A Novel Session Password Security Technique using Textual Color and Images

P Kavitha Rani¹, Sai Krishna R¹, Siddarth U S¹ and Vidya Sagar E¹
¹Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India.
kavitharanip@skcet.ac.in, 17eucs131@skcet.ac.in, 17eucs149@skcet.ac.in, 17eucs175@skcet.ac.in

Abstract. Traditionally people will be using a weak password that has to be often changed can be influenced by a dictionary attack, shoulder surfing, and other methods of password cracking. After the past years, graphical passwords came into existence however; they are not as useful as the traditional password method, since they take more time to authenticate the passcode. As a result, this paper has taken a study of session password strategy in which the password is used only once for each session and, as that session ends, the password no longer provides access. The suggested session password scheme would us a "text" session password. Once upon a time, textual passwords were the most often used technique for authentication. Password are vulnerable to many scenarios, such as shoulder surfing, social engineering attacks, and lazy password selection. Graphical keys are introduced as a way to express very important passwords. Nearly all of the graphical schemes are vulnerable to shoulder pack design. To contend with the downside of being unable to remember passwords, pictures may be used to pair with session passwords for authentication. A session secret of a completely new password can only be used any time a new password is created. During this article, two approaches are expected to become a welcome cure for depression with an in-session approach that is unpredictable to shoulder ache and color. Strategies for Digital Assistants that is suitable for private uses. The proposed system measures the security and usability of the proposed system and displays the assistance of the proposed system to shoulder surfing assault.

Keywords: Authentication, Graphical password, Text, Digital Assistants

1. INTRODUCTION

Internet has been a staple of operation today. Due to the fact that all types of user names and passwords are being fake, account details must be given something unique to prevent hackers from purchasing and altering the data present in the account. Phishing is a type of attack in which the attacker tries to obtain the person's information such as user-id,\password, pin no, etc. by showing the user to assume that he is communicating with a trustworthy person. A phishing email will be sent out to users asking them to click a connection from their email and it will take them to a fake web site that can exploit their computer and install malicious code into their computer. Often you may receive a phishing email in which it would ask you to provide your account information for verification purpose. Therefore, you would need to create and use separate user accounts to secure the accounts. The standard technique used for authentication is the use of a text-based password. The biggest vulnerabilities of this form of technology are dictionary attack, social engineering attack, and shoulder surfing attack. A book of definitions.
Attack is a technique for defeating authentication mechanisms with the purpose of ... The attacker tries to discover or produce the key necessary for entry into user's It is a systematic method in which words or terms being looked up from a dictionary file are entered as the password to a password protected system. Then instead of surfing the Internet, the hacker looks over the person's shoulder in their desk while they are typing in words from the dictionary as the password. The "pass-the-hash" method is an attack where an observer attempts to watch the characters typed by the user to learn the password entered by the user. Out of all possible ways of surfing the web, I think the top three are shoulder surfing, true knitting surfing and surfing the web while sleeping. As the keyboard is openly displayed on the screen of the device, it makes very easy to observe what key has been pressed by the user. Shoulder surfing could be possible if there was a full recording of your keyboard entry or if the crime was committed using a CCTV camera or if you saw the typist still typing on the keyboard. The shoulder surfing attack mostly happened at public places or on public networks because the login process can be watched by several people and because the device is not entirely under the user control. Password files that include nicks and items such as drawers and digits are easy to work with, which are a serious problem with the limited space on the letter-based password. The issue of having passwords stolen by unauthorised users while being typed manually is one reason why a virtual keyboard that stores passwords in the browser is one of the most secure ways to enter passwords. It is an on-screen alternative to a keyboard that minimises the use of a keyboard. Users can only press the screen to enter their passwords. However, it is not mandatory upon the user to use the virtual keyboard. This is much easier to use in terms of entering a password as opposed to a standard keyboard. Online banking operations are vulnerable to criminal offence and fraud as they are done in public places like Internet cafes, computer labs at schools, etc. etc. Instead of passwords that are long and complex, passwords that have more graphical aspects are added. Graphical passwords are easier for us to recall than textual passwords. That's also caused by their graphical nature and implementation of single-use passwords. However, all existing graphical password authentication methods are vulnerable to shoulder surfing, which is a proven attack where an observer captures the current password by recording the session of authentication or by direct surveillance. In addition, graphical login. The authentication involves a greater expense than the textual passwords. There are some drawbacks of using passwords with a text-based password, and it can be difficult to remember them all. As a parallel, graphical passwords can be affected by shoulder-surfing attacks, and implementing it can be costly. In a practise, it is easier to have more than one username and two different types of passwords. This paper proposed a technique that creates a session password by using two random factors. This protoge of an access designed by the authors of this paper is known as the PAIR-based password scheme In the paper (E-Authentication-Based-Session-Based-AES-BASIC-Authentication) session based authentication scheme is proposed. We have designed a password scheme where we generate the password by pairing it with a password stored in servers. Session keys, or session codes, are temporary codes that are used for only one transaction. After the session has been ended, the session password is not of any use again. In order to successfully log in, users have to enter various passwords. Session passwords make sure that shoulder surfing is not possible because each purchase (i.e. each session) changes the session password.

2. RELATED WORK

From this book, we shall understand the basic concepts this book describes in a simple, step-by-step, screen-by-screen approach on how to learn four authentication methods. The common authentication techniques used are alphanumeric and graphical. [1,2, 3]

In alpha numeric password,

- The password must be at least 8characters long.
- The password should not be easy to crack.
- The password should not be a term in plain English [4].
Since humans live in a world where the sense of sight is dominant, our brains are capable of processing vast quantities of information with ease. Despite being able to recall fifty plus characters, it's very wide in size, and offer large password spaces to hackers to hack. Graphical password schemes can have clearer passwords when maximizing the security measures.\[5\][6]

Session authentication systems involve special password that is used only once. If the session ends, the password can no longer be used. Users are required to enter different passwords for every login operation. The session passwords provide better protection against dictionary and brute force hacking attempts. This happens because the user still has to repeat the password. It is difficult to recall the password to take part in the voting.

Retain ability and ease of use are drawbacks of using graphical passwords as they are easily traceable. Here text and picture were combined to create the session password and is then changed once users log out.\[7\]

Dhamija and Perrig suggested a graphical authentication strategy, where users have to pick some images from a collection of random pictures when they want to register and then when they sign in, they would have to choose the same sequence of images which they have pre-established when they registered. This algorithm can be a simple target to shoulder-surf. Though you take a long time to log in, this system has very low failure rate. \[8\]

Real User Corporation has created Pass face technique, whereby a user must pick one face previously selected by the user. Then, user acknowledges this and clicks anywhere on the known face. Please perform the same measure for multiple rounds of time. The user at this technique has to use photos of friends as the password. As the user has selected four images from the list, he or she is asked to select four images again.\[9\]

The method to allocate representation on the basis of colour has been proposed. After the user clicks a button on the keyboard, all keys on the keyboard are scrambled. Here, user must write down the exact location of the key before pressing the exact key. Finally, it is to press "Hide Keys" button, which will hide all keys from the keyboard. Then, you can find the desired key in the page. For this purpose, one may use colours as a memory tool. \[10\]

Another notion for this project is the eye tracking way. This article has being contrasted with its format present in the database. By this way, it reveals many disadvantages. \[11\]

We suggest an innovative technique called "Draw a Secret," where the user re-draws predetermined picture on two-dimensional map. After you draw specific starting grids in the same series, it is impossible to retrace them. This approach in authentication is susceptible to shoulder surfing assault. \[12\]

A second technique, in which the user has to sign using the mouse, has been developed by Syukri. It has two stages; initial registration and then the later verification. Users must sign up in order to be validated for membership only. However, the bad point of this idea is that there are many individuals who are not so much familiar with working with mouse; therefore, this idea may not work out as well as anticipated.

Haichang et al suggested a new scheme where the users draw pictures of their password in a straight line. Here the users do not have to click on photos which are pre-defined as their passwords. Jansen then suggested a graphical password scheme for mobile devices. A good and original theme makes one password stands out from other. When authenticating files, user must identify them in the same order. Each picture selected for encoding will form a password. Here are six files. All the above. In reality, all systems are vulnerable for various attacks.

Syukri said that input must be accurate so that the input can be processed well. This work will lead to the development of the framework for the protection of users' login information and authentication.
3. EXISTING SYSTEM
The general technique which was previously employed is a Textual password technique which has its own disadvantages. The methodology suggested by technicians is the use of biometric method. A graphical password technique is difficult to be defeated by shoulder surfing attacks but this method is also moderately challenged in nature and costly. We proposed new password authentication technique, which would be virtual keyboard-based. What new authentication system is used? Pair-based? It allows the user to choose numerical grid password. The main objective of this paper is to prevent the shoulder surfing assault. Users have to apply password at the time of registration. And to make it hard, the password should be 8 characters long. Only even or odd numbers are used in the hidden key. Then login process occurs, the grid view of six rows and six columns screened before consumer. The grid display is made up of alphabets and numbers. In this way, this grid keeps every transaction data sequentially. In pair-based scheme, the first letter from the password is looked up as the row and the second letter is looked up as the column and then the intersection which shape will be the part of the session password. Due to shuffling of the keyboard, everybody will not be able to enter and will immediately reset the password. In the proposed scheme new user register would complete data such as username, first name, last name, E-mail, birth date, gender and so on to register new user. In a textual password scheme, strong passwords should be easy to recall, and thus, easier to crack. But the password guessing problem is not simple in a token-based system. But it is safer. This technique is simple to use for the consumer. Suppose the password of user is ARCHIT at login, then a gridded grid will appear on the computer. At the intersection of ARCHIT and RCHAR are all instances of the letters W. Just click on the W for login. See if all letters in the string are in pairs and find intersections by matching identical letters. If the password is right, the user is allowed to enter.

4. PROPOSED SYSTEM
This paper has taken a study of session password strategy in which the password is used only once for each session and, as that session ends, the password no longer provides access in figure 1. The suggested session password scheme would us a "text" session password. Once upon a time, textual passwords were the most often used technique for authentication. Password are vulnerable to many scenarios, such as shoulder surfing, social engineering attacks, and lazy password selection. Graphical keys are introduced as a way to express very important passwords. Nearly all of the graphical schemes are vulnerable to shoulder pack design. To contend with the downside of being unable to remember passwords, pictures may be used to pair with session passwords for authentication. A session secret of a completely new password can only be used any time a new password is created. During this article, two approaches are expected to become a welcome cure for depression with an in-session approach that is unpredictable to shoulder ache and color. Strategies for Digital Assistants that is suitable for private uses. The proposed system measures the security and usability of the proposed system and displays the assistance of the proposed system to shoulder surfing assault.

Secured Login System

![Secured Login System](image)

Figure 1. Flow diagram
Modules:

Registration Process:

Personal Details:
- Providing user's details such as Name, Email, Phone, Gender and Date of Birth.
- In first step, we are securing the login with text passwords by creating and confirming password fields.
- The entered password will be automatically encrypted into hash using SHA1, MD5 which cannot be read by user from the database.
- Once the step 1 process is completed, the user data will be saved into the database but the login will not be activated until the second and third steps are fulfilled.

Image Selection:
The second step of security system in the application will be image keys where there are 6 different types of random numbers generated automatically and the user has to choose and confirm one to be added into their account details as a level 2 security key. Once it's submitted the chosen key data will be updated into their registered row data in figure 2-4.

Process:

Step 1: Display six image keys.

Step 2: User has to choose and confirm one image containing specific keys.

Step 3: The selected image will be added into their account details as a level 2 security measure.

Step 4: Once it's submitted the chosen key data will be updated into their registered row data in the database.

Image coordinates selection:
In this step, there will be an image contains multiple objects within it and each object have some coordinate point value. When user choose one of the object from the image, that specific coordinate point value will be selected and on confirming to submission, the coordinate value will be updated into the database row for the same user. The registration process will be completed with these three steps and the user account is ready to login once success message is shown.

Process:

Step 1: Display an image containing multiple objects within it and each objects having some coordinate point values.

Step 2: User has to choose one of the objects from the image.

Step 3: The specific coordinate point value will be selected and confirmed based on the selected object.

Step 4: The coordinate value will be updated into the database row for that specific user.

Step 5: The registration process will now be completed with these steps and the user is now ready to login.
Login Process:

Login Form:

- The first step contains default way of entering their registered username and password to validate their account.
- If the provided details are not validated, it'll show the error message and if it's validated success, then the application will take the user to next step of authentication Figure 5 and 6.

Image Key verification:

The second step of verification is the image key where the user can see 6 different codes same as in the registration process and one of the key shown in the screen is registered with the user details. When the user refreshes the page, the keys will be refreshed and reordered with its positions. If the user chooses right key, the system will navigate the user to next level verification.

Process:

Step 1: Display 6 different images containing keys

Step 2: The user has to choose the correct image which they selected during the registration process

Step 3: If the user refreshes the page, the images will be reordered with its positions

Step 4: The user has maximum of three attempts to select the correct image

Step 5: If it exceeds the limit, the application goes back to the login page and sends an alert message through whatsapp

Step 6: If the user chooses right key, the system will navigate the user to next level verification

Image coordinates verification:
Once step 2 is authenticated successfully, user can see the next screen with image where the user need to choose the right position on the image to verify with previously chosen location. If the user clicks on right place which matches with the registered coordinate location. The third step of verification will be succeeded and the user will be redirected to dashboard screen.

Process:

Step 1: Display the image showed during the registration phase.

Step 2: If the user clicks on right place which matches with the registered coordinate location. The third step of verification will be succeeded.

Step 3: The user has a maximum limit of three attempts.

Step 4: If the user has exceeded the amount of attempts the application redirects to the login page and also sends an alert message through whatsapp Figure 7.

5. EXPERIMENTAL RESULT
REGISTRATION STEPS

Figure 2. Registration step 1

Figure 3. Registration step 2

Figure 4. Registration step 3

LOGIN STEPS

Figure 5. Login step 1
There are several methods for the prevention of shoulder surfing attacks. Of all developed techniques, the session based one has a considerable protect from shoulder surfing attack due to having a specific session password each session and transactions. This method has potential uses both for defensive purposes and technological advance.

REFERENCES

[1] A User Study Using Images for Authentication, Proceedings of the 9th USENIX Security Symposium, Vol 9, August 2000
[2] Agarwal M et al. Secure authentication using dynamic virtual keyboard layout, Proceedings of the International Conference and Workshop on Emerging Trends in Technology, pp 288-291 ACM
[3] A User Study Using Images for Authentication, Proceedings of the 9th USENIX Security Symposium, Vol 9, August 2000
[4] D. Weinshall, Cognitive authentication schemes safe against spyware, in Proc.IEEE Symp. Security Privacy, May 2006, pp. 300–306.
[5] H. Tao and C. Adams, Pass-Go: A proposal to improve the usability of graphical passwords, Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.
[6] P. Dunphy and J. Yan, Do background images improve Draw a Secret graphical passwords?, in Proc. ACM CCS, 2007.
[7] S. Chiasson, P. C. van Oorschot, and R. Biddle, Graphical password authentication using cued click points, in Proc. ESORICS, 2007, pp. 359–374.
[8] C. van Oorschot and J. Thorpe, On predictive models and UserDrawn Graphical passwords,
ACM Trans. Inf. Syst. Security, vol. 10, no. 4, 2008.

[9] J. Yan and A. S. El Ahmad, A low-cost attack on a Microsoft CAPTCHA, in Proc. ACM CCS, 2008, pp. 543–554.

[10] H. Anandakumar and K. Umamaheswari, A bio-inspired swarm intelligence technique for social aware cognitive radio handovers, Computers & Electrical Engineering, vol. 71, pp. 925–937, Oct. 2018. doi:10.1016/j.compeleceng.2017.09.016

[11] R. Arulmurugan and H. Anandakumar, Early Detection of Lung Cancer Using Wavelet Feature Descriptor and Feed Forward Back Propagation Neural Networks Classifier, Lecture Notes in Computational Vision and Biomechanics, pp. 103–110, 2018. doi:10.1007/978-3-319-71767-8_9.

[12] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, Picture Password: A VisualLogin Technique for Mobile Devices, National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.