tion system named PassMatrix that protects users from be-coming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time 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.

## Motivation

As the mobile marketing statistics compilation by Danyl, the mobile shipments had overtaken PC shipments in 2011, and the number of mobile users also overtaken desktop users at 2014, which closed to 2 billion [17]. However, shoulder surfing attacks have posed a great threat to users' privacy and confidentiality as mobile devices are becoming indis-pensable in modern life. People may log into web services and apps in public to access their personal accounts with their smart phones, tablets or public devices, like bank ATM. Shoulder-surfing attackers can observe how the passwords were entered with the help of reflecting glass windows, or let alone monitors hanging everywhere in public places.

Passwords are exposed to risky environments, even if the passwords themselves are complex and secure. A secure authentication system should be able to defend against shoulder surfing attacks and should be applicable to all kinds of devices. Authentication schemes in the literature such as those in [6], [18], [19], [20], [21], [22], [23], [24],are resistant to shoulder-surfing, but they have either usability limitations or small password space. Some of them are not suitable to be applied in mobile devices and most

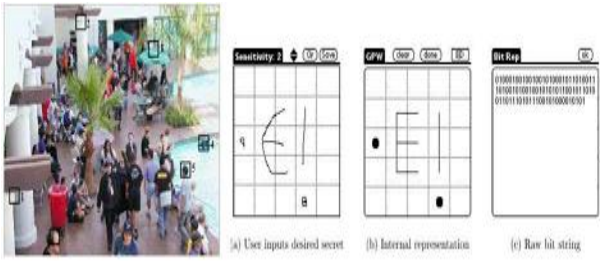

Fig. 1. (a) Pixel squares selected by users as authentication passwords in PassPoints [7]. (b) Authentication password drew by users and the raw bits recorded by the system database [6].

of them can be easily compromised to shoulder surfing attacks if attackers use video capturing techniques like

Google Glass [15], [26]. The limitations of usability include issues such as taking more time to log in, passwords being too difficult to recall after a period of time, and the authentication method being too complicated for users without proper education and practice.

In 2006, Wiedenbeck et al. proposed PassPoints [7] in which the user picks up several points (3 to 5) in an image during the password creation phase and re-enters each of these pre-selected click-points in a correct order within its tolerant square during the login phase. Com-paring to traditional PIN and textual passwords, the Pass-Points scheme substantially increases the password space and enhances password memorability. Unfortunately, this graphical authentication scheme is vulnerable to shoulder surfing attacks. Hence, based on the PassPoints, we add the idea of using one-time session passwords and distractors to develop our PassMatrix authentication system that is resistant to shoulder surfing attacks.also extended the DAS based on finger-drawn doodles and pseudosignatures in recent mobile device [32], [33]. This au-thentication system is based on features which are extracted from the dynamics of the gesture drawing process (e.g., speed or acceleration). These features contain behavioral biometric characteristic. In other words, the attacker would have to imitate not only what the user draws, but also how the user draws it. However, these three authentication schemes are still all vulnerable to shoulder surfing attacks as they may reveal the graphical passwords directly to some unknown observers in public.

### 1.2 Organization

This paper is organized as follows. Section 2 provides the backgrounds of related techniques about graphical authen-tication schemes and Section 3 describes attack models. The proposed PassMatrix is presented in Section 4. The user study and its results are available in Section 5 and Section 6 respectively. A security analysis is discussed in Section 7. Section 8 concludes the paper.

touching at or clicking on them during the registration phase.

Overview

PassMatrix is composed of the following components (see Figure 6):

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

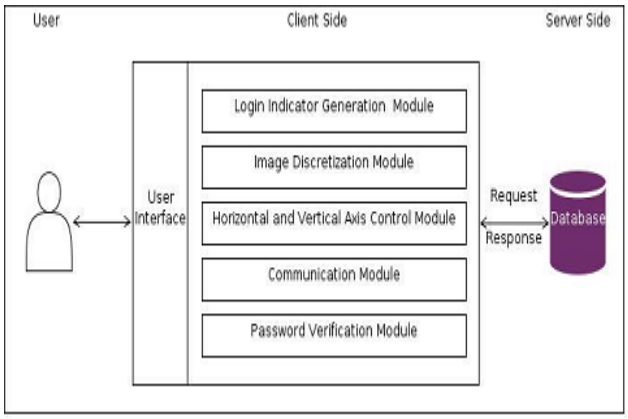


Fig. 6. Overview of the PassMatrix system.

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. Hence, in our implementation, a division was set at 60-pixel intervals in both

Horizontal and vertical directions, since 60 pixels$^2$ is the best size to accurately select specific objects on touch screens.

**Login Indicator Generator Module.** This module generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual mate-rials (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.

For the former case, the indicator could be shown on the display (see Figure 7(a)) directly or through another predefined image. If using a predefined image, for instance, if the user chooses the square (5, 9) in the image as in Figure 7(b), then the login indicator will be (E, 11). For the acoustical delivery, the indicator can be received by an audio signal through the ear buds or Bluetooth. One principle is to keep the indicators secret from people other than the user, since the password (the sequence of pass-squares) can be reconstructed easily if the indicators are known.

**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 provides **drag** and **fling** functions for users to control both bars. Users can fling either bar using their finger to shift one alphanumeric at a time. They can also shift several checks at a time by dragging the bar for a distance. Both bars are circulative, i.e., if the user shifts the horizontal bar in Figure 8(c) to left by three checks, it will become the bar shown in Figure 8(d). The bars are used to implicitly point out (or in other words, align the login indicator to) the location of the user's pass-square.

**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 [41] and thus, is safe from being eavesdropped and intercepted.

**Password Verification Module.** This module verifies the user password during the authentication phase. A pass-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. The details of how to align a login

indicator to a pass-square will be described in the next section

**Database.** The database server contains several tables that store user accounts, passwords (ID numbers of pass-images and the positions of pass-squares), and the time duration each user spent on both registration phase and login phase. PassMatrix has all the required privileges to perform operations like insert, modify, delete and search.

## II. PASSMATRIX

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

Registration phase

Figure 9 is the flowchart of the registration phase. At this stage, the user creates an account which contains a user-name 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 [42]. 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 pass-square 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.

Authentication phase

Figure 10 is the flowchart of the authentication phase. At this stage, 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 cre-ated 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

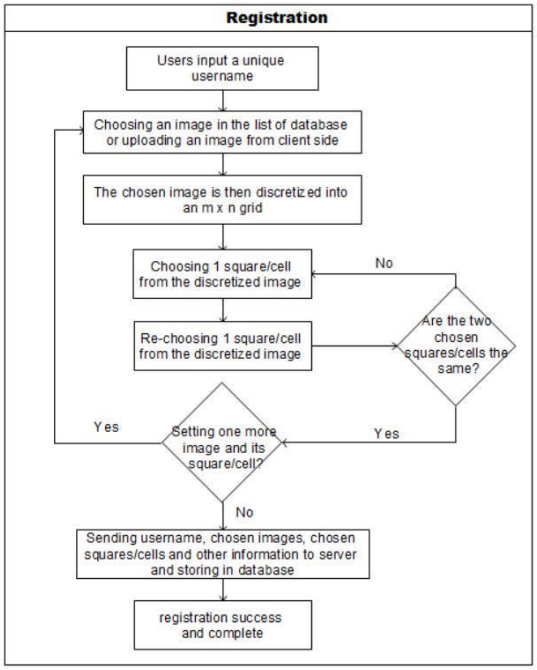


Fig. 9. The flowchart of registration phase in PassMatrix.

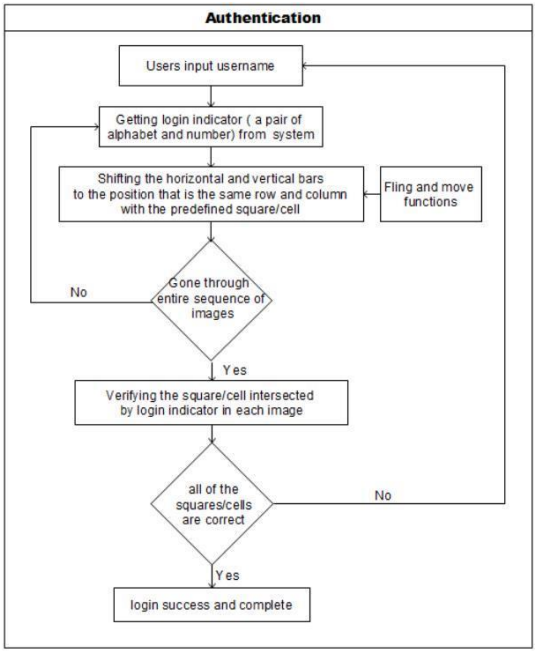


Fig. 10. The flowchart of authentication phase in PassMatrix.

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 also be delivered through a predefined image or by audio feedback that we have mentioned in the previous section.

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 (see Figure 12).

4) Repeat step 2 and step 3 for each pre-selected pass-image.

5) The communication module gets user account infor-mation from the server through HttpRequest
POST method.

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

## III. COLLECTED RESULTS

We analyzed the collected data from our experiments and surveys to evaluate the effectiveness of the proposed sys-tem. The results are presented in two perspectives: accuracy and usability. The accuracy perspective focuses on the suc-cessful login rates in both sessions, including the practice logins. The usability perspective is measured by the amount of time users spent in each PassMatrix phase. The results of these two analyses strongly suggested that PassMatrix is practical to use. At the end of this section, we also presented the statistics of the survey data from participants about their personal background and user experience on smart phones and PassMatrix.

### Accuracy

In the practice phase of the first session, participants prac-ticed the login process on an average of 4 times ranging from 1 to 14 (excluding one outlier) and then moved onto the authentication (login) phase. As we defined in the pre-vious section, participants can keep trying to log in to their account until they have failed six times. In other words, a successful attempt means that a user, in less than or equal to six tries, is able to pass the authentication with a correct password. If all six tries failed, this attempt will be marked as failure. Below, we define two terms First Accuracy and Total Accuracy that were used in our experiment:

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

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

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 shows the First Accuracy and the Total Accuracy of the practice and login phases in both sessions with 30

participants. On average, 3:2 pass-images were selected by each participant. The result shows that both the First and Total Accuracies in the first session are higher than those in the second session. In the first session, 26 out of 30 (86:67%) participants were able to log into the system successfully with just one try and all of them were authenticated within six tries (i.e., the Total Accuracy is 100%). After more than two weeks (for an average of 16:3 days), the First Accuracy in the second session was down to 66:67%, but the Total Accuracy is still 93:33%. We surveyed the participants for the possible reasons of the big drop in the First Accuracy and also analyzed those failed login attempts in the second session. We found out that the participants did not really forget their passwords. Most of them still remember the locations of their pass-squares. However, they accidentally shifted the horizontal or vertical bar to a wrong position and submitted without checking. Most of them could log into the system successfully in the very next try and that is why the Total Accuracy (93:33%) is much higher than the First Accuracy (66:67%) in the second session.

Table 2 shows the average number of re-tries until the user finally logged in successfully. Even after more than two weeks, participants were able to log into the system successfully in an average of 0:64 (Median=0) re-tries, or in other words a total of 1:64 tries. 25 out of 30 (83:33%) participants were able to log into their account within three tries. For the rest, 4 participants logged in successfully within ten tries and only one participant failed to log in after trying ten times. According to the data recorded, these 5 participants failed to log in within 3 tries were all having trouble to pass only one of the three pass-images they set in the registration phase.

In summary, we conclude that the passwords of our PassMatrix are easy to memorize. Users can log into the system with only 1:64 (Median=1) authentication requests on average, and the Total Accuracy of all login trials is 93:33% even after 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 | 0.350.64 | 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 shows the elapsed time that participants consumed in the registration phase. The registration took

1 minute and 46 seconds on average. Though it seems the average registration time is a bit lengthy in records, 73:33% of participants felt that the registration process is actu-ally not time consuming and 10% of them said that they spent most of their registration time in finding pass-squares that are meaningful to them. Based on the survey data from participants, we concluded that the time required for registration is

acceptable to users in practice. During registration, participants can choose 3 to 5 pass-images as their passwords. In our experiment, all but five participants chose 3 images (mean=3:2 images). The average time each user spent on practice and login (see Table 4) in the first session was 47:86 seconds and 31:31 seconds respectively. The required time to log into PassMatrix is reduced by 16:55 seconds after practicing

4 times on average to get familiar with the shifting (i.e., dragging and flinging) operations on touch screens. The results are good due to the fact that 73% of participants have either no or less than one year of

experience of using smart phones (see Figure 13). Furthermore, even after more than two weeks (16:3 days on average), the average login time was still as low as 37:11 seconds, not far away from that (31.11 seconds) in the first session. The reason that the time was slightly increased was because participants needed to recall their passwords.

A survey showed that the time spent in the login process is acceptable to 83:33% of participants. They felt that spending a little bit extra time is worthwhile if the authentication system can protect their passwords from being seen by others peeking over their shoulders.

For the shifting operations, while aligning a login in-dicator to a pass-square in each pass-image (see Table

4), there is no significant difference ($F=3:6$, $p> 0:05$) in the number of such operations in the practice phase and in the login phase in both sessions, where F means the F-test (http://en.wikipedia.org/wiki/F-test) and p means the p-value (http://en.wikipedia.org/wiki/P-value). Because the login indicator is randomly generated for each pass-image and elements in both the horizontal bar and vertical bar are also

randomly shuffled, the number of shifting operations used to move the login indicator to the right position may differ as well. There are two types of shifting operations, which are dragging (aligning the login indicator with the pass-square in a single move) and flinging (fast finger movement on the screen; only shifting one unit at a time). As shown in the experimental results, participants only shifted 4 to 5 times per pass-image on average.

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 summary, the experimental results showed that all participants can operate the login process through the Pass-Matrix's authentication interface. Thus, our PassMatrix is friendly to use in practice. Users may need to spend more time to log into PassMatrix in the practice phase (47:86 seconds on average) right after registering their accounts. However, they can log into the system more quickly, even two weeks after registration (in between 31:31 seconds and 37:11 seconds). The results also showed that users could easily control the horizontal and vertical bars to align lo-gin indicators with pass-squares. Hence, our PassMatrix is practical in the perspectives of easy-to-use and efficiency.

## IV. SECURITY ANALYSIS

In this section we evaluate the security of the proposed authentication system against three types of attacks: random guess attack, shoulder surfing attack, and smudge attack.

### Random Guess Attack

To perform a random guess attack, the attacker randomly tries each square as a possible pass-square for each pass-image until a successful login occurs. The key security determinants of the system are the number of pass-images and the degree of discretization of each image. To quantify the security of PassMatrix against random guess attacks, we define the entropy of a password space as in equation

3. Table 7 defines the notations used in the equation. If the entropy of a password space is k

bits, there will be $2^k$ possible passwords in that space.

$$\text{Entropy} = \log_2((D_x \quad D_y)^i)^n \qquad (3)$$

**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 |

## V. 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 prop-erty, 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 tradi-tional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones.

To overcome this problem, we proposed a shoulder-surfing resistant authentication system based on graphi-cal 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.

Based on the experimental results and survey data, PassMatrix is a novel and easy-to-use graphical pass-word authentication system, which can effectively alleviate shoulder-surfing attacks. In addition, PassMatrix can be ap-plied to any authentication scenario and device with simple input and output capabilities. The survey data in the user study also showed that PassMatrix is practical in the real world.

## 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.



Mr.T.Sudharan Simha has received B.Tech review degree in Information Technology(INF) in the year 2014 and Pursuing M.Tech in Computer Science and Engineering (CSE) from Priyadarshini College of Engineering and Technology(Affiliated to JNTUniversity, Ananthapuram), Nellore, Andhra Pradesh, India



Prof.D.Srinivasulu has received B.Tech review degree in Computer Science and Engineering from K..L College of Engineering, Vijayawada and M.Tech in Computer Science and Engineering from JNTUnversity, Kukatpally, Hydearbad.. Presently Pursuing Ph.D in Computer

Science and Engineering from Rayalaseema University, Kurnool(A.P). His interesting domain is Wireless Networks, he attended 5 International and 2 National Conferences and published 5 papers in various International Journals. He is dedicated to teaching field from last 23 Years, presently working as Professor and HOD in Computer Science and Engineering Department at Priyadarshini College of Engineering and Technology (Affiliated to JNTUniversity, Ananthapuram), Nellore, Andhra Pradesh, India