International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

A Shoulder Surfing Resistant Graphical Verification System

A Sai Manoj[1], Dr. T. Sudhir[2], A. V. Jayanth[3], Ch. Pavan[4], A. Phani Lalith[5]

[1,3,4,5] Student, Dept. of Computer Science and Engineering, VVIT, AP, India
[2]Professor, Dept. of Computer Science and Engineering, VVIT, AP, India

---

Abstract - Confirmation in light of passwords is used, all things considered, in applications for PC security and insurance. Regardless, human exercises, for instance, picking unpleasant passwords and contributing passwords in an unverifiable way are seen as "the weakest association" in the affirmation chain. Rather than self-self-assured alphanumeric strings, customers tend to pick passwords either short or noteworthy for straightforward recognition. With web applications and convenient applications loading up, people can get to these applications at whatever point and wherever with various devices. This advancement brings magnificent solace yet also grows the probability of displaying passwords to hold up under surfing attacks. Aggressors can observe clearly or use external narrative contraptions to accumulate customers' accreditations. To vanquish this issue, we proposed a novel confirmation system PassMatrix, in perspective of graphical passwords to contradict hold up under surfing strikes. With a one-time considerable login marker and circulative level and vertical bars covering the entire degree of pass-pictures, PassMatrix offers no knowledge for attackers to comprehend or restrict the watchword even they coordinate various camera-based ambushes. We in like manner executed a PassMatrix demonstrate on Android and finished bona fide customer examinations to evaluate its memorability and usability. From the exploratory result, the proposed system achieves better security from bear surfing attacks while taking care of convenience.

Key Words: Graphical Passwords, Confirmation, Shoulder Surfing Assault, Sliding Authentication.

1. INTRODUCTION

Printed passwords have been the most generally utilized validation strategy for quite a long time. Involved num-bers and upper-and lower-case letters, literary passwords are viewed as sufficiently solid to oppose against animal power assaults. In any case, a solid printed secret word is difficult to remember and recall [1]. Thusly, customers tend to pick passwords that are either short or from the word reference, instead of unpredictable alphanumeric strings. Shockingly more repulsive, it isn't a remarkable case that customers may use only a solitary username and mystery word for various records [2]. As indicated by an article in Computer world, a security group at an extensive organization ran a system secret word saltine and shockingly broke around 80% of the workers' passwords inside 30 seconds [3]. Literary passwords are regularly uncertain due to the trouble of keeping up solid ones.

1.1 MOTIVATION

As the portable showcasing insights accumulation by Danyl, the versatile shipments had overwhelmed PC shipments in 2011, and the quantity of portable clients likewise surpassed work area clients at 2014, which shut to 2 billion [17]. Be that as it may, bear surfing assaults have represented an awesome risk to clients' security and secrecy as cell phones are getting to be indis-pensable in current life. Individuals may sign into web administrations and applications openly to get to their own records with their PDAs, tablets or open gadgets, similar to bank ATM. Shoulder-surfing assailants can watch how the passwords were entered with the assistance of reflecting glass windows, or not to mention screens hanging wherever openly puts. Passwords are presented to dangerous conditions, regardless of whether the passwords themselves are perplexing and secure. A safe confirmation framework ought to have the capacity to protect against bear surfing assaults and ought to be pertinent to a wide range of gadgets. Validation plots in the writing, for example, those in [6], [18], [19], [20], [21], [22], [23], [24], [25] are impervious to bear surfing, however they have either ease of use confinements or little secret key space. Some of them are not appropriate to be connected in cell phones and the vast majority of them can be effortlessly bargained to bear surfing assaults if assailants utilize video catching systems like Google Glass [15], [26]. The impediments of ease of use incorporate issues, for example, setting aside greater opportunity to sign in, passwords being excessively troublesome, making it impossible to review after a timeframe, and the confirmation strategy being excessively convoluted for clients without legitimate training and practice.

1.2 ORGANIZATION

This paper is sorted out as takes after. Area 2 gives the foundations of related procedures about graphical authentication plans and Segment 3 portrays assault models. The proposed PassMatrix is introduced in Area 4. The client study and its outcomes are accessible in Segment 5 and Area 6 separately. A security investigation is examined in Segment 7. Area 8 closes the paper.

2. BACKGROUND AND RELATED WORK

In the previous a very long while, a great deal of research on watchword confirmation has been done in the writing. Among these proposed plans, this paper centers for the most part

around the graphical-based verification frameworks. To keep this paper compact, we will give a concise survey of the most related plans that were specified in the past area. Numerous different plans, for example, those in [27], [28], [29], [30], [31] may have great convenience, they are not graphical-based and require extra help from additional equipment, for example, sound, multi-touch screen, vibration sensor, or whirligig, and so on.

In the good 'ol days, the graphical capacity of handheld gadgets was powerless; the shading and pixel it could indicate was constrained. Under this impediment, the Draw-a-Mystery (DAS) [6] strategy was proposed by Jermyn et al. in 1999, where the client is required to re-draw a pre-characterized picture on a 2D lattice. We specifically remove the figure from [6] and demonstrate it in Figure 1(b). In the event that the illustration touches similar matrices in a similar grouping, at that point the client is verified. From that point forward, the graphical capacity of handheld gadgets has relentlessly and incessantly enhanced with the advances in science and innovation. In 2005, Susan Wiedenbeck et al. presented a graphical validation conspire Pass Points [7], and around then, handheld gadgets could as of now demonstrate high determination shading pictures. Utilizing the Pass Point conspire, the client needs to tap on an arrangement of pre-characterized pixels on the foreordained photograph, as appeared in Figure 1(a) (this figure is separated from [7]), with a right grouping and inside their tolerant squares amid the login organize. Additionally, Marcos et al.

likewise expanded the DAS in light of finger-drawn doodles and pseudo signatures in late cell phone [32], [33]. This authentication framework depends on highlights which are separated from the elements of the motion drawing process (e.g., speed or increasing speed). These highlights contain behavioral biometric trademark. As it were, the aggressor would need to emulate what the client draws, as well as how the client draws it. Be that as it may, these three verification plans are still all defenseless against bear surfing assaults as they may uncover the graphical passwords straightforwardly to some obscure eyewitnesses in broad daylight.

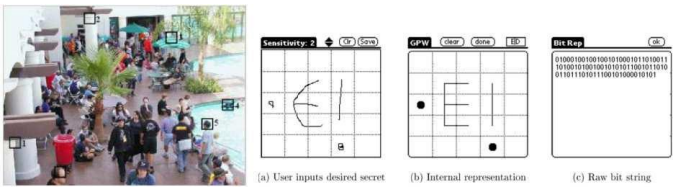

Fig. 1. (a) Pixel squares chose by clients as validation passwords in PassPoints [7]. (b) Confirmation secret key drew by clients and the crude bits recorded by the framework database [6].

Notwithstanding graphical validation plans, there was ome exploration on the expansion of regular personal distinguishing proof number (Stick) passage verification systems. In 2004, Roth et al. [34] displayed an approach for Stick section against bear surfing assaults by expanding the commotion to spectators. In their approach, the Stick digits are shown in either dark or white arbitrarily in each round. The client must react to the framework by distinguishing the shading for every secret word digit. After the client has settled on a progression of paired options (dark or white), the framework can make sense of the Stick number the client expected to enter by meeting the client's decisions. This approach could confound the spectators on the off chance that they simply watch the screen with no assistance of video catching gadgets. Be that as it may, if onlookers can catch the entire validation process, the passwords can be broken effortlessly.

Keeping in mind the end goal to guard the shoulder surfing assaults with video catching, FakePointer [35] was presented in 2008 by T. Takada. We utilize Figure 2 (from [35]) underneath to demonstrate the use of FakePointer. Notwithstanding the Stick number, the client will get another "answer pointer" each time for the validation procedure at a bank ATM. At the end of the day, the client has two insider facts for confirmation: a Stick as a settled mystery and an answer marker as an expendable mystery. The appropriate response pointer is a succession of n shapes if the Stick has n digits. At each login session, the FakePointer interface will display the client a picture of a numeric keypad with 10 numbers (like the numeric keypad for telephones), with each key (number) over a haphazardly picked shape. The numeric keys, however not the shapes, can be moved circularly utilizing the left or right bolt keys. Amid confirmation, the client should more than once move numeric keys circularly as appeared in the furthest left figure in Figure 2, until the point when the main digit of the Stick covers the principal state of the appropriate response marker on the keypad and afterward affirm a determination by squeezing the space key. This task is rehashed until the point that all the Stick digits are entered and affirmed. This approach is very strong notwithstanding when the assailant catches the entire authentication process. Notwithstanding, there is still space to make strides the secret key space. For instance, if the gadget utilized for confirmation is a cell phone, a tablet or a PC instead of a bank ATM, the secret word space can be expanded significantly since the Stick could be any mix of alphanumeric characters as opposed to simply numeric digits.

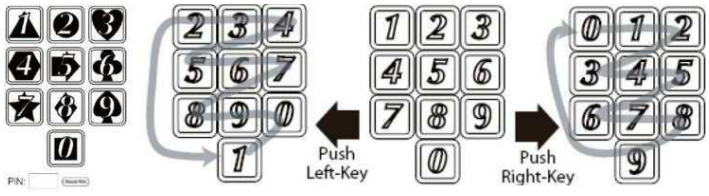

Fig. 2. FakePointer, where a client can move a numeric key format circularly utilizing right and left bolt keys. [35]

Wiedenback et al. [36] portrayed a graphical secret key section conspire in 2006, as appeared in Figure 3(b) (the figure is separated from [36]). This plan is impervious to bear surfing assaults utilizing an arched frame strategy. The client needs to perceive an arrangement of pass-symbols on the screen and snaps inside the raised structure shaped by all these pass-symbols. Keeping in mind the end goal to make the secret word hard to figure, countless diverse symbols can be embedded into the screen to expand the watchword space. In any case, an extensive number of items will swarm the show and may make objects indistinct.

In 2010, David Kim et al. [25] proposed a visual authentication plot for tabletop interfaces called "Shading Rings", as appeared in Figure 3(a) (the figure is removed from [25]), where the client is doled out I validation (key) symbols, which are all in all relegated one of the four shading rings: red, green, blue, or pink. Amid login, I networks of symbols are given, with 72 symbols being shown per framework. There is just a single key symbol exhibited in every network. The client must drag every one of the four rings (in a perfect world with pointer and thumb from two hands) simultaneously and put them in the network. The unmistakable key symbol ought to be caught by the right shading ring while whatever is left of rings simply make distraction determinations. The client affirms a determination by dropping the rings in position. The rings are sufficiently extensive to incorporate in excess of one symbol and would thus be able to jumble the immediate onlooker. Tragically, these sorts of passwords can be broken by converging the client's determinations in each login on the grounds that the shade of the doled out ring is settled and a ring can incorporate at most seven symbols. Along these lines, the aggressor just requires a predetermined number of trials to figure the client's secret key.

Fig. 3. (a) Shading Rings strategy [25]. (b) Arched Frame strategy [36].

3. PROBLEM STATEMENT, ATTACK MODEL AND ASSUMPTIONS

3.1 PROBLEM STATEMENT

With the expanding measure of cell phones and web administrations, clients can get to their own records to send private business messages, transfer photographs to collections in the cloud or transmit cash from their e-financial balance whenever and anyplace. While signing into these administrations out in the open, they may open their passwords to obscure gatherings un-intentionally. Individuals with vindictive aim could watch the entire validation system through inescapable camcorders and reconnaissance gear, or even a pondered picture a window [37]. Once the aggressor acquires the watchword, they could get to individual records and that would represent an extraordinary risk to one's benefits. Shoulder surfing assaults have increased increasingly consideration in the previous decade. The accompanying records the examination issues we might want to address in this investigation:

1) The issue of how to perform verification openly with the goal that shoulder surfing assaults can be allevi-ated.

2) The issue of how to expand secret key space than that of the customary Stick.

3) The issue of how to proficiently seek correct pass-word objects amid the validation stage.

4) The issue of expecting clients to remember additional data or to perform additional calculation amid confirmation.

5) The issue of restricted ease of use of verification conspires that can be connected to a few gadgets as it were.

3.2 ATTACK MODEL

3.2.1 SHOULDER SURFING ATTACKS

In light of past research [20], [21], [25], [34], [35], clients' activities, for example, writing from their console, or tapping on the pass-pictures or pass-focuses in broad daylight may uncover their passwords to individuals with awful expectation. In this paper, in view of the methods the aggressors utilize, we order bear surfing assaults into three sorts as underneath:

1) Sort I: Bare eyes.
2) Sort II: Video catches the whole validation process just once.
3) Sort III: Video catches the whole validation process more than once.

The last sorts of assaults require more exertion and systems from aggressors. In this way, if a validation conspire can oppose against these assaults, it is likewise secure against past kinds of assaults. A portion of the proposed verification plans [4], [5], [6], [7], [25], [38], including customary content secret key and Stick, are powerless against bear surfing Write I assaults and in this way are additionally subject to Sort II and Sort III assaults. These plans uncover passwords to aggressors when clients enter their passwords by straightforwardly squeezing or tapping on particular things on the screen. Different plans, for example, those in [19], [34] can oppose against Sort I however

are helpless against Sort II and Sort III assaults since the assailants can break passwords by meeting their video catches from various strides of the whole verification process.

3.2.2 SMUDGE ATTACKS

As indicated by a past report [39], verification conspires that expect clients to touch or hurl on PC screens or show screens amid the login stage are powerless against smear assaults. The aggressor can acquire the client's secret word effortlessly by watching the smear left on the touch screen (see Figure 4 which is specifically removed from [39])

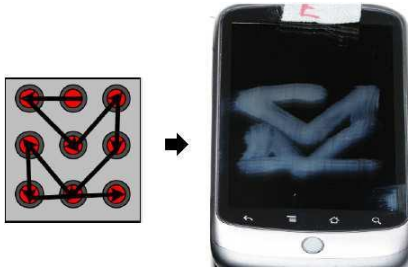

Fig. 4. (a) Android design screen secure which a client draws an individual open example that associates no less than four dabs on screen [39]. (b) The buildup from fingerprints left on the screen [39].

4. PASSMATRIX

To conquer (1) the security shortcoming of the customary Stick technique, (2) the ease of acquiring passwords by eyewitnesses in broad daylight, and (3) the similarity issues to gadgets, we presented a graphical validation framework called PassMatrix. In PassMatrix, a watchword comprises of just a single pass-square per pass-picture for a succession of n pictures. The quantity of pictures (i.e., n) is client characterized. Figure 5 exhibits the proposed conspire, in which the principal pass-square is situated at (4, 8) in the main picture, the second pass-square is on the highest point of the smoke in the second picture at (7, 2), and the last pass-square is at (7, 10) in the third picture.

In PassMatrix, clients pick one square for every picture for a grouping of n pictures instead of n squares in a single picture as that in the PassPoints [7] plot. In light of the client investigation of Prompted Snap Focuses (CCP) [40] proposed by Chiasson et al.,

Fig. 5. A watchword contains three pictures (n=3) with a pass square in each. The pass squares are appeared as the orange-filled territory in each picture.

The CCP strategy completes a great job in helping clients recall and recollect their passwords. On the off chance that the client taps on a mistaken district inside the picture, an alternate picture will be appeared to give the client a notice criticism. Nonetheless, going for reducing shoulder surfing assaults, we don't suggest this approach since the input that is given to clients may likewise be gotten by assailants.

Because of the way that individuals don't enroll another record or set up another screen bolt every now and again, we expect that these setup occasions should be possible in a sheltered domain instead of openly puts. Along these lines, clients can get pass-squares by just touching at or tapping on them amid the registra-tion stage.

4.1 OVERVIEW

PassMatrix is made out of the accompanying segments (see Figure 6):

Picture Discretization Module

Even and Vertical Hub Control Module
Login Pointer generator Module

Correspondence Module

Secret key Confirmation Module Database

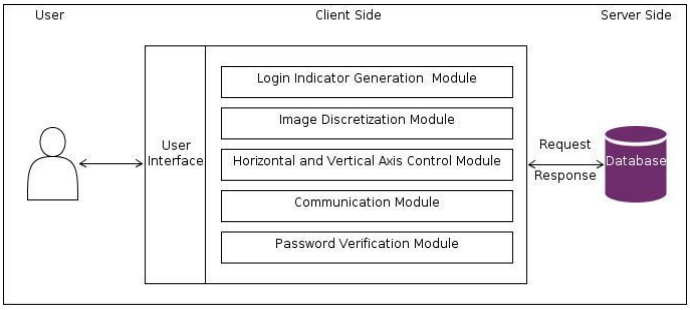

Fig. 6. Review of the PassMatrix framework.

Picture Discretization Module. This module partitions each picture into squares, from which clients would pick one as the pass-square. As appeared in Figure 5, a picture is separated into a 7 11 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 tasks on palm-sized cell phones. Thus, in our execution, a division was set at 60-pixel interims in both flat and vertical bearings, since 60 pixels2 is the best size to precisely choose particular questions on touch screens.

Login Pointer Generator Module. This module generates a login pointer comprising of a few discernable characters, (for example, letter sets and numbers) or visual materials, (for example, hues and symbols) for clients amid the authentication stage. In our usage, we utilized characters A to G and 1 to 11 for a 7 11 matrix. The two letters and numbers are produced haphazardly and in this manner an alternate login marker will be given each time the module is called. The created login pointer can be given to clients outwardly or acoustically. For the previous case, the marker could be appeared on the show (see Figure 7(a)) specifically or through another predefined picture. On the off chance that utilizing a predefined picture, for example, if the client picks the square (5, 9) in the picture as in Figure 7(b), at that point the login pointer will be (E, 11). For the acoustical conveyance, the marker can be gotten by a sound flag through the ear buds or Bluetooth. One standard is to keep the pointers mystery from individuals other than the client, since the secret key (the arrangement of pass-squares) can be reproduced effortlessly if the markers are known.

Fig. 7. (a) Get the login pointer (E,11) straightforwardly. (b) Get the login marker through a predefined picture.

Even and Vertical Hub Control Module. There are two parchment bars: a level bar with a grouping of letters and a vertical bar with an arrangement of numbers. This control module gives drag and excursion capacities to clients to control the two bars. Clients can hurl either bar utilizing their finger to move one alphanumeric at once. They can likewise move a few checks at any given moment by dragging the bar for a separation. The two bars are circulative, i.e., if the client moves the level bar in Figure 8(c) to left by three checks, it will end up being the bar appeared in Figure 8(d). The bars are utilized to verifiably call attention to (or as it were, adjust the login pointer to) the area of the client's pass-square.

Correspondence Module. This module is responsible for all the data transmitted between the customer gadgets and the validation server. Any correspondence is ensured by SSL (Secure Attachment Layer) convention [41] and accordingly, is protected from being listened in and blocked.

Secret key Check Module. This module checks the client secret word amid the validation stage. A pass-

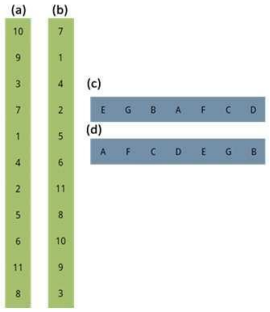

Fig. 8. Flat parchment bar (on the right/blue) and vertical bar (on the left/green).

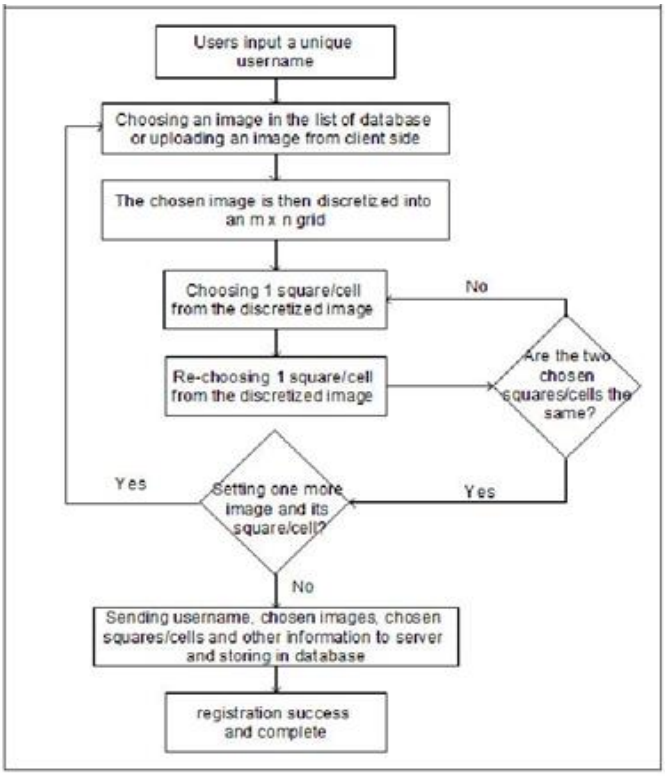

Fig. 9. The flowchart of enlistment stage in PassMatrix.

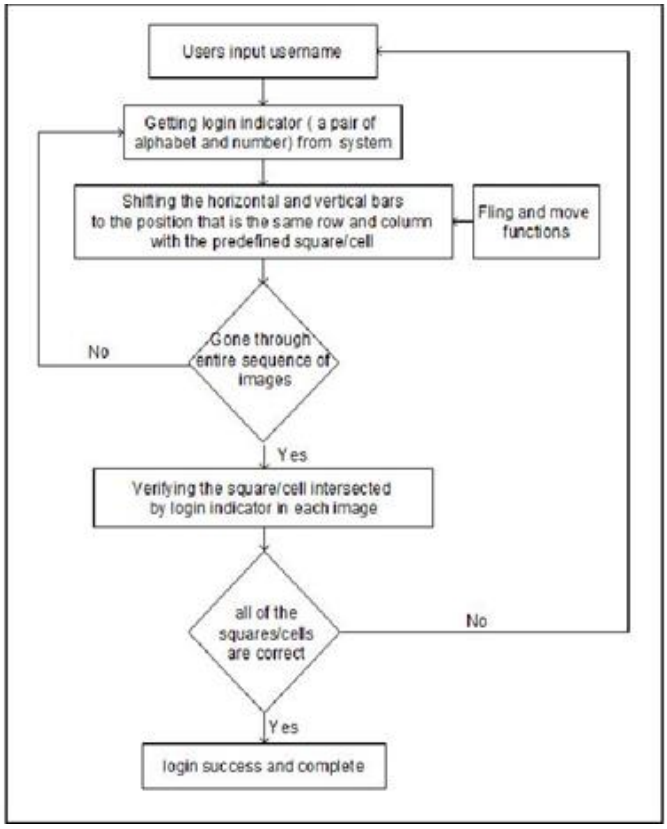

Fig. 10. The flowchart of verification stage in PassMatrix.

5 IMPLEMENTATION AND USER STUDY

In spite of the fact that the PassMatrix model was executed on an Android framework which has a little screen, it isn't restricted to the applications on little screen gadgets, for instance screen locking. Truth be told, it could be connected to an extensive variety of validation situations. For example, client account login in Windows 8, email account login on web program, and application login/open on Android OS. It can likewise be connected to any customer gadget, for example, PCs, workstations, tablets, cell phones, or bank ATM because of the way that the technique for verification is straightforward and the whole validation process can be finished by just touching or tapping on the screen.

In our execution, we accepted that clients down-stack an application from Google Play [43] and enroll a record for later login to utilize the administration. Since Android [44] is an open source working framework in view of Linux portion and is broadly utilized as a part of cell phones, for example, tablet PCs and PDAs, we executed a PassMatrix model on Android and did client trials to assess its memorability and ease of use. In this area we will portray our PassMatrix execution and the client ponder exper-imental plan, condition, members and methods. The consequence of the client study will be appeared in Area 6.

5.1 IMPLEMENTATION

The PassMatrix model was worked with Android SDK 2.3.3 since it was the standard form of the dissemination in 2012 [45]. In the wake of interfacing with the Web, clients can enroll a record, sign in a couple of times practically speaking mode, and afterward sign in for the explore different avenues regarding a customer's gadget (see Figure 11(a)). In the customer side of our model, we utilized XML to fabricate the UI and utilized JAVA and Android Programming interface to actualize capacities, including username checking, pass-pictures posting, picture discretization, pass-squares choice, login marker conveyance, and the level and vertical bars course. In the server side of our usage, we utilized PHP and MySQL to store and bring enlisted records to/from the database to deal with the secret key confirmation.

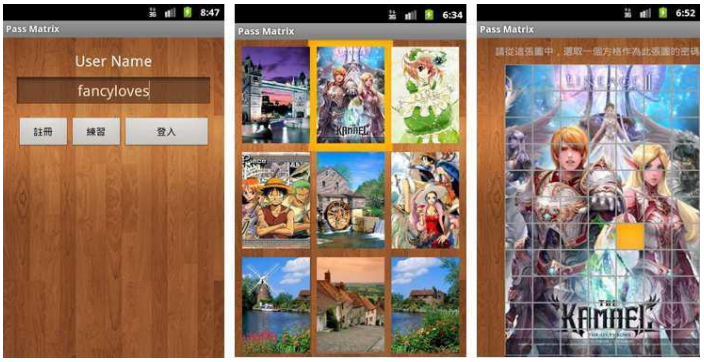

Fig. 11. (a) The Primary page of PassMatrix, clients can enroll a record, practice or begin to sign in for analyze. (b) Clients can look over a rundown of 24 pictures as their pass-pictures. (c) There are 7 11 squares in each picture, from which clients pick one as the pass-square.

In spite of the fact that in our proposed framework we said that clients can import their own particular pictures, we utilized a rundown of 24 settled test pictures in our examination (see Figure 11(b)). Each picture is shown in a size of 420 660 pixels and is discretized into 60 pixel squares. In this manner, clients have 7 11 squares to choose in each picture (see Figure 11(c)). After a client chooses three to five pictures with one pass-square per picture, the secret word will be put away as a rundown of directions in a database table (i.e., the areas of those chose pass-squares in the 7 11 framework). The secret key space relies upon the quantity of pictures set by clients. For example, if a client makes a record with four pictures, the secret word space is (7 11)4.

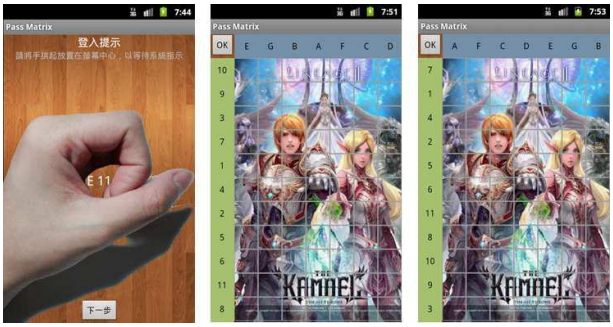

Fig. 12. (an) A visual route for clients to get a one-time legitimate login indicator. (b) The stages of alphanumeric in flat and vertical bars are haphazardly produced for each picture. (c) Clients can move the bars to the right position so that the login pointer lines up with the pass-square.

The initial phase in the login stage is getting the one-time legitimate login pointer from the framework. There are numerous approaches to get the marker and we've represented a few cases in Segment 4.1. In our execution, we embraced the least complex way: getting a handle on the hand with a little space left in the inside and after that touching the screen of advanced mobile phones (see Figure 12(a)). To secure against bear surfing, the marker isn't appeared until the point when the hand touches the screen and will vanish instantly when the hand leaves the screen.

The quantity of components on both the flat and vertical bars relies upon the discretization level of the pictures. In our usage, there are 7 letters (from A to G) and 11 numbers (from 1 to 11) on the even bar and on the vertical bar, separately. They are utilized to adjust the one-time pointer to the pass-square in each pass-picture amid the confirmation stage. Keeping in mind the end goal to jumble and in this way conceal the arrangement designs from onlookers, we haphazardly rearranged the components on the two bars in each pass-picture and let clients move them to the correct position (see Figure 12(b) and (c)). We actualized two bar-moving capacities: dragging and tossing. Since the whole bar is shift able and can be circled on either side (i.e., bi-directional and circulative), clients don't have to put their finger on a particular component with a specific end goal to move it.

5.2 PARTICIPANTS

30 fledgling clients (11 females and 19 guys), who are un-acquainted with PassMatrix or even graphical validation plans, were enlisted from our college to take an interest in this examination. At the season of this examination, the members are 24:53 years of age by and large (StdDev=3:14), in which three of them are post-specialists and most of the rest are graduate understudies. All members are either in Software engineering, Data Framework Administration or other information innovation majors. 76:67% of them have a foundation of data security. As Figure 13(b) appears, 73 % of members have short of what one year or no involvement with all of utilizing advanced mobile phones, though 20% of members have more than one however under two years of experience and the last 7% are veteran clients with over two years of experience. The study demonstrated that previously, they experienced confirmation forms on a normal of 12:6 times each day out in the open (see Figure 13(a)).

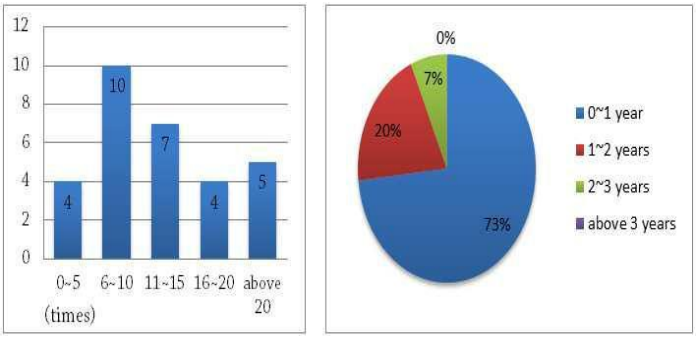

Fig. 13Patterns of Different conditions a part experienced confirmation shapes out in the open each day, and (b) Customer association in cutting edge cells with touch screens

6. CONCLUSIONS

6.1 DISCUSSION

With the expanding pattern of web administrations and applications, clients can get to these applications whenever and anyplace with different gadgets. To ensure clients' advanced prop-arty, confirmation is required each time they endeavor to get to their own record and information. Notwithstanding, leading the confirmation procedure openly may bring about potential shoulder surfing assaults. Indeed, even a confused secret word can be broken effectively through shoulder surfing. Utilizing traditional printed passwords or Stick strategy, clients need to type their passwords to verify themselves and consequently these passwords can be uncovered effectively in the event that somebody looks over shoulder or uses video recording gadgets, for example, phones.

To beat this issue, we proposed a shoulder-surfing safe validation framework in view of graphical passwords, named PassMatrix. Utilizing a one-time login marker per picture, clients can bring up the area of their pass-square without specifically clicking or touching it, which is an activity powerless against bear surfing assaults. As a result of the outline of the level and vertical bars that cover the whole pass-picture, it offers no sign for assailants to limit the secret word space regardless of whether they have in excess of one login records of that record. Besides, we executed a PassMatrix model on Android and completed client tests to assess the memorability

and convenience. The test result demonstrated that clients can sign into the framework with a normal of 1:64 tries (Median=1), and the Aggregate Precision of all login trials is 93:33% even two weeks after enrollment. The aggregate time devoured to sign into PassMatrix with a normal of 3:2 pass-pictures is in the vicinity of 31:31 and 37:11 seconds and is viewed as worthy by 83:33% of members in our client think about.

In light of the test results and overview information, PassMatrix is a novel and simple to-utilize graphical pass-word confirmation framework, which can successfully lighten bear surfing assaults. What's more, PassMatrix can be ap-utilized to any confirmation situation and gadget with basic info and yield abilities. The review information in the client think about likewise demonstrated that PassMatrix is handy in reality.

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 Engi-neering, Dumpster Diving, and Shoulder Surfing. Elsevier Science, 2011.

[14] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surf-ing: Human adversaries are more powerful than expected," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6, qq.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 linka human/computer interaction approach to usable and effec-tive 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 Interna-tional 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 Interac-tion 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, 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. Nicholson, 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/.