Dynamic Authentication using Random Art Images

Aneesh K[1], Brolin Michael M[2], Subbaraman C S[3]
Department of Information Technology
Government Engineering College
Palakkad, India

***Abstract*—Authentication is the first step in information security. It requires the users to memorize their password and remember at login time. Textual passwords are the most traditional schemes that are used for providing security, but textual passwords are vulnerable to dictionary attacks, shoulder surfing, and spyware. Graphical password schemes overcome the shortcomings of textual passwords, but they are vulnerable to shoulder surfing attacks. To address this problem, text can be used in combination with the colors and images to generate a session password, thereby making a stronger authentication means. In general, session passwords are those that can be used only once and for every session, a new password is engendered. Session passwords provide better security against dictionary and brute force attacks as password changes for every session. The proposed system uses random arts and texts for generating session passwords.**

***Index Terms*—Authentication, Security, Random art, Shoulder Surfing, Dictionary attacks.**

I. INTRODUCTION

The most common method used for authentication is textual password. The vulnerabilities of this method like eaves dropping, 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. 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. Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these devices**.**

Thus we propose a new authentication technique which uses session passwords. Session passwords are passwords that are used only once. Once the session is terminated, the password is no longer useful. For every login process, user has to input a different password. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. The proposed authentication scheme uses random arts for generating session passwords.

II. LITERATURE SURVEY

Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these devices. The most common methods used for authentication are textual passwords, graphical passwords, biometrics etc. The vulnerabilities of these methods are eves dropping, dictionary attacks, social engineering attacks and shoulder surfing. Several types of authentication schemes have been reviewed for this work and this paper eliminates almost all the drawbacks in these schemes. Some of the authentication techniques are given below.

Ms Grinal Tuscano, Aakriti Tulasyan, Akshata Shetty, Malvina Rumao, Aishwarya Shetty et al.[3] proposed a graphical password authentication technique which focuses on providing more powerful secure authentication mechanism. The system goes through several phases before creating a password and logging into the system, such as image selection, image distortion, text association and finally password generation.

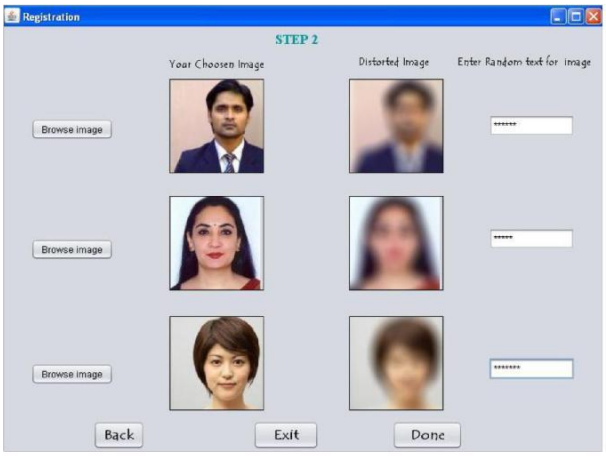

Fig.1: Registration

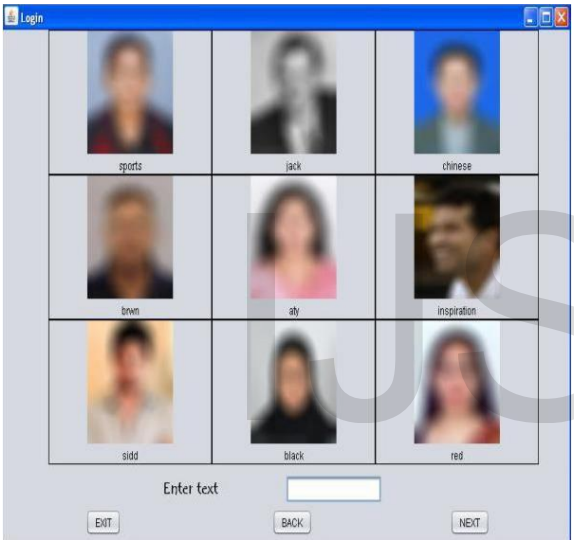

Fig.2: Login

The user provided images are distorted using distortion techniques. During authentication phase the user need to identify the distorted version of the original image from a set of images and also enter the associated text. The system shuffles the images in the grid during each login.

Manjunath G, Satheesh K, Saranyadevi C, Nithya M et al.[4] introduced a shoulder surfing resistant graphical password authentication mechanism. The alphabets used in this scheme contains 64 characters, including 26 upper case letters, 26lower case letters, 10 decimal digits, and symbols "." and "/".

During registration the user has to set his textual password K of length L characters, and choose one color as his pass color from 8 colors assigned by the system. During login the system displays a circle composed of 8 equally sized sectors. The colors of the arcs of the 8 sectors are different, and each sector is identified by the color of its arc. The 64 characters are placed randomly among these sectors.

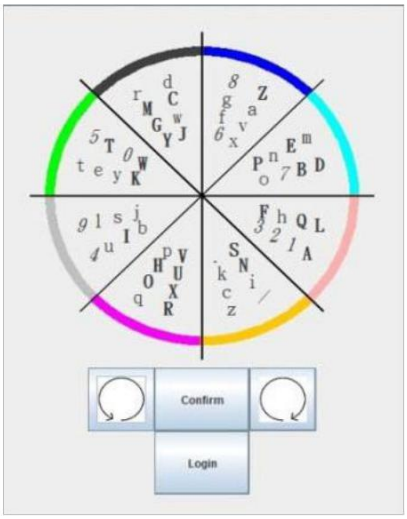

Fig.3: Spin wheel Authentication

All the displayed characters can be simultaneously rotated in clockwise or anti clockwise by clicking the clockwise or anti clockwise button respectively. The user has to rotate the sector containing the i-th pass character of his password K, denoted by Ki, into his pass-color sector, and then click the "Confirm" button. After entering the password in this way user needs to click the login button.

S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara Reddy et al. [6] developed a high security graphical and textual password authentication system that will resist almost every attacks to a limit. It includes 3 phases: registration, primary level authentication and secondary level authentication (draw-a-secret).

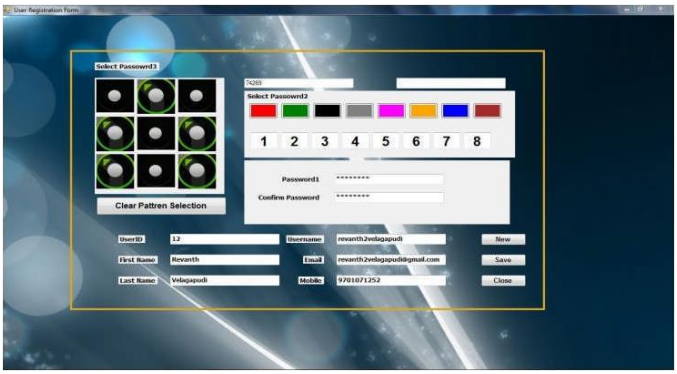

Fig.4: Authentication

A new user has to register by providing a secret pass which is remembered as pair based and also should rank colors from 1 to 8.At last a graphical password should also be sketched.

During primary level authentication the user can choose either pair-based or textual-based authentication.

In pair based authentication, a grid which consists of both numbers and alphabets arranged randomly. The secret pass is remembered as pair where first letter describes the row and second, the column. The intersection letter of the selected row

and column generates the character which is a part of the session password.

Hybrid textual authentication uses a set of colors displayed on the login interface are ranked based on the ranking given during registration. The ranking of colors needs to be remembered as a pair where the first number denotes the row and second, the column. The intersection number of the row and column in the interface grid will be the password for the session.

In the secondary level authentication a 3x3 grid with dots is shown and the user has to draw the pattern which he has given during registration. If both the patterns match, then the user will be given access to the files and folders .

Dhamija and Perrig et al. [2] proposed Dej'a Vu, a system for user authentication. Dej'a Vu is based on the observation that people have an excellent memory for images. Using Dej'a Vu, the user creates an image portfolio, by selecting a subset of p images out of a set of sample images. To authenticate the user, the system presents a challenge set, consisting of n images.

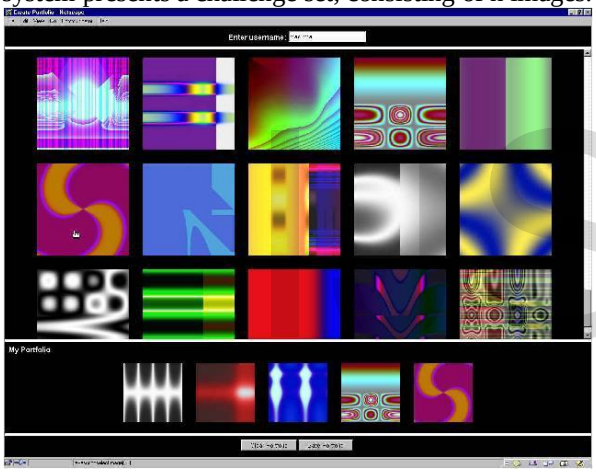

Fig.5: Portfolio images

This challenge set contains m images out of the portfolio. The remaining n-m images are called the decoy images. To authenticate, the user must correctly identify the images which are part of his portfolio.

Sonia Chiasson, van Oorschot and Robert Biddle et al.[5] developed a technique called Cued Click Points(CCP). In this, user clicks one point on each of c (for example c=5) images rather than on five points on one image. In CCP, each click results in showing a next-image, in effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click.

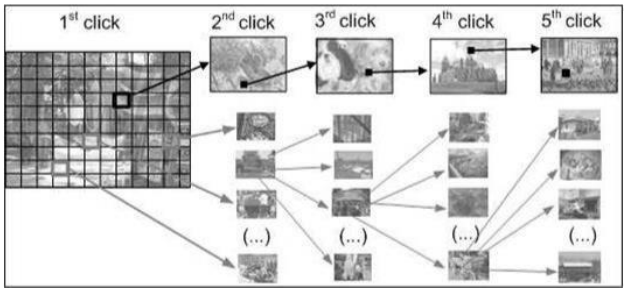

Fig.6: Cued Click Points

III. PROPOSED SYSTEM

General

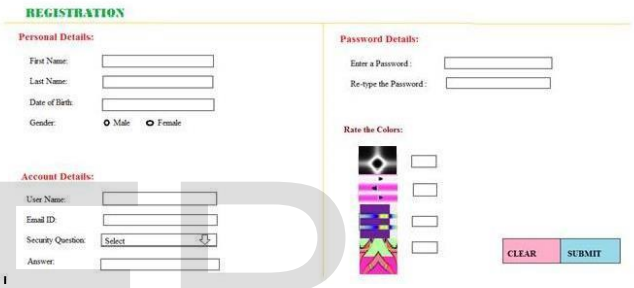

Fig.1: Registration

First the system checks whether the user is already registered or not. If yes, then it advances to the login phase, but if the user is not registered then first he will go through registration and then to the login step. At the time of transaction the random art pairs and grid will be shown. From this interface, the user can enter the session password. This password will be verified at the verification phase. Once the user logs out, a new session will be generated and, the grid and random art pairs will be shown to the user again.

Authentication Scheme

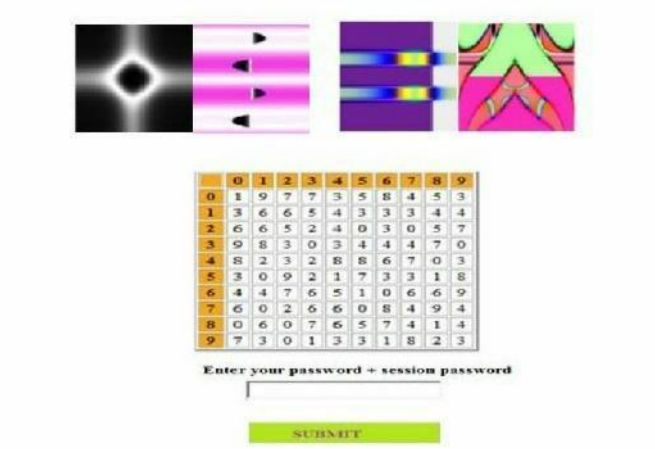

Fig.2: Login

1. During registration, user should rate random arts as shown in figure 1. The user should rate random arts using numbers from 0-9. Same rating can be given to different random arts.

2. During the login phase, when the user enters his username, an interface is displayed based on the random art images selected by the user. The login interface consists of grid of size 10x10. This grid contains digits 0-9 placed randomly in grid cells. The interface also contains strips of random arts as shown in figure 2. The random art grid consists of 2 pairs of random art images. Each pair of random art represents the row and the column of the grid.

Figure 2 shows the login interface having the random arts and number grid of 10 x 10 having numbers from 0 to 9 randomly placed in the grid. Depending on the ratings given to random arts, we get the session password. As discussed above, the first random art of every pair represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. Consider figure 1 ratings and figure 2 login interface for demonstration. Suppose the ratings for the figure 6 is given as 5362 at the time of registration. Now at the time of login after verifying the existence of username the user is expected to enter the session password. Consider figure 2; first pair has black shaded and pink shaded random arts. The black shaded random art rating is 3 and pink shaded random art rating is 6. So the first letter of session password is 3rd row and 6th column intersecting element i.e. **4**. The same method is followed for pairs of violet and green shaded random arts. For figure 7 the password is **"40".** Instead of digits, alphabets can also be used. For every login, both the number grid and the random art grid get randomized and thus the session password changes for every session. Similarly we can implement this system using 8 eight different random arts and correspondingly there will be a 4 digit session password to be entered at the time of registration.

IV. CONCLUSION

The proposed technique generates session passwords and is resistant to dictionary, brute force and shoulder-surfing attacks. This technique uses grid for session password generation. As we use random art images, the system eliminates almost all the vulnerabilities of other authentication techniques. Based on the ratings given to random arts and the grid displayed during login, session passwords are generated. However this scheme is completely new to the users and the proposed authentication techniques should be verified extensively.

V. REFERENCES

[1] Shefali Amlani, Shweta Jaiswal, Suchitra Patil, " Session Authentication using Color Scheme" in*(IJCSIT) International Journal of Computer Science and Information Technologies*, Vol. 6 (2) , 2015, 1420-1423.

[2] Rachna Dhamija, Adrian Perrig, "D´ej`a Vu: A User Study Using Images for Authentication" in *SIMS / CS, University of California Berkeley.*

[3] Ms Grinal Tuscano, Aakriti Tulasyan, Akshata Shetty, Malvina Rumao, Aishwarya Shetty, "Graphical password authentication using Pass faces" in *Int. Journal of Engineering Research and Applications www.ijera.com* ISSN : 2248-9622, Vol. 5, Issue 3, (Part -5) March 2015.

[4] Monali Bendale, Neeta Singh, Sujata Baid, Aman Maurya, " A Simple Text Based Graphical PasswordScheme toOvercome Shoulder Surfing Attacks" in *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 4, Issue 3, March 2015.

[5] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points" in *Springer- Verlag* Berlin Heidelberg June 29, 2007.

[6] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara Reddy, " Authentication Techniques for Engendering Session Passwords with Colors and Text" in *Advances in Information Technology and Management*, Vol. 1, No.2,pp.71-78,2012.