Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 6, June -2017

PassMatrix: Graphical Based Authentication System for Shoulder Surfing Attack Resistant

Priyanka Karale[1],Snehal Shinde[2], Ashwini Sandbhor[3], Vaishnavi Ramekar[4]
Prof. Deepak Gupta[5]

[1,2,3,4,5] *Department of Computer Engineering, Siddhant College of Engineering, Pune*

Abstract — *The authentication based on the passwords is used mostly in applications for the computer security and privacy. However, the human actions such as selecting less secured passwords credentials and inputting passwords in an insecure way are considered "the weakest link" within the authentication chain. Instead of arbitrary alphanumeric strings, users tend to select passwords either short or purposeful for simple memorization. With internet applications and mobile apps pile up, individuals will access these applications anywhere and anytime with different devices. This evolution brings good convenience however it will increases the probability of exposing passwords credentials to shoulder surfing attacks. Attackers will observe directly or use external recording devices to get users' credentials. To overcome this issue, proposed a novel authentication system named PassMatrix, which is based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and change of location horizontal and vertical bars covering the complete scope of pass-images, PassMatrix offers no hint for attackers to work out or narrow down the password even they conduct multiple camera-based attacks. Implemented a PassMatrix prototype on web applications and allotted real user experiments to describee its memorability and usefulness. From the experimental result, is shown that, the proposed system achieves better resistance to shoulder surfing attacks whereas maintaining usability.*

Keywords- *Graphical Passwords, Authentication, Shoulder Surfing Attack..*

I. INTRODUCTION

Shoulder surfing technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, by helping attackers to gain access to the system. Key logging is the practice of noting the keys struck on keyboard, typically in manner so that person using the system keyboard is unaware that such action is monitored. There are two types of key loggers viz. software key logger and hardware key logger. Software key logger is installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. Textual passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- case and lower-case Alphabets, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect . Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is not a rare case that users may use only one username and password for multiple accounts . According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds . Textual passwords are often insecure due to the difficulty of maintaining strong ones. Various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in, humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information. The human actions such as choosing wrong passwords for new accounts and entering passwords in an not secure way for later logins are regarded as the weakest link in the authentication chain . Therefore, an authentication scheme should be designed to overcome these vulnerabilities. In this project, we purposed a secure graphical authentication system named Pass Matrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of onetime login indicators. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly. The shoulder surfing attack in an attack that can be performed by the adversary to obtain the user's password by watching over the user's shoulder as he enters his password. As conventional password schemes are vulnerable to shoulder surfing, Sobrado and Birget proposed three shoulder surfing resistant graphical password schemes. Since then, many graphical password schemes with different degrees of resistance to shoulder surfing have been proposed, and each has its pros and cons. Seeing that most users are more familiar with

textual passwords than pure graphical passwords, Zhao et al. proposed a text-based shoulder surfing resistant graphical password scheme,S3APS. InS3PAS, 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,e.g.,Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this paper, we will propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to login the system without using any physical keyboard or on-screen keyboard.

II. RELATED WORK

A Graphical Password schemes resistant to shoulder surfing. In this scheme the user draws a curve across the selected images in the same order that he had selected during registration. The image grid contains decoy images to resist shoulder surfing. the user has to draw some pattern as password and a scanner scans that pattern and registers Automatically. There are two software's, one of them guides for the user while drawing and the other does registration process the approach is based on the capacity of users to recognize the well-known faces. An image grid with three human faces in each row is displayed. The user has to specify the number of human faces that he knows is Even or Odd. each user is given a different set of images, from which he has to select two images. The image set is based on some calculation which involves the position of characters in alphabets. Describes two approaches. One is the pair based authentication. Here the user has to select 8 pair of images. He has to match the images with its pair during authentication as well. The other approach is text based image authentication. In this a set of images are selected by the user and a character is assigned to each image. During authentication images are displayed. the user has to select 4 single digit numbers as password and place them in a grid with 16 positions. During authentication grid with 16 positions containing numbers from 0-9 is displayed at random positions is displayed. User finds all original pass-characters that were selected and clicks inside invisible triangles created by characters. Different session characters are entered that are chosen from inside or on the border of pass-triangles formed in previous step. Implementation of coloured keyboards is proposed. Every characters and alphabets are shuffled every time after the user clicks on the key. Before clicking on the key the user has to note down the position of the key, then he has to press a button caption "Hide Keys", which will hide the characters. If the user clicks on the correct position of alphabets then he will be given access.

III. PROPOSED SYSTEM

In PassMatrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the PassPoints scheme. Based on the user study of Cued Click Points. However, aiming at alleviating shoulder surfing attacks, we do not recommend this approach since the feedback that is given to users might also be obtained by attackers. Due to the fact that people do not register a new account or set up a new screen lock frequently, we assume that these setup events can be done in a safe environment rather than in public places. Thus, users can pick up passsquares by simple touching at or clicking on them during the registration phase.

IV. SYSTEM ARCHITECTURE

1. Image Discretization Module. This module divides each image into squares, from which users would choose one as the pass-square. As shown in Figure 5, an image is divided into a 7 * 11 grid. The smaller the image is discretized, the larger the password space is. However, the overly concentrated division may result in recognition problem of specific objects and increase the difficulty of user interface operations on palm-sized mobile devices.

2.Login Indicator Generator Module. This module generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual materials (such as colors and icons) for users during the authentication phase. In our implementation, we used characters A to G and 1 to 11 for a 7 * 11 grid. Both letters and numbers are generated randomly and therefore a different login indicator will be provided each time the module is called. The generated login indicator can be given to users visually or acoustically in our system we are sending this patterns on users email.

3. Horizontal and Vertical Axis Control Module. There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers.

4. Communication Module. This module is in charge of all the information transmitted between the client devices and the authentication server. Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe from being eavesdropped and intercepted.

5. Password Verification Module. This module verifies the user password during the authentication phase. A pass Horizontal scroll bar (on the right/blue) and vertical bar (on the left/green). square acts similar to a password digit in the

text-based password system. The user is authenticated only if each pass-square in each pass-image is correctly aligned with the login indicator.

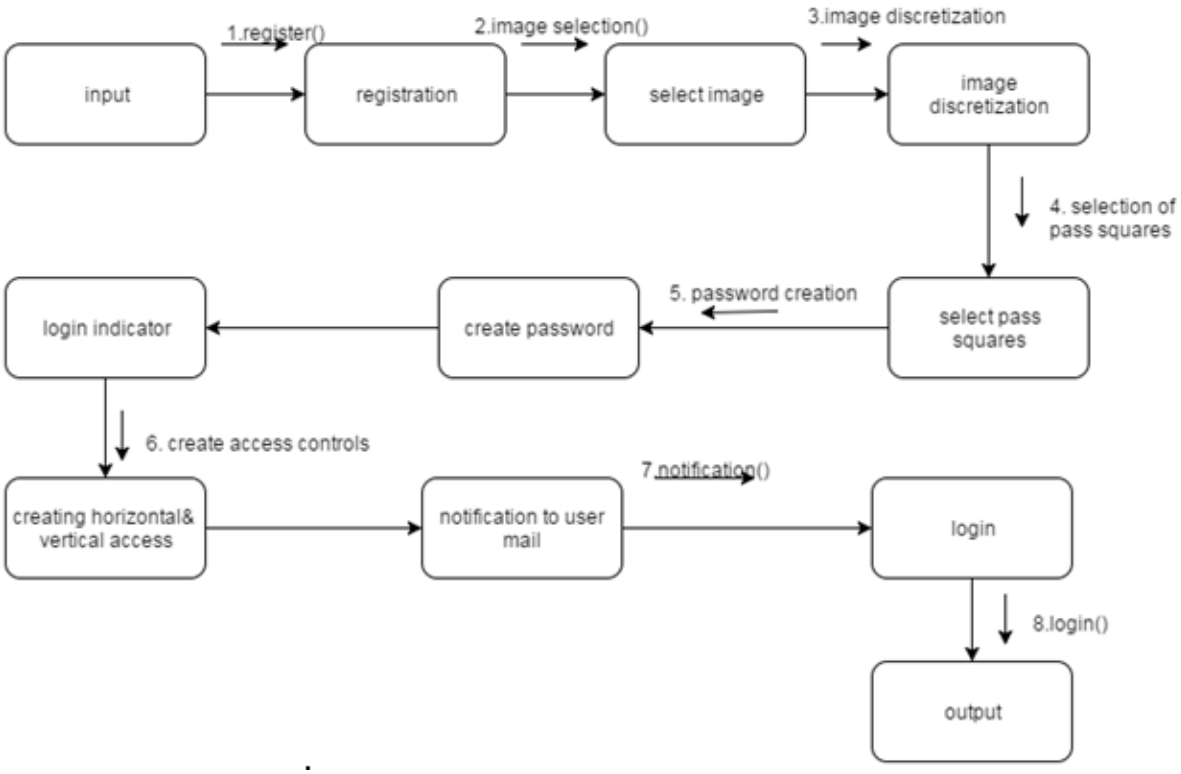


Fig.1 System Architecture

METHODOLOG OF PROPOSED SYSTEM

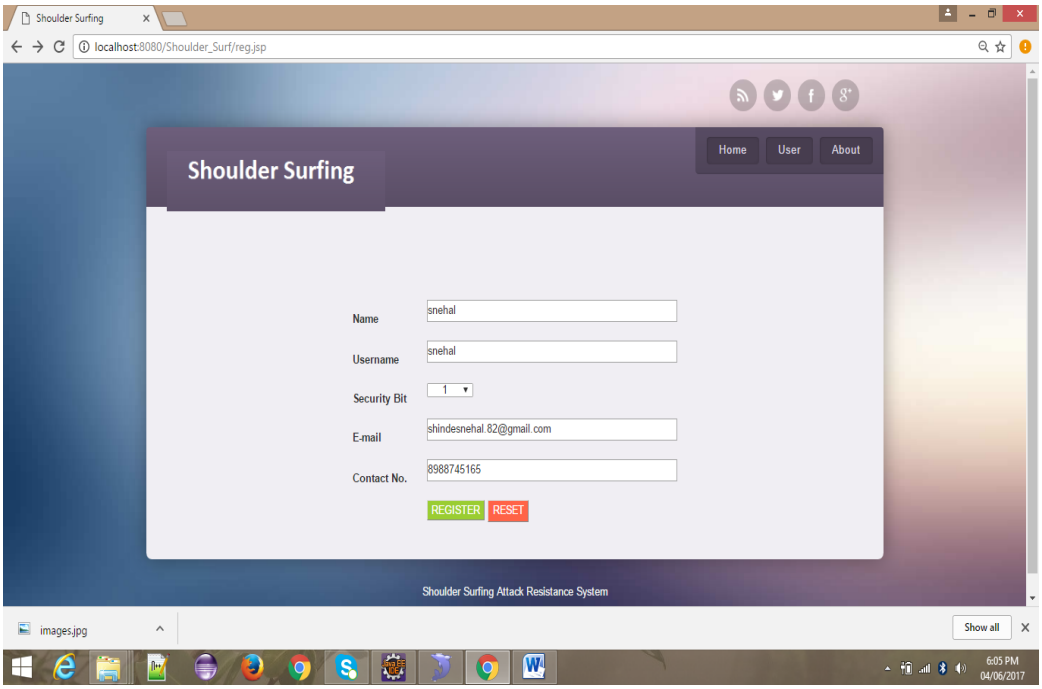
1. Registration phase The user creates an account which contains a username and a password. The password consists of only one pass-square per image for a sequence of n images. The number of images (i.e., n) is decided by the user after considering the trade-off between security and usability of the system. The only purpose of the username is to give the user an imagination of having a personal account. The username can be omitted if PassMatrix is applied to authentication systems like screen lock. The user can either choose images from a provided list or upload images from their device as pass-images. Then the user will pick a passsquare for each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set.

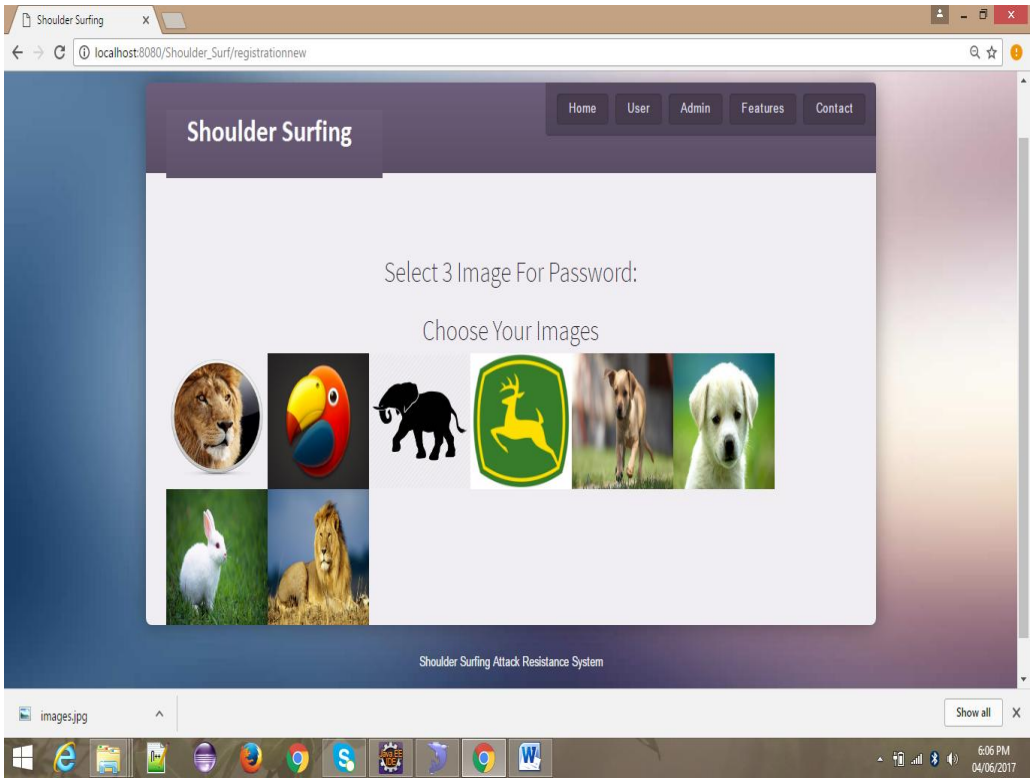
2 Authentication phase The user uses his/her username, password and login indicators to log into PassMatrix. The following describes all the steps in detail:

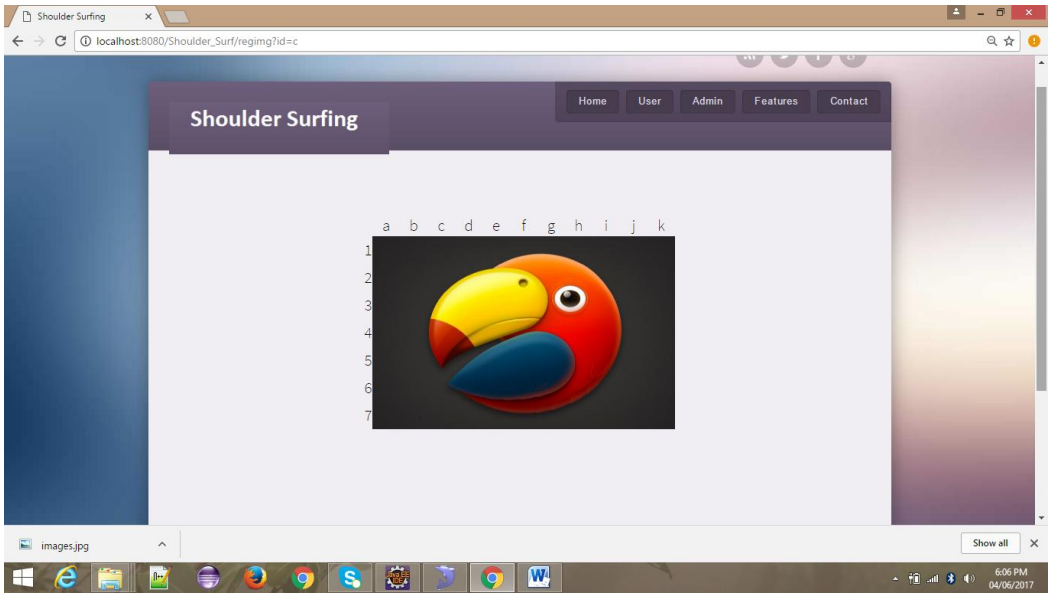
1) The user inputs his/her username which was created in the registration phase.
2) A new indicator comprised of a letter and a number is created by the login indicator generator module. The indicator will be shown when the user uses his/her hand to form a circle and then touch the screen. In this case, the indicator is conveyed to the user by visual feedback. The indicator can be delivered to user by email.
3) Next, the first pass-image will be shown on the display, with a horizontal bar and a vertical bar on its top and left respectively. To respond to the challenge, the user flings or drags the bars to align the pre-selected pass-square of the image with the login indicator. For example, if the indicator is (E, 11) and the pass-square is at (5, 7) in the grid of the image, the user shifts the character ‖E‖ to the 5th column on the horizontal bar and ‖11‖ to the 7th row on the vertical bar
4) Repeat step 2 and step 3 for each pre-selected passimage.
5) The communication module gets user account information from the server through HttpRequest POST method.

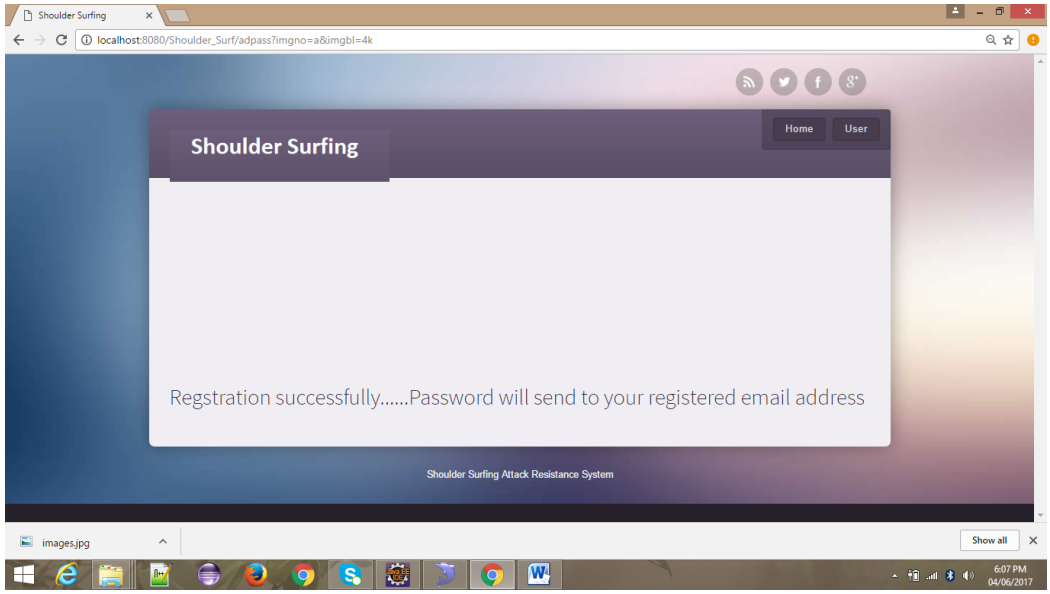
6) Finally, for each image, the password verification module verifies the alignment between the passsquare and the login indicator. Only if all the alignments are correct in all images, the user is allowed to log into PassMatrix.

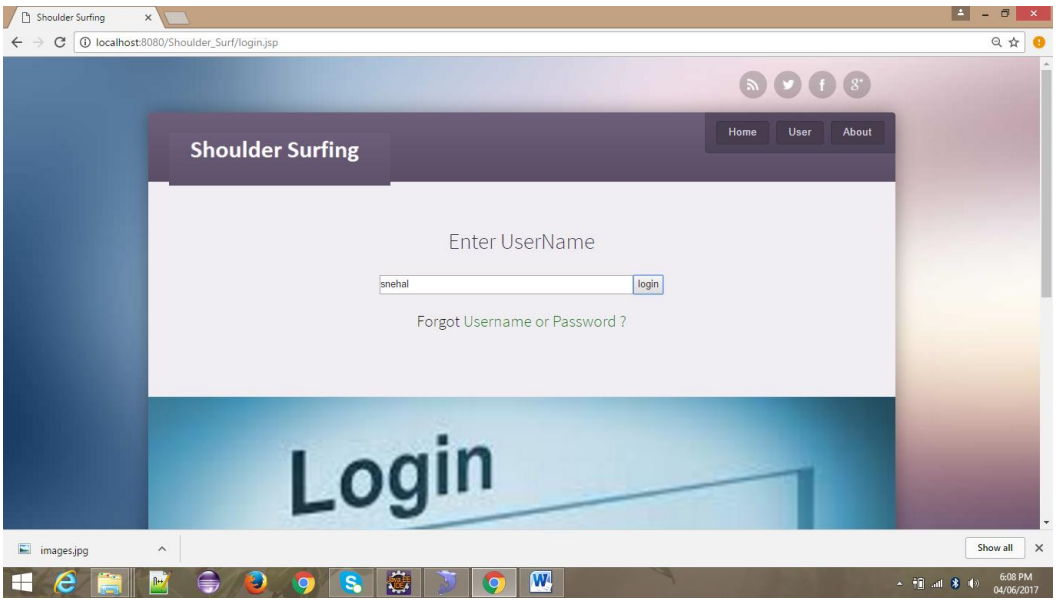
V. Snapshots

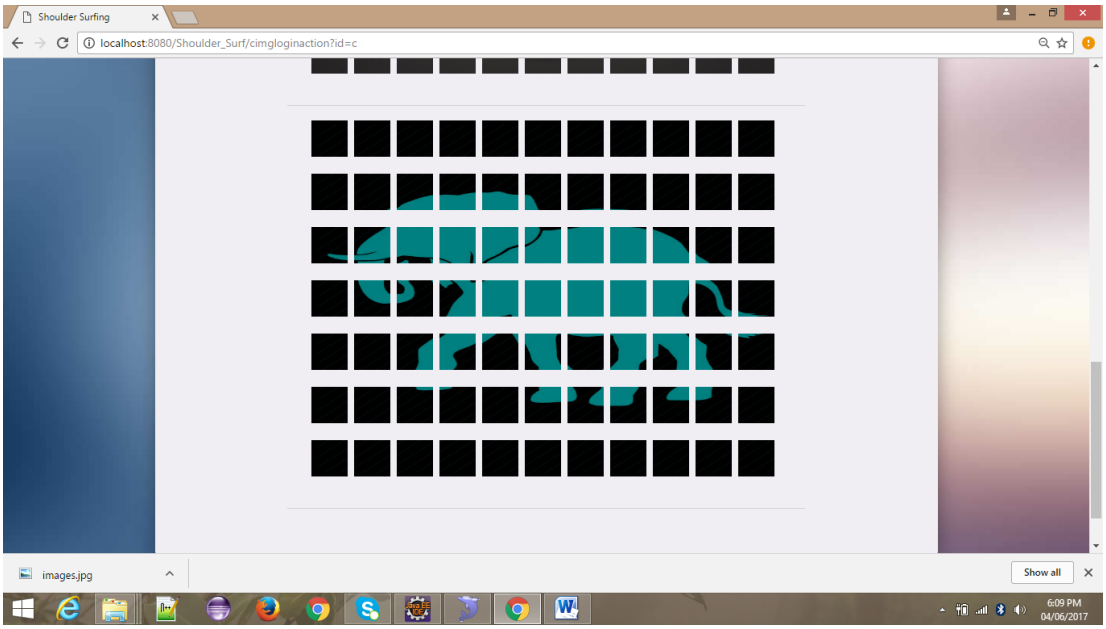


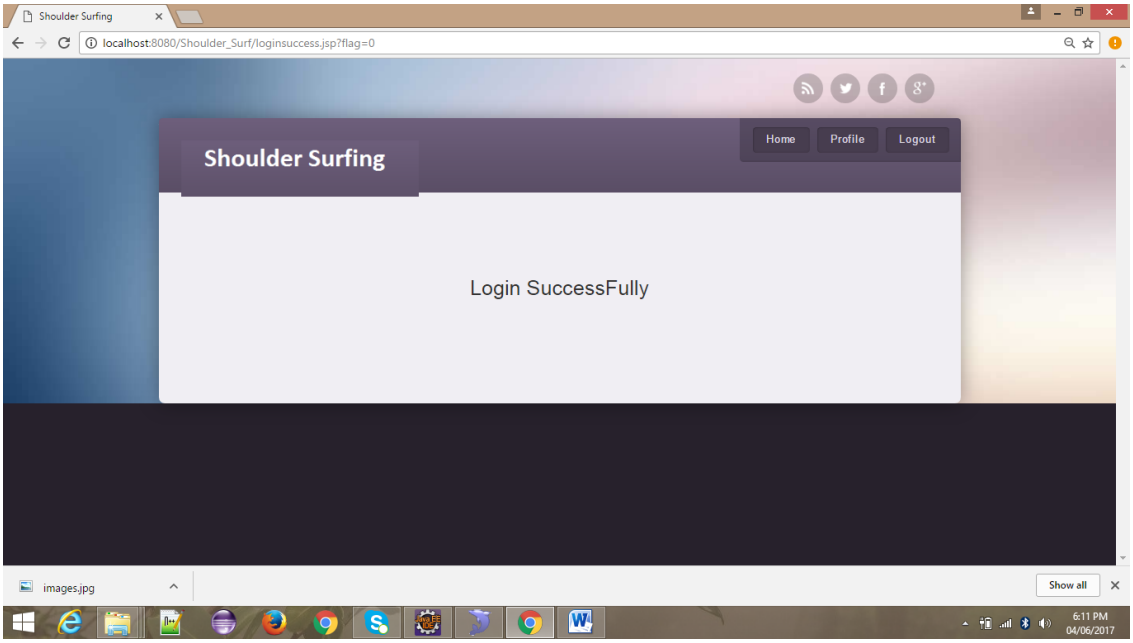












VI. Conclusion and Future Work

We present a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of the one-time login indicators. The login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic selection to figure out the location of their passwords rather than clicking on the password object directly.

VII. ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

VIII. REFERANCES

[1] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical Authentication System", IEEE Transactions on Dependable and Secure Computing, 2016.

[2] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in Proceedings of the 3rd symposium on Usable privacy and security. ACM, 2007, pp. 13–19.

[3] H. Zhao and X. Li, "S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, vol. 2. IEEE, 2007,pp. 467–472.

[4]S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.

[5] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[6] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, 2005. R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[7] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

[8] A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.

[9] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485–497, 1977.

[10] A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron, and M. Fischer, "Vip: a visual approach to user authentication," in Proceedings of the Working Conference on Advanced Visual Interfaces. ACM, 2002, pp. 316–323.

