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 10, October -2017

# Picture Based System To Resist Surfing Attack Over Web

Vilas Babar[1], Rakesh Chavan[2], Nakul Mapari[3], Prof. Rupali Nirgude[4]

[1,2,3,4]*Computer Engineering, Dr. D.Y. Patil Institute of Engineering & Technology*

**Abstract** — *Verification in view of passwords is utilized to a great extent in applications for PC security and protection. Be that as it may, human activities, for example, picking awful passwords and contributing passwords in a shaky way are viewed as quote the weakest connection quote in the verification chain. As opposed to discretionary alphanumeric strings, clients have a tendency to pick passwords either short or significant for simple remembrance. With web applications and versatile applications heaping up, individuals can get to these applications whenever and anyplace with different gadgets. This development brings extraordinary accommodation additionally expands the likelihood of presenting passwords to bear surfing assaults.*

*Assailants can watch specifically or utilize outside recording gadgets to gather client's qualifications. To defeat this issue, we proposed a novel verification framework PassMatrix, in light of graphical passwords to oppose bear surfing assaults. With a one-time legitimate login marker and circulate level and vertical bars covering the whole extent of pass-pictures, PassMatrix offers no indication for aggressors to make sense of or limit the secret word even they lead different camera-based assaults. We likewise executed a PassMatrix model on Android and completed genuine client tests to assess its memorability and ease of use. From the trial result, the proposed framework accomplishes better imperviousness to bear surfing assaults while looking after ease of use.*

***Keywords***- *Graphical Passwords, Authentication, Shoulder Surfing Attack, PassMatrix, Security and protection.*

## I. INTRODUCTION

Textual passwords have been the most generally utilized validation technique for a considerable length of time. Included numbers and upper-and lower-case letters, printed passwords are viewed as sufficiently solid to oppose against animal power assaults. Be that as it may, a solid printed secret word is difficult to retain and remember. In this way, clients have a tendency to pick passwords that are either short or from the word reference, as opposed to arbitrary alphanumeric strings. Much more terrible, it is not an uncommon case that clients may utilize just a single username and secret key for different records According to an article in Computer world, a security group at a substantial organization ran a system watchword saltine and shockingly broke around 80% of the representatives' passwords inside 30 seconds. Printed passwords are frequently unreliable because of the trouble of keeping up solid ones.

Different graphical secret word confirmation plans were produced to address the issues and shortcomings related with literary passwords. In view of a few investigations, for example, those in people have a superior capacity to remember pictures with long haul memory (LTM) than verbal portrayals. Picture based passwords were ended up being less demanding to remember in a few clients contemplates. Therefore, clients can set up a complex confirmation secret key and are fit for remembering it after quite a while regardless of the possibility that the memory is not actuated occasionally. Be that as it may, the greater part of these picture based passwords is powerless against bear surfing assaults (SSAs).

This kind of assault either utilizes coordinate perception, for example, viewing behind someone or applies video catching methods to get passwords, PINs, or other delicate individual data. The human activities, for example, picking awful passwords for new records and contributing passwords in an unreliable path for later logins are viewed as the weakest connection in the verification chain. In this way, a validation plan ought to be intended to beat these vulnerabilities. In this paper, we introduce a safe graphical validation framework named PassMatrix that shields clients from getting to be casualties of shoulder surfing assaults while contributing passwords in broad daylight through the use of one-time login markers. A login pointer is haphazardly produced for each pass-picture and will be futile after the session ends. The login marker gives better security against bear surfing assaults, since clients utilize a dynamic pointer to call attention to the position of their passwords instead of tapping on the watchword question straightforwardly.

## II. LITERATURE SURVEY

We proposed a shoulder surfing resistant authentication system based on graphical passwords, named PassMatrix. Using a one-time login indicator per image, users can point out the location of their pass-square without directly clicking or touching it, which is an action vulnerable to shoulder surfing attacks. Because of the design of the horizontal and vertical bars that cover the entire pass-image, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account. [1] In this paper, we shall present the result of our survey through all currently available password authentication related scheme. In this study, we have surveyed all currently available password authentication schemes and analyses how they work over insecure networks.is and get them classified in terms

 

of several crucial criteria. [2] Thus, graphical password authentication can be given by taking cloud as a platform. The new scheme provides solves the many problems of existing system. It can also be useful for user in security point of view. In this paper we are representing the authentication given to cloud by using graphical password. We have proposed cloud with graphical security by means of image password. [3] Present secure systems suffer because they neglect the importance of human factors in security. We address a fundamental weakness of knowledge - based authentication schemes, which is the human limitation to remember the secure passwords. Our methodology to improve the security of these systems relies on recognition - based, rather than recall - based authentication. We examine the requirements of recognition - based authentication system and propose Deja Vu, which authenticates a user through her ability to recognize previously seen images. [4] In this paper we describe Pass-Points, a new and more secure graphical password system. We report an empirical study comparing the use of PassPoints to alphanumeric passwords. Participants created and practiced either an alphanumeric or graphical password. In the longitudinal trials the two groups performed similarly on memory of their password, but the graphical group took more time to input a password. [5] We present a number of design choices and discuss their effect on usability and security. We conducted user studies to evaluate the speed, accuracy and user acceptance of our approach. Our results demonstrate that gaze-based password entry requires marginal additional time over using a keyboard, error rates are similar to those of using a keyboard and subjects preferred the gaze-based password entry approach over traditional methods. [6]

## III. SYSTEM IMPLEMENTATION

In this System, we are using PassMatrix, Graphical user password Instead of using text password to secure the confidential data and online banking system. In this system, User will set his/her own image and can set the points. So, whenever user is doing online shopping, or using recommendation system, at that time they will be asked for graphical password PassMatrix which were previously settled by users. The image PassMatrix can be verified with database, and if the points are correct the transaction will be successful or it will fail. This is the highly secured system to protect the confidential data.

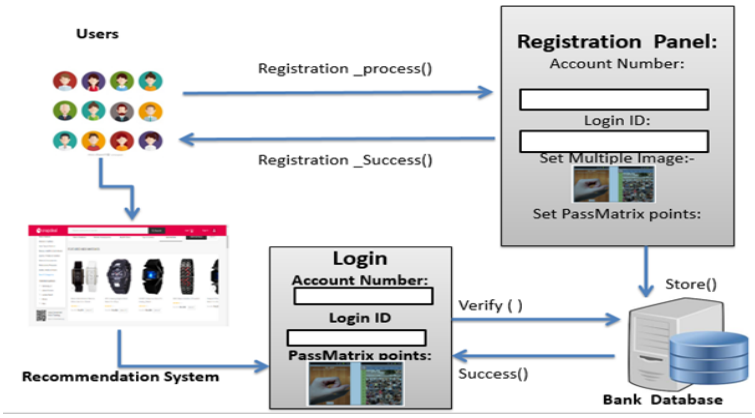


***Figure 1. System Architecture***

### 3.1 PASSMATRIX

To beat the security shortcoming of the conventional PIN technique, the effectiveness of getting passwords by onlookers out in the open, and the similarity issues to gadgets, we presented a graphical verification framework called PassMatrix. In PassMatrix, a watchword comprises of just a single pass-square per pass-picture for an arrangement of n pictures. The quantity of pictures (i.e., n) is client characterized. Figure exhibits the proposed plot, in which the primary pass-square is situated at in the principal picture, the second pass-square is on the highest point of the smoke in the second picture at and the last pass-square is at in the third picture. In PassMatrix, clients pick one square for each picture for a succession of n pictures as opposed to n squares in one picture as that in the Pass Points plot. In light of the client investigation of Cued Click Points (CCP) proposed by Caisson et al., Fig. A secret word contains three pictures (n=3) with a pass square in each. The pass squares are appeared as the orange-filled range in each picture. The CCP technique makes a decent showing with regards to in helping clients recall and recollect their passwords. In the event that the client taps on a mistaken area inside the picture, an alternate picture will be appeared to give the client a notice criticism. In any case, going for easing shoulder surfing assaults, we don't prescribe this approach since the input that is given to clients may likewise be gotten by aggressors. Because of the way that individuals don't enlist another record or set up another screen bolt every now and again, we accept that these setup occasions should be possible in a protected situation instead of in broad daylight places. Along these lines, clients can get pass-squares by essentially touching at or tapping on them amid the enlistment stage.

 

**3.2 Overview**

PassMatrix is composed of the following components (see Figure2):

- Image Discretization Module
- Horizontal and Vertical Axis Control Module
- Login Indicator Generator Module
- Communication Module
- Password Verification Module
- Database

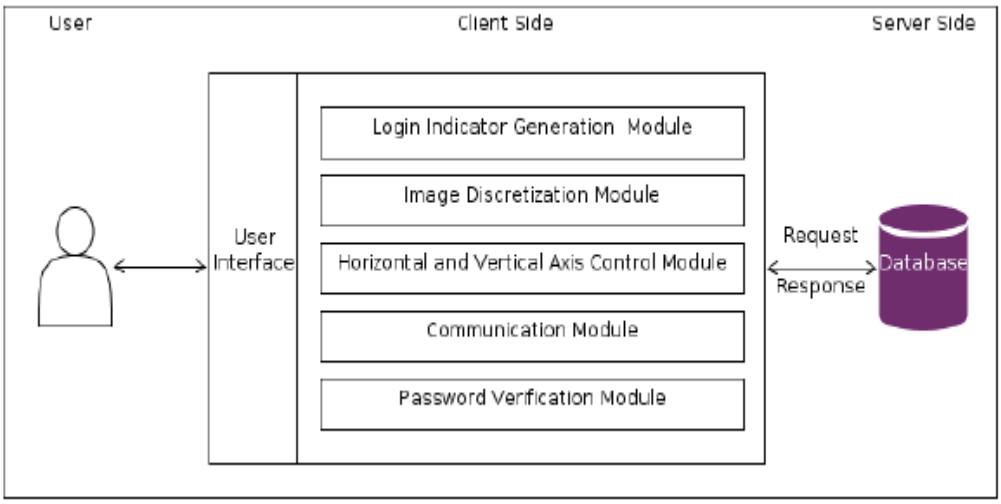


***Figure 2. Overview of the PassMatrix system***

**3.3 Image Discretization Module.**

This module isolates each picture into squares, from which clients would pick one as the pass-square. As appeared in Figure 2, a picture is isolated into a network. The littler the picture is discretized, the bigger the secret key space is. In any case, the excessively focused division may bring about acknowledgment issue of particular questions and increment the trouble of UI operations on palm-sized cell phones. Henceforth, in our usage, a division was set at 60-pixel interims in both even and vertical headings, since 60 pixels2 is the best size to precisely choose particular questions on touch screens.

**a) Shoulder Surfing Attack**

Due to the fact that shoulder surfing has been a real threat to authentication systems with either textual or graphical passwords, many novel authentication schemes were proposed to protect systems from this attack. Unfortunately, most of them were unsuccessful to alleviate the threat if the shoulder-surfing attack is camera-based. For instance, some schemes such as PIN-entry method and spy resistant keyboard were designed based on the difficulties of short-term memory. Camera-based shoulder surfing attacks can easily crack the passwords of these schemes. The password spaces of other schemes such as those in CAPTCHA-based method, Pass-icons and Colorings can be narrowed down by camera-based shoulder surfing attacks.

The proposed authentication system PassMatrix takes full advantage of adding extra information to obfuscate the login process, using an approach to point out the locations of pass-squares implicitly instead of typing or clicking on password objects directly. Since the horizontal and vertical bars are circulate and thus cover the entire area of the image, the password space will not be narrowed down even if the whole authentication process is recorded by attackers. Furthermore, the login indicator for each pass-image varies so that each pass-image is an independent case. Thus, no pattern can be extracted from a set of pass-images in an authentication trial, neither from multiple login processes. With the above security features, PassMatrix should be strong enough to resist shoulder surfing attacks, even if the attacks are camera-equipped.

**3.4 Smudge Attack**

A smudge attack is an implicit attack where attackers attempt to extract sensitive information from recent users 'input by inspecting smudges left on touch screens. Since both the horizontal and vertical bars in PassMatrix are scrollable, shifting on any element within the bar can circulate the whole bar. Thus, users do not have to shift the bars by touching the login indicators. The smudge left by users may be quite fixed, but it only indicates the habitual stretching range of the thumb or finger. The length of the smudge left on the screen also provides no useful information since the login indicator is generated randomly for each pass-image and the permutations of elements on both bars are also randomly re-arranged in each pass-image and in each login session. Therefore, the proposed PassMatrix is immune from smudge attacks.

 

## IV. CONCLUSION

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. In order to protect users' digital property, authentication is required every time they try to access their personal account and data. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Even a complicated password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves.

## V. ACKNOWLEDGMENT

Working on this project on "Image Based System To Resist Surfing Attack Over Web" was a source of immense knowledge to me. We would like to express my sincere gratitude to Prof. Rupali Nirgude for his guidance and valuable support thought out the course of this project work. We acknowledge with a deep sense of gratitude, the encouragement and inspiration received from our faculty members and colleagues. We would also like to thank our parents for their love and support.

## REFERENCES

[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 (Volume:PP , Issue: 99 ),09 March 2016

[2] 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. 17.

[3] 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. 479483.

[4] 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. 44.

[5] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, The design and analysis of graphical passwords, in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 11.

[6] 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. 102127, 2005.

[7] 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. 316323.

[8] B. Ives, K. Walsh, and H. Schneider, The domino effect of password reuse, Communications of the ACM, vol. 47, no. 4, pp. 7578, 2004.

[9] J. Long and K. Mitnick, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Elsevier Science, 2011.

[10] T. Kwon, S. Shin, and S. Na, Covert attentional shoulder surfing: Human adversaries are more powerful than expected, IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6, pp. 716727, June 2014.

[11] Google glass snoopers can steal your passcode with a glance, http://www.wired.com/2014/06/google-glass-snoopers-cansteal- your-passcode-witha- glance/.

 