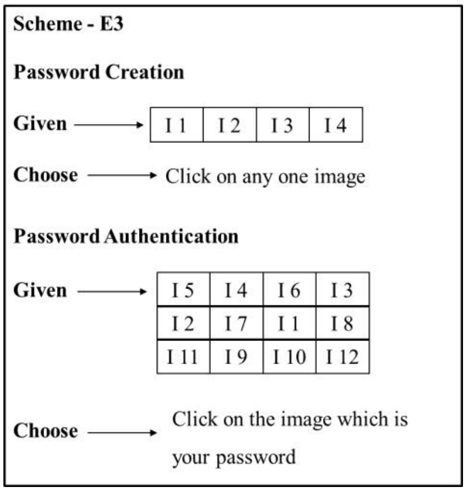

Figure 3. Scheme-E3

With reference to Figure 3, during signup, the user selects an image out of 4 images. During sign-in, he has to select the same image.

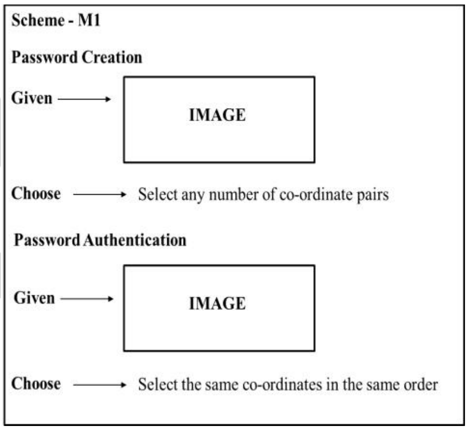
Scheme - M1
Password Creation
Given
IMAGE
Choose
Select any number of co-ordinate pairs
Password Authentication
Given
IMAGE
Choose
Select the same co-ordinates in the same order

Figure 4. Scheme-M1

With reference to the Figure 4, during signup, an image is displayed. User has to select one or more points on the image displayed. During sign-in,the points have to be clicked in the same order.These points are called cued points.

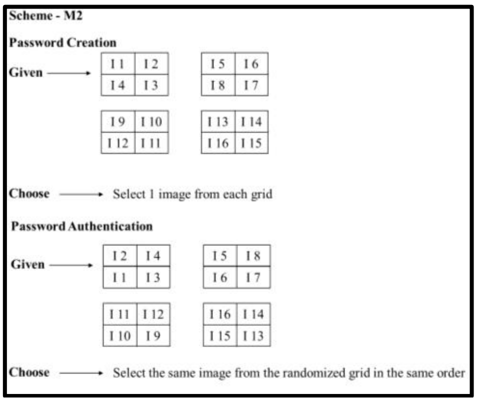

Figure 5. Scheme-M2

With reference to Figure 5, during signup, 4 grids with 4 images are displayed. User has to select one image from each grid. During sign-in, images have to be clicked in the same order.

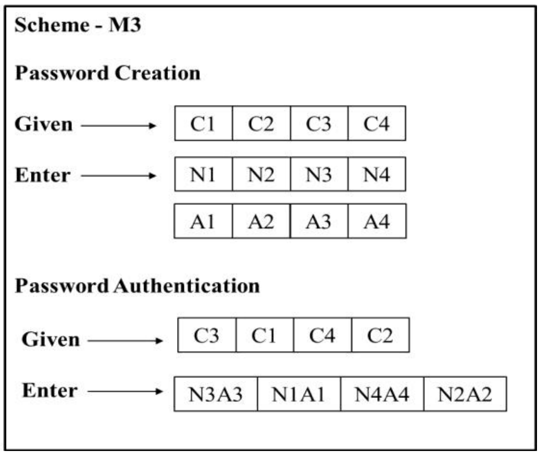

Figure 6. Scheme-M3

With reference to Figure 6, during signup, the user enters both alphabetic and numeric priority for each colour displayed in the form of matrix and has to remember the priority he has entered for each colour. During sign-in, the colours are displayed in random order in the form of a matrix. The user has to enter the right priority, which is a combination of a number and alphabet in the right order, for every colour.

Expert Level has a two-step authentication scheme:

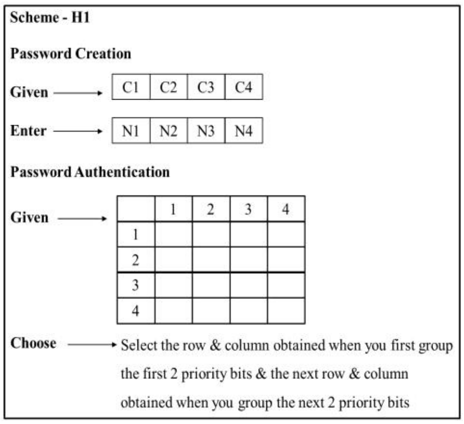
Scheme - H1
Password Creation
Given
C1 C2 C3 C4
Enter
N1 N2 N3 N4
Password Authentication
Given
1 2 3 4
1
2
3
4
Choose
Select the row & column obtained when you first group the first 2 priority bits & the next row & column obtained when you group the next 2 priority bits

Figure 7. Scheme-H1

With reference to Figure 7, during signup, the user enters numeric priority for each colour displayed in the form of matrix and has to remember the priority he has entered for each colour. During sign-in, a 4x4 grid is displayed. User has to select grid [priority1][priority2] as the first pair of row & column and [priority3][priority4] as the second pair of row & column.

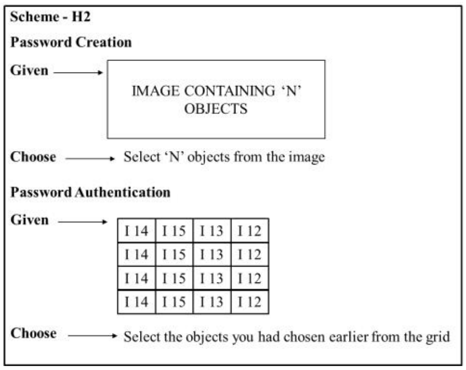

Figure 8. Scheme-H2

With reference to Figure 8, during signup, the user selects one or more images out of the many displayed images. During sign-in, he has to select the same set of images in the same order.

IV. SECURITY ANALYSIS

As the interface changes every-time, the password changes. Even if the user chooses the same password sensibility level, since the schemes appear in random, the password generation would become a dynamic process.

A. *Dictionary Attack:* These attacks are directed towards textual passwords where the hacker uses a dictionary & tries one word after another. This attack can be resisted by using the authentication schemes that uses just images, alphabets & numbers as proposed by this paper.
B. *Shoulder Surfing:* These schemes are resistant to shoulder surfing as every-time, a colour & a number or an alphabet need to be associated. These colours appear in random order during authentication every-time. The schemes appear randomly & therefore become difficult for the hacker to recollect & crack the password.
C. *Guessing:* The authentication schemes appear randomly & involve a combination of colours & images. The colours need to be associated with numbers & alphabets. The co-ordinate points in the images need to be remembered. The images & their order need to be remembered. This system is very hard to be broken by guessing. The chances are very minimal.
D. *Brute-Force Attack:* The use of colours & images rapidly minimize the possibility for a brute-force attack. The authentication schemes appear in random every-time a user wants to use this system. This drastically reduces the possibility of a brute-force attack.
E. *Complexity:* The complexity of this system is high as it uses 8 authentication schemes in all. Easy & Intermediate levels have 3 authentication schemes each which appear randomly for the user. So the probability of a single user, being exposed to all the authentication schemes is very less. The Expert Level provides a 2 step authentication facility. These factors increase the complexity of the system enabling security.

CONCLUSION

The proposed authentication schemes influence users choose stronger passwords.

Users can successfully login by giving the right password and the forgot password functionality allows user to reset the password.

This paper proposed a unique idea of using colour matrices and images in various authentication schemes. Colours were allocated priority and the user was expected to input the right priority during authentication. A combination of alphabets and numbers has been used to increase the strength of the password.

This system, when compared to the existing text-based authentication systems, is less prone to shoulder surfing as mapping of 4 colours to 4 numbers within seconds is difficult. Further it is less prone to eavesdropping, as every time a different sequence of numbers is sent over the network for the same user.

Images played a major role in creating strong passwords. This system proposed the concept of persuasive click points implemented on images such that the coordinates of the clicked points were mapped onto the database and later, verified to confirm the user's identity. Images create greater visual appeal that leads to better memorability of the password. Also, the system is cost efficient than the image processing and biometric systems.

This application is now a desktop-based application. It can be developed into a web-based application & deployed on the cloud. Several other authentication schemes can be devised in accordance with the environment in which the application can be deployed. A customized version of this authentication system can be developed after analyzing the industry where it would be deployed, the number of users, the various levels of employees in that industry or enterprise.

ACKNOWLEDGEMENT

It gives us immense pleasure to thank the Head of Department, Dr. K.G Srinivasa, for giving us an opportunity to present this paper. We extend our sincere gratitude to the Project Co-ordinator, Mrs.Seema, Associate Professor; Dept of CSE for her regular inputs. We take pleasure in thanking Ms. Shikha, Asst Professor, Dept. of CSE, MSRIT for constantly guiding us. We are obliged to the staff members of CSE Dept MSRIT for the valuable information provided by them as & when necessary.

REFERENCES

[1] M Sreelatha , M Shashi , M Anirudh , MD Sultan Ahamer, V Manoj Kumar, "Authentication Schemes for Session Passwords using Colour and Images," International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011

[2] D.Anu Radha ,C.Abdul Hakeeem, "A Persuasive Cued Click-point based Authentication Mechanism with Dynamic User Blocks ," (IJREAT) International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013.

[3] Shruti Bhavsar, Tejasvini Waingankar , Rupali Thorat, "TCM: Password Protection Using Text And Colour Matrix"

[4] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and P. C.van Oorschot, "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism"

[5] http://www.youtube.com/watch?v=jJjFK4_izp8

[6] http://www.youtube.com/watch?v=mhOvHCS2J6w

[7] http://www.youtube.com/watch?v=2yG0aMOUt-Q

[8] http://www.youtube.com/watch?v=zibcQM9JQEg

[9] http://en.wikipedia.org/wiki/Password

[10] http://en.wikipedia.org/wiki/Encryption

[11] http://en.wikipedia.org/wiki/Shoulder_surfing

[12] http://en.wikipedia.org/wiki/Dictionary_attack

[13] http://en.wikipedia.org/wiki/Eavesdropping