A Novel Approach of Graphical Authentication System Using Pass Matrix.

B.Swetha[1],Dr.B.Geetha Vani[2]
M.Tech(CSE)[1], Professor[2]
Department of Computer Science and Engineering
Narayana Engineering College
(Affiliated to JNTUniversity, Ananthapuram)
Nellore
Andhra Pradesh-India.

Abstract: Authentication in light of passwords is used, all things considered, in applications for computer security and assurance. Nevertheless, human exercises, for instance, picking horrendous passwords and contributing passwords in an untrustworthy way are seen as "the weakest association" in the authentication chain. Rather than arbitrary alphanumeric strings, customers tend to pick passwords either short or vital for basic maintenance. With web applications and adaptable applications stacking up, people can get to these applications at whatever point and wherever with various contraptions. This improvement brings amazing convenience yet moreover assembles the probability of exhibiting passwords to shoulder surfing strikes. Aggressors can observe clearly or use external narrative devices to assemble customers' capabilities. To beat this issue, we proposed a novel authentication system PassMatrix, in light of graphical passwords to restrict hold up under surfing attacks. With a one-time considerable login marker and circulative level and vertical bars covering the entire degree of pass-pictures, PassMatrix offers no sign for aggressors to understand or constrain the mystery key even they lead distinctive camera-based strikes. We in like manner executed a PassMatrix show on Android and finished certifiable customer investigations to evaluate its memorability and usability. From the exploratory result, the proposed structure achieves better assurance from bear surfing attacks while caring for accommodation.

Key words: Graphical Passwords, Authentication, Shoulder Surfing Attack.

1.INTRODUCTION

Texual passwords have been the most extensively used authentication system for a significant long time. Contained num-bers and promoted and cut down case letters, printed passwords are seen as adequately strong to restrict against creature control attacks. In any case, a strong printed mystery word is hard to recall and recollect [1]. Thusly, customers tend to pick passwords that are either short or from the vocabulary, rather than arbitrary alphanumeric strings. Shockingly more terrifying, it's definitely not a remarkable case that customers may use only a solitary username and mystery word for various accounts [2]. According to an article in Computer world, a security gather at a far reaching association ran a system watchword wafer and shockingly split around 80% of the specialists' passwords inside 30 seconds [3]. Printed passwords are every now and again insecure on account of the inconvenience of keeping up strong ones.

Different graphical password authentication scheme [4] ,[5],[6],[7]were created to address the issues and shortcomings related with literary passwords. In view of a few investigations, for example, those in[8],[9], people have a superior capacity to retain pictures with long haul memory (LTM) than verbal portrayals. Picture based passwords were turned out to be less demanding to remember in a few client studies[10],[11],[12]. Accordingly, clients can set up a mind boggling authentication secret key and are equipped for recalling it after quite a while regardless of whether the memory isn't actuated occasionally. In any case, the majority of these picture based passwords are helpless against bear surfing assaults (SSAs). This kind of attack either uses arrange recognition, for instance, seeing behind somebody or applies video getting strategies to get passwords, PINs, or other sensitive individual information [13],[14],[15] .

The human actions, for instance, picking awful passwords for new records and contributing passwords in an insecure way for later logins are seen as the weakest association in the authentication chain [16]. Therefore, an authentication design should be expected to overcome these vulnerabilities.

In this paper, we show a secure graphical authentication system named PassMatrix that shields customers from be-coming setbacks of shoulder surfing attacks while contributing passwords without trying to hide through the usage of one-time login markers. A login marker is discretionarily made for each pass-picture and will be trivial after the session closes. The login marker gives better security against bear surfing strikes, since customers use a dynamic pointer to raise the circumstance of their passwords as opposed to tapping on the mystery word question particularly And we give the most secure way so their pixel extent of their passwords won't be obvious to anyone.

1.2 Organization

This paper is composed as follows Section 2 gives the foundation of related systems about the graphical authentication blueprints. Section 3 gives working model of PassMatrix method and Section 4 gives the periods of PassMatrix display. Segment 5 Provides the Experimental Analysis and exactness. A Security Analysis is examined in Section 6. Section 7 concludes up the paper.

2. Motivation

As the mobile marketing statistics collection by Danyl, the mobile shipments had outperformed PC shipments in 2011, and the amount of mobile customers furthermore overpowered work region customers at 2014, which close to 2 billion[17]. Regardless, bear surfing strikes have spoken to a phenomenal hazard to customers' security and protection as mobile devices are getting the opportunity to be indispensable in current life. Individuals may sign into web associations and applications out in the open to get to their own particular records with their PDAs, tablets or open gadgets, similar to bank ATM. Shoulder-surfing aggressors can watch how the passwords were entered with the assistance of reflecting glass windows, or likewise screens hanging wherever out in the open spots. Passwords are acquainted with hazardous conditions, paying little personality to whether the passwords themselves are bewildering and secure. A secure authentication system should have the ability to shield against bear surfing ambushes and should be suitable to an extensive variety of contraptions. Authentication plots in the written work, for instance, those in,[6],[18],[19],[20],[21],[22],[23],[24] impenetrable to shoulder surfing, anyway they have either usability are impediments or minimal mystery key space. Some of them are not sensible to be associated in mobile contraptions and a vast bit of them can be successfully bargained to shoulder surfing attacks if aggressors use video getting systems like Google Glass[15],[26]. The limitations of usability fuse issues, for instance, putting aside more prominent chance to sign in, passwords being unreasonably troublesome, making it difficult to survey after a timeframe, and the authentication procedure being too much convoluted for customers without fitting guideline and practice.

In 2006, Wiedenbeck et al. proposed PassPoints[7] in which the client gets several focuses (3 to 5) in a photograph amidst the watchword creation stage and re-enters each of these pre-picked click-focuses in a right request inside its tolerant square amidst the login orchestrate. Com-paring to standard PIN and imaginative passwords, the Pass-Points plot fundamentally amasses the riddle word space and improves watchword memorability. Grievously, this graphical authentication plot is unprotected against bear surfing strikes. Along these lines, in context of the PassPoints, we consolidate utilizing one-time session passwords and distractors to build up our PassMatrix authentication structure that is invulnerable to continue surfing attacks also extended the DAS[6] in light of finger-drawn doodles and pseudosignatures in late mobile contraption. This authentication structure relies upon features which are isolated from the elements of the movement drawing process (e.g., speed or animating). These features contain direct biometric trademark. By the day's end, the attacker would need to mimic what the customer draws, and also how the customer draws it. Nevertheless, these three authentication designs are still all weak against bear surfing ambushes as they may reveal the graphical passwords clearly to some dark onlookers transparently.

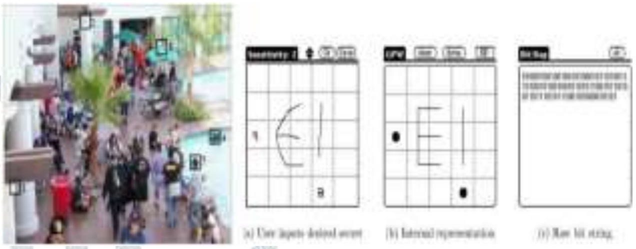


Fig. 1. (a) Pixel squares selected by users as authentication passwords in PassPoints [7]. (b) Authentication password drew by users and the raw bits recorded by the system database [6].

3. Working Model Of PassMatrix Technique

PassMatrix is utilized to defeat the security shortcoming of the conventional PIN technique and ease of acquiring passwords by eyewitnesses out in the open and furthermore the similarity issues to the gadgets.
PassMatrix is composed of the following components

(see Figure 2):

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

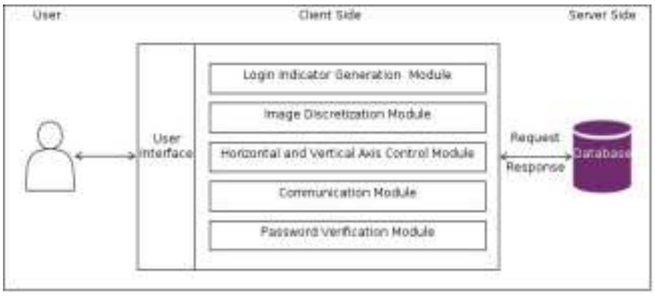

User
Client Side
Server Side
User Interface
Login Indicator Generation Module
Image Discretization Module
Horizontal and Vertical Axis Control Module
Communication Module
Password Verification Module
Request
Response
Database

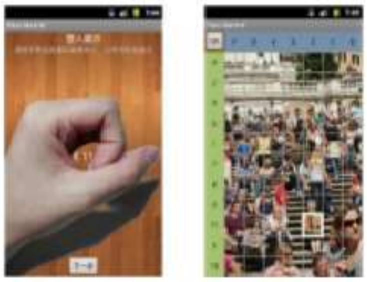
Fig. 2. Overview of the PassMatrix system.

Image Discretization Module. This module isolates every photograph into squares inside, from which clients would pick one as the pass-square. A photograph is limited into a 7 11 lattice. The humbler the photograph is discretized, the more noteworthy the secret key space is. In any case, the nonsensically considered certification issue of particular disputes and expansion the bother of UI practices on palm-sized mobile contraptions. Along these lines, in our execution, a division was set at 60-pixel interims in both level and vertical headings, since 60 pixels2 is the best size to pick particular request on contact screens.

Login Indicator Generator Module. This module makes a login marker including a few unquestionable characters, (for example, letter sets and numbers) or visual materials, (for example, shades and pictures) for clients amidst the authentication organize. In our execution, we utilized characters A to G and 1 to 11 for a 7 11 orchestrate. The two letters and numbers are made subjectively and along these lines another login marker will be given each time the module is called. The influenced login marker to can be given to clients clearly or acoustically.

For the previous case, the pointer could be appeared on the show (see Figure 3(a)) specifically or through another predefined picture. In the event that utilizing a predefined picture, for example, if the client picks the square (5, 9) in the picture as in Figure

3(b), at that point the login marker will be (E, 11). For the acoustical conveyance, the pointer can be gotten by a sound flag through the ear buds or Bluetooth. One guideline is to keep the pointers mystery from individuals other than the client, since the watchword (the sequence of pass-squares) can be remade effectively if the markers are known.



ı Obtain the login indicator (E,11) directly. (b) Obtain the login ıhrough a predefined image.

Fig:3(a) Obtain the login indicator(E,11) directly 3(b)Obtain the login indicator through predefined image

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. This control module gives drag and trip abilities to customers to control the two bars. Customers can fling either bar using their finger to move one alphanumeric without a moment's delay. They can in like manner move a couple of checks at any given minute by dragging the bar for a partition. The two bars are circulative, i.e., if the customer moves the horizontal bar .The bars are used to unquestionably raise (or toward the day's end, modify the login pointer to) the zone of the customer's pass-square.

Communication Module. This module is responsible for all the data transmitted between the customer gadgets and the authentication server. Any correspondence is ensured by SSL (Secure Socket Layer) convention and in this manner, is protected from being eavesdropped and captured.

Password Verification Module. This module confirms the client secret word amid the authentication stage. A pass-square acts like a secret key digit in the text-based watchword system. The client is verified just if each pass-square in each pass-picture is accurately lined up with the login pointer. The points of interest of how to adjust a login pointer to a pass-square will be portrayed in the following segment

Database. The database server contains a few tables that store client accounts, passwords (ID quantities of pass-pictures and the places of pass-squares), and the time term every client spent on both enlistment stage and login stage. PassMatrix has all the expected benefits to perform tasks like embed, alter, erase and look.

4.Phases Of PassMatrix

PassMatrix's authentication consists of a registration phase and an authentication phase as described below:

Registration phase

Figure 4 is the flowchart of the registration stage. At this stage, the client makes a record which contains a client name and a secret key. The secret word comprises of just a single pass-square per picture for a sequence of n pictures. The quantity of pictures (i.e., n) is chosen by the client subsequent to considering the exchange off amongst security and ease of use of the system .

The main motivation behind the username is to give the client a creative ability of having an individual record. The username can be discarded if PassMatrix is connected to authentication systems like screen lock. The client can either pick pictures from a gave list or transfer pictures from their gadget as pass-pictures. At that point the client will pick a pass-square for each chosen pass-picture from the lattice, which was separated by the picture discretization module. The client rehashes this progression until the point when the secret key is set.

Authentication phase

Figure 5 is the flowchart of the authentication stage. At this stage, the client utilizes his/her username, watchword and login markers to sign into PassMatrix. The accompanying depicts every one of the means in detail:

1) The client inputs his/her username which was made in the registration stage.

2) another pointer contained a letter and a number is made by the login marker generator module. The pointer will be indicated when the client utilizes his/her hand to frame a circle and afterward contact the screen. For this situation, the pointer is passed on to the client by visual input. The pointer can likewise be conveyed through a predefined picture or by sound criticism that we have specified in the past area.

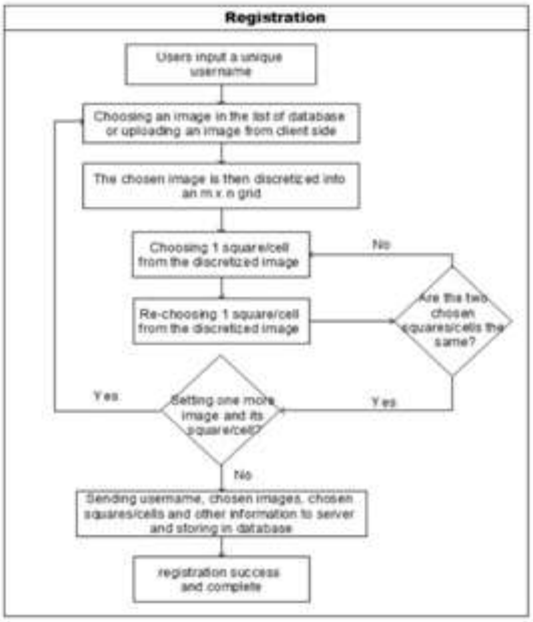

Registration
Users input a unique username
Choosing an image in the list of database or uploading an image from client side
The chosen image is then discretized into an m x n grid
Choosing 1 square/cell from the discretized image
No
Re-choosing 1 square/cell from the discretized image
Are the two chosen squares/cells the same?
Yes
Getting one more image and its square/cell?
Yes
No
Sending username, chosen images, chosen squares/cells and other information to server and storing in database
registration success and complete

Fig.4.The flowchart of registration phase in PassMatrix

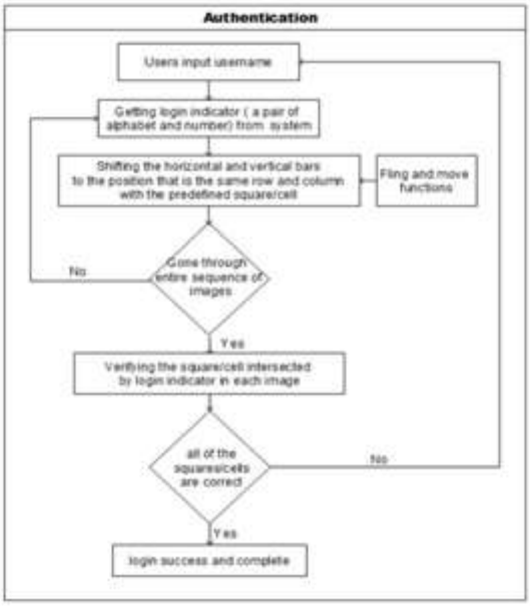

Authentication
Users input username
Getting login indicator (a pair of alphabet and number) from system
Shifting the horizontal and vertical bars to the position that is the same row and column with the predefined square/cell
Fling and move functions
Gone through entire sequence of images
No
Yes
Verifying the square/cell intersected by login indicator in each image
all of the squares/cells are correct
No
Yes
login success and complete

Fig. 5 The flowchart of authentication phase in PassMatrix.

3) Next, the principal pass-picture will be appeared on the show, with a horizontal bar and a vertical bar on its best and left individually. To react to the test, the client indulgences or drags the bars to align the pre-chosen pass-square of the picture with the login marker. For instance, if the marker is (E, 11) and the pass-square is at (5, 7) in the network of the picture, the client moves the character "E" to the fifth segment on the horizontal bar and "11" to the seventh column on the vertical bar.

4) Repeat stage 2 and stage 3 for each pre-chosen pass-picture.

5) The correspondence module gets client account data from the server through HttpRequest POST technique.

6) Finally, for each picture, the watchword confirmation module checks the alignment between the pass-square and the login pointer. Just if all the alignments are right in all pictures, the client is permitted to sign into PassMatrix.

5.Experimental Analysis

We investigated the gathered information from our experiments and overviews to assess the adequacy of the proposed system. The outcomes are displayed in two points of view: exactness and ease of use. The exactness point of view centers around the effective login rates in the two sessions, including the training logins. The ease of use viewpoint is estimated by the measure of time clients spent in each PassMatrix stage. The consequences of these two investigations unequivocally proposed that PassMatrix is commonsense to utilize. Toward the finish of this segment, we additionally exhibited the statistics of the study information from members about their own experience and client encounter on advanced cells and PassMatrix.

Accuracy

In the training period of the main session, members honed the login procedure on a normal of 4 times extending from 1 to 14 (barring one anomaly) and after that moved onto the authentication (login) stage. As we characterized in the past segment, members can continue attempting to sign in to their record until the point when they have bombed six times. At the end of the day, a fruitful endeavor implies that a client, in under or equivalent to six tries, can pass the authentication with a right secret word. On the off chance that every one of the six tries fizzled, this endeavor will be set apart as disappointment. Underneath, we characterize two terms First Accuracy and Total Accuracy that were utilized as a part of our trial:

$$\text{First Accuracy} = \frac{\text{Successful attempts in first Try}}{\text{Total attempts}}$$

$$\text{Total Accuracy} = \frac{\text{Successful attempts}}{\text{Total attempts}} \qquad (2)$$

TABLE 1

The accuracy of practice/authentication(login) in two sessions

	First session		**Second session**	
	First	Total	First	Total
Practice Phase	60.00%	100%	-	-
Login Phase	86.67%	100%	66.67%	93.33%

Table 1 demonstrates the First Accuracy and the Total Accuracy of the training and login stages in the two sessions with 30 members. By and large, 3:2 pass-pictures were chosen by every member. The outcome demonstrates that both the First and Total Accuracies in the primary session are higher than those in the second session. In the principal session, 26 out of 30 (86:67%) members could sign into the system effectively with only one attempt and every one of them were confirmed inside six tries (i.e., the Total Accuracy is 100%). After over two weeks (for a normal of 16:3 days), the First Accuracy in the second session was down to 66:67%, however the Total Accuracy is as yet 93:33%. We overviewed the members for the conceivable reasons of the huge drop in the First Accuracy and furthermore dissected those fizzled login endeavors in the second session. We discovered that the members did not by any means overlook their passwords. The vast majority of regardless them recall the areas of their pass-squares. In any case, they incidentally moved the horizontal or vertical bar to a wrong position and submitted without checking. The vast majority of them could sign into the system effectively in the precise next attempt and that is the reason the Total Accuracy (93:33%) is substantially higher than the First Accuracy (66:67%) in the second session.

Table 2 demonstrates the normal number of re-tries until the point that the client at long last signed in effectively. Indeed, even after over two weeks, members could sign into the system effectively in a normal of 0:64 (Median=0) re-tries, or as it were an aggregate of 1:64 tries. 25 out of 30 (83:33%) members could sign into their record inside three tries. For the rest, 4 members signed in effectively inside ten tries and just a single member neglected to sign in the wake of attempting ten times. As per the information recorded, these 5 members neglected to sign in inside 3 tries were all experiencing difficulty to pass just a single of the three pass-pictures they set in the registration stage.

In outline, we infer that the passwords of our PassMatrix are anything but difficult to retain. Clients can sign into the system with just 1:64 (Median=1) authentication requests on normal, and the Total Accuracy of all login trials is 93:33% even following two weeks

TABLE 2

The mean, median and standard deviation of the number of retries in a successful attempt.

	First Session			**Second Session**		
	Mean	Median	S.D	Mean	Median	S.D
Practice Phase	0.41	0	0.50	-	-	-
Login Phase	0.13	0	0.35	0.64	0	2.64

Usability

We counted the number of shifts and the elapsed time per pass-image in our experiment to measure the usability of our PassMatrix in practice.

TABLE 3

The mean, median and standard deviation of total time in the registration phase

	Registration(1st)		
	Mean	Median	S.D
Total Time(s)	106.6	90.5	55.58

Table 3 demonstrates the elapsed time that members expended in the registration stage. The registration took 1 minute and 46 seconds by and large. In spite of the fact that it appears the normal registration time is somewhat long in records, 73:33% of members felt that the registration procedure is really not time expending and 10% of them said that they invested the greater part of their registration energy in discovering pass-squares that are significant to them. Based on the review information from members, we inferred that the time required for registration is satisfactory to clients by and by. Amid registration, members can pick 3 to 5 pass-pictures as their passwords. In our analysis, everything except five members picked 3 pictures (mean=3:2 pictures). The normal time every client spent on training and login (see Table 4) in the main session was 47:86 seconds and 31:31 seconds individually. The expected time to sign into PassMatrix is decreased by 16:55 seconds subsequent to rehearsing 4 times by and large to get comfortable with the moving (i.e., dragging and hurling) tasks on contact screens. The outcomes are great because of the way that 73% of members have either no or short of what one year of experience of utilizing smart telephones (see Figure 13). Besides, even after over two weeks (16:3 days by and large), the normal login time was still as low as 37:11 seconds, not far from that (31.11 seconds) in the primary session. The reason that the time was marginally expanded was on account of members expected to review their passwords.

A survey demonstrated that the time spent in the login procedure is adequate to 83:33% of members. They felt that investing somewhat additional energy is beneficial if the authentication system can shield their passwords from being seen by others looking over their shoulders. For the moving tasks, while aligning a login marker to a pass-square in each pass-picture (see Table 4), there is no critical distinction (F=3:6, p> 0:05) in the quantity of such activities in the training stage and in the login stage in the two sessions, where F implies the F-test (http://en.wikipedia.org/wiki/F-test) and p implies the p-esteem (http://en.wikipedia.org/wiki/P-esteem). Since the login marker is arbitrarily produced for each pass-picture and elements in both the horizontal bar and vertical bar are additionally haphazardly rearranged, the quantity of moving activities used to move the login pointer to the correct position may vary too. There are two kinds of moving tasks, which are dragging (aligning the login pointer with the pass-square in a solitary move) and hurling (quick finger development on the screen; just moving one unit at a time). As appeared in the trial comes about, members just moved 4 to 5 times for every pass-picture by and large

TABLE 4

The mean, median and standard deviation of total time and the number of shifts in practice/authentication phase

	Practice(1st)		Login(1st)		Login(2nd)	
	Mean	Median	Mean	Median	Mean	Median
Time(s)	47.86	41	31.31	29.5	37.11	34
shift	5.67	5	4.91	5	4.9	4

In outline, the experimental results demonstrated that all members can work the login procedure through the Pass-Matrix's authentication interface. Subsequently, our PassMatrix is benevolent to use by and by. Clients may need to invest more energy to sign into PassMatrix in the training stage (47:86seconds by and large) directly subsequent to enlisting their records. Notwithstanding, they can sign into the system all the more immediately, even two weeks after registration (in the middle of 31:31 seconds and 37:11 seconds). The outcomes likewise demonstrated that clients could without much of a stretch control the horizontal and vertical bars to align lo-gin markers with pass-squares. Consequently, our PassMatrix is functional in the points of view of simple to-utilize and proficiency

6.SECURITY ANALYSIS

In this area we assess the security of the proposed authentication system against three kinds of assaults: irregular figure assault, bear surfing assault, and smear assault.

Random Guess Attack

To play out an arbitrary figure assault, the aggressor haphazardly tries each square as a conceivable pass-square for each pass-picture until an effective login happens. The key security determinants of the system are the quantity of pass-pictures and the level of discretization of each picture. To measure the security of PassMatrix against irregular figure assaults, we characterize the entropy of a secret word space as in condition

Table 5 characterizes the documentations utilized as a part of the condition. On the off chance that the entropy of a secret key space is k bits, there will be 2k conceivable passwords in that space.

Entropy = log2((Dx Dy)i)n (3)

Table 5

The definition of notations used in equation 3.

Notation	Definition
Dx	The number of partitions in x-direction
Dy	The number of partitions in y-direction
i=1	Obtain login indicators by touching the screen with hand grasped
i=2	Obtain login indicators by predefined images

7.CONCLUSION

With the expanding pattern of web services and applications, clients can get to these applications anytime and anyplace with different gadgets. With a specific end goal to ensure clients' computerized property, authentication is required each time they endeavor to get to their own record and information. Be that as it may, leading the authentication procedure in broad daylight may bring about potential shoulder surfing assaults. Indeed, even an entangled secret word can be split effectively through shoulder surfing. Utilizing traditional textual passwords or PIN technique, clients need to type their passwords to validate themselves and in this way these passwords can be uncovered effectively in the event that somebody looks over shoulder or uses video recording gadgets, for example, mobile phones.

To defeat this issue, we proposed a shoulder-surfing safe authentication system based on graphical passwords, named PassMatrix. Utilizing a one-time login marker per picture, clients can call attention to the area of their pass-square without straightforwardly clicking or contacting it ,and furthermore we give the stature and width pixel go in most secure way so it can't be obvious to the unapproved clients so which is an activity powerless against bear surfing assaults.

Based on the experimental results and survey information, PassMatrix is a novel and simple to-utilize graphical pass-word authentication system, which can viably ease bear surfing assaults. Likewise, PassMatrix can be connected to any authentication situation and gadget with straightforward information and yield capacities. The survey information in the client consider likewise demonstrated that PassMatrix is commonsense in reality .As a future enhancement we can erase the documents at whatever point it isn't essential.

REFERENCES

[1] 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.

[2] 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.

[3] K. Gilhooly, "Biometrics: Getting back to business," Computer-world, May, vol. 9, 2005.

[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. 4–4.

[5] "Realuser," http://www.realuser.com/.

[6] 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. 1–1.

[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] S. Brostoff and M. Sasse, "Are passfaces more usable than pass-words? a field trial investigation," PEOPLE AND COMPUTERS, pp. 405–424, 2000.

[11] 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.

[12] B. Ives, K. Walsh, and H. Schneider, "The domino effect of pass-word reuse," Communications of the ACM, vol. 47, no. 4, pp. 75–78, 2004.

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

[14] 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. 716–727, June 2014.

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

[16] M. Sasse, S. Brostoff, and D. Weirich, "Transforming the weakest link human/computer interaction approach to usable and effective security," BT technology journal, vol. 19, no. 3, pp. 122–131, 2001.

[17] "Mobile marketing statistics compilation," http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/.

[18] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management, 2004.

[19] D. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard: Towards more secure password entry on publicly observable touch screens," in Proceedings of OZCHI-Computer-Human Interaction Special Interest Group (CHISIG) of Australia. Canberra, Australia: ACM Press. Citeseer, 2005.

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

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

[22] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma, "Pas: predicate-based authentication services against powerful passive adversaries," in 2008 Annual Computer Security Applications Conference. IEEE, 2008, pp. 433–442.

[23] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A stroke-based textual password authentication scheme," in Education Technology and Computer Science, 2009. ETCS'09. First International Workshop on, vol. 3. IEEE, 2009, pp. 90–95.

[24] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using captcha in graphical password scheme," in 2010 24th IEEE International Conference on Advanced Information Networking and Applications. IEEE, 2010, pp. 760–767.

[25] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nichol-son, and P. Olivier, "Multi-touch authentication on tabletops," in Proceedings of the 28th international conference on Human factors in computing systems. ACM, 2010, pp. 1093–1102.

[26] "Black hat: Google glass can steal your passcodes," https://www.technologyreview.com/s/529896/black-hat-google-glass-can-steal-your-passcodes/.

Author's Profile:

Miss.B.Swetha has received B.Tech review degree in Computer Science and Engineering(CSE) in the year 2016 and Pursuing M.Tech in Computer Science and Engineering (CSE) from Narayana Engineering College. (Affiliated to JNTU, Anantapur), Nellore, AndhraPradesh

Dr. B. GeethaVani has received the B.Tech degree in Computer Science and Engineering from JNTU Hyderabad in 1993 and M.Tech degree in Computer Science and Engineering from JNTU Hyderabad. She has obtained Ph.D in Computer Science and Engineering from JNTU Kakinada, India. She is working as HOD & Professor in the Department of ComputerScience and Engineering at Narayana Engineering College, Nellore, A.P. Her research interests includes Artificial Neural Networks, Image Processing and Information Security.

,