ISSN 2320 - 2602
Volume 9 No.4, April 2020
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst01942020.pdf
https://doi.org/10.30534/ijacst/2020/01942020

# Improved Session Based Password Security System

**Dr M Surya Bhupal Rao [1], Dr V S Giridhar Akula[2]**
[1]R G M College of Engineering and Technology, India, suryabhupal@gmail.com
[2]Princeton Institute of Engineering & Technology for Women,India,seshagiridhar.a@gmail.com

## ABSTRACT

Traditionally people use textual passwords as a security but these passwords get affected to the various attacks like dictionary attack, shoulder surfing, etc. After the period, graphical passwords are coming to the existence but the graphical passwords have some own disadvantages such as they require more time to authenticate. Hence, This paper has taken a review of session password technique in which the password is used only once for each and when session will end the password is not useful. The proposed session password scheme uses Text session password. The session password scheme uses pair-based authentication scheme. Textual passwords generally used for login authentication. Graphical password is introduced exactly opposite technique to textual passwords. As most users are well known about textual passwords than pure graphical passwords. Shoulder-surfing is an attack where an attacker can capture a password by direct show or by listening the authentication session password. Session password can use only once because every time a new password will generate. Session Password supports Pair based scheme which is secure and more efficient. In this paper, it is proposed an improved text-based shoulder surfing resistant scheme by using pair based scheme is used for alphabet, digit , symbols where session password will form at every session or transaction using virtual shuffling keyboard. The user can easily and efficiently login to the system. Proposed system analyzes the security and usability of the proposed scheme, and shows the support of the scheme to shoulder surfing attack.

**Key words:** Pair based scheme, Secret Key, Shoulder-Surfing Attack, Virtual Keyboard.

## 1. INTRODUCTION

Internet usage in the present day scenario is more abundant. Today for authentication, user name and password is used basically, hence the security must be provided in order to prevent hackers from accessing the data present in account of particulars. Phishing is a type of attack in which the attacker attempts to acquire the person's information such as user-id, password, pin no, etc. by showing the user to believe that he is communicating with a trustworthy person . The users would normally receive a phishing email with a link and if user clicked that link, it will take them to a fake web site which could add malicious programs into the user's compute. Sometimes a phishing email can ask the users to provide their account details to carry verification purpose. So, it is necessary that the authentication should secure to protect user accounts.

The common technique used for authentication is textual password technique. The vulnerabilities of this type of technique is dictionary attack, social engineering and shoulder surfing attack, A Dictionary Attack is a technique for defeating with authentication mechanism by trying to determine or generate its decryption key to enter into once account. It is such method in which there is breaking to a password protected system by systematic manner by entering every word in a dictionary as password and in Shoulder Surfing, the hacker tries to look over persons shoulder to catch password .This is an attack in which an observer try to watch the keyboard entries to learn password characters entered by the user. Shoulder surfing could be carried out in a number of ways. As the keyboard is openly displayed on the screen of computer, it makes very easy to observe the key entered by person. Shoulder surfing is possible by watching the keyboard entry from some distance or by recording complete process through CCTV camera or by taking screen shots of keys pressed by person. The shoulder surfing attack mainly happened at public places or on public systems because login process can be monitored by many people and system is not completely in user control. It is observed that graphical passwords are predictable, a serious problem specifically related with text- based password. To avoid the problem of password stealing when logging by keyboard, several password based sites like banks sites provide a virtual keyboard option to enter passwords. It is an on-screen keyboard that helps users to enter their passwords by mouse click, which avoids the use of keyboard. But, it is not compulsory to users to use virtual keyboard. It is simple to see onscreen password entry than the entry by a normal keyboard. Particularly when online banking operations are performed at public places like Internet cafe, computer centers at colleges, etc.

Specifically, graphical passwords are introduced as a substitute to the textual passwords technique. Graphical

passwords are easy to remember than textual passwords. Also it is difficult to formulate automated attack on graphical passwords. But, most of the existing graphical password authentication techniques are suffering through shoulder-surfing attack, a known attack where an observer catches the password by recording the session of authentication or by direct surveillance. Also, Graphical password Authentication is more costly than the textual passwords.

There are many drawbacks associated with the textual passwords such as brute-force and dictionary attacks. Similarly, graphical passwords can affected by shoulder-surfing attack and it is expensive to implement. For this purpose, the use of both the textual and graphical password techniques is better. This paper proposed, authentication technique called as pair-based authentication scheme for generating the session passwords.

In this paper, session based authentication scheme is proposed. This scheme authenticates the user by session passwords by using pair based scheme. Session passwords are passwords that are used for only one transaction. Once the session is terminated, the session password is not useful. For every login process, users have to enter different passwords. The session passwords provide better security against shoulder surfing attack as password changes according to each transaction.

## 2. RELATED WORK

Dhamija and Perrig proposed a graphical authentication technique , where the user has to select some images from a set of random pictures when user is going to register and then at the time of login user must have to select the same sequence of images which he has pre-defined at the time of registration. But this technique is vulnerable to shoulder surfing attack. The advantage of this technique is that, though the average time taken to login to the system is much longer than that of the regular approach, it has very low rate of failure.

Real User Corporation has developed Pass face technique , where the user observes nine faces grid display and have to select one face previously chosen by the user. Then, user recognizes it and clicks anywhere on the known face. Same procedure is repeated for several round of time. In this technique, the user chooses four human face images as the password and from eight decoy images, user has to select their pass images. As user has selected four images it is followed for complete four times.

Again one approach is proposed which is named as colour keyboard implementation , where alphabets and numbers of keyboard are given with different colours. After the user click, all keys on the keyboard shuffles every time. Here, user has to note down particular position of key before pressing desired key. Then a button named 'Hide Keys' have to be pressed, which will hide all characters from the keys and empty keys will be displayed before user. Then user has to click on that key which has the desired key earlier. For which the user can make use of key colour for remembering it.

Another approach , is based on tracking user's eye movement for determination of the shape to be conceived based on the movements. As finally the shape which is constructed is compared with the shape present in the database to perform authentication. But, in this way shows many drawbacks. A new technique called "Draw-a-Secret" (DAS) is proposed by Jermyn.et al., where the user have to re-draw the predefined picture on a2D grid. Authentication is possible only when drawing will touch the same grids in particular same sequence. This technique of authentication is vulnerable to shoulder surfing attack. Another technique , in which user has to draw signature by using mouse, this technique is developed by Syukri. It has two stages such as initially registration and then verification. When user is registering, user must draw his signature and then afterwards user will be verified only by matching the previous defined signature. The disadvantage of this technique is that, many of people are not so much familiar with handling mouse properly; hence it may be difficult to draw the signature in same perimeter.

Haichang et al proposed new scheme, where the user have to draw a curve across their password images orderly, here user do not have to click on images which is predefined as his passwords. For mobile devices, Jansen proposed a graphical password scheme. When user is creating password, he must select a theme consist of photos and set a sequence of pictures as his password. When authenticating, user must recognize the images in the same order. Every image is assigned with numerical value, thus the sequence of the chosen images will create a password. But the number of images is limited to 30, the password space is small. All above Systems were defined just for security but all they had some disadvantages and they can be easily cracked by different techniques. According to Syukri, the accuracy of the original user is also very important, otherwise system may show original user as a fake user, because drawing the signature by using mouse is very difficult and the possibility of showing Difference in signature. So after studying all previous related works, it motivates us to work on system for security of user login information and authentication.

## 3. PROPOSED WORK

The general technique which is used earlier is a Textual password technique which has its own drawbacks. The new technique is proposed which is called as biometric system. This graphical password technique avoid shoulder surfing attack in Textual passwords but this technique also followed by some limitations and disadvantages like time consuming for Authentication and expensive in nature. So, we proposed new password authentication technique is Session password using virtual keyboard. In which new scheme is used which is

called as Pair-based Authentication scheme. It gives options for user to select the password as alphanumerical grid.

In this paper, the main objective is to avoid shoulder surfing attack using pair based scheme which will generate session password for the particular session or transaction where there will be virtual keyboard which will shuffle at every another transaction accordingly. At the time of registration user have to submit password. Particularly the length of the password is 8 and it can be named as secret key. The secret key consists of even or odd number of characters. Then next stage is the login phase, when the user enters his username as an interface, the 6 x 6 grid display of row and column size screened before user. The grid display consists of alphabets and numbers. These are sequentially placed on the grid at every cell and this interface changes every time according to every transaction. According to pair based scheme, user have taken first letter from his registered password as row wise and second letter as column wise and then the intersection which will form will be the part of session password.. As each and every time the keyboard will shuffle, the session password will also change and hence automatically security is getting to login.


**Figure 1**: 6x6 Grid Display

In the proposed scheme, when new user want to register, then new user can register by filling the data such as username, his E- mail address, birth date, gender, local address, city, mobile number first name, last name etc. In textual password scheme passwords should be easy to remember and then easy to cracked. But, in pair-based scheme, the password guessing is not easy. So it tends to security. Also, this technique is easy to use to the user. Suppose the password of user is ARCHIT then at the time of login, 6 X 6 grid display on the screen will be place and have to select first row having A and select alphabet having R and then where they intersect click on W .In same way, take all the letters in pair and find intersect and click on the respective intersect sequentially. If the password is correct, the user will enter into the system. The grid size can be increased to include alphabet and digits in the Password.

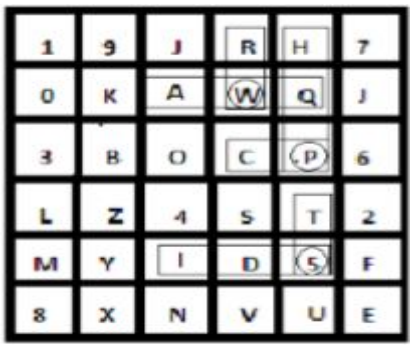


**Figure 2**: Pair Based Scheme

The session password of this process will be WP5. Hence according to Pair based scheme, there is resistant to the shoulder surfing attack, and because the registered password like ARCHIT is not necessary to enter at the time of login, as at every transaction there should be new session password as there is virtual shuffling keyboard. After this transaction the virtual keyboard will shuffle and hence there will be new session password for every transaction.

## 4. ADVANTAGES

1. More Complexity to hack: This technique has session password scheme due to what every transaction is performed with other session password, hence hacking to the user account is very hard.
2. Shuffling of keyboard: Due to this facility of shuffling keyboard, there should be new session password at every transaction and hence less chances of shoulder surfing attack.
3. More Secured: In pair-based scheme password guessing is not easy to do. So it is more secure.

## 5. CONCLUSION

There are many techniques which are proposed for preventing shoulder surfing attack. Among all proposed techniques the session based password scheme using shuffling keyboard with Pair Based method is more effective and secure to shoulder surfing attack, as this technique is providing a particular session password for every session or transaction Also, it is easy to use and handle, hence in near future , this technique has scope to use in many fields for the security purpose.

## REFERENCES

1. Sanket Prabhu and Vaibhav Shah. **Authentication Using Session based Password**, *International Conference on Advanced Computing Technologies and Applications*, Procedia Computer Science, pp 460-464,2015. https://doi.org/10.1016/j.procs.2015.03.079
2. N. S. Joshi. **Session Passwords Using Grids and colors for Web applications and PDA**, *International Journal of Emerging Technologyand Advanced Engineering*, vol. 3, May 2013.

3. R .Dhamija and A. Perrig. **A User Study Using Images for Authentication**, *Proceedings of the 9th USENIX Security Symposium, Vol 9, August 2000*
4. Agarwal M et al. **Secure authentication using dynamic virtual keyboard layout,** *Proceedings of the International Conference and Workshop on Emerging Trends in Technology, pp 288-291ACM.*