International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June-2018 www.irjet.net p-ISSN: 2395-0072

PASSMATRIX- An Authentication System to Resist Shoulder Surfing Attacks

Pallavi Shinde[1], Prof. K. N. Shedge[2]

[1]PG Student, Computer Engineering Department,
[2]Assistant. Professor, Computer Engineering Department, SVIT, Nashik, India.

Abstract - *Textual passwords are widely used in authentication method. Strong textual passwords are hard to memorize. To address the weakness of textual password graphical passwords are proposed. Click based or pattern based approaches are widely used techniques for mobile authentication system. Such textual and graphical passwords a scheme suffers from shoulder surfing attacks. Attacker can directly observe or can use video recorder or webcam to collect password credentials. To overcome the problem, shoulder surfing attack resistant technique is proposed. This technique contains pass-matrix. More than one image are used to set the password. For every login session, user needs to scroll circulatory horizontal and vertical bars. A password hint is provided to the user to select desired image password grid. Horizontal and vertical scroll bar covers the entire scope of pass-images. For password selection, password hint and horizontal and vertical scroll bar are used. The proposed technique is implemented on android platform. The system performance is measured using memorability and usability of a password scheme with respect to the existing technique.*

***Key Words*: Authentication system, Graphical Passwords, Shoulder surfing attack**

1. INTRODUCTION

Most of the authentication system uses text based passwords. For higher security against brute force attack strong password is generated using combination of upper case and lowercase characters, numerical values and special characters. Strong passwords are randomly generated and not have specific meaning. Such passwords are hard to memorize and recollect. Due to this reason user tried to set easy passwords having some dictionary meaning. As per the article [3] in computer world, 80% user set such easy password and those can be cracked by hackers within 30 seconds.

Based on the Psychological study [9] user is able to memorize images with long terms memory rather than textual words. To overcome the problems of text based passwords, image based passwords technique is proposed. User can be able to set complex image based password and can be recollect it after long time. But most of the image based password authentication systems are vulnerable to shoulder surfing attack. In shoulder surfing attack, attacker can directly get the information by standing next to the user or indirectly using video recorder or web cam.Most of the handheld devices uses pattern based password. These patterns based authentication system is vulnerable to shoulder surfing attack as well as the Smudge Attacks. The attacker can easily get the password pattern by observing the smudge left on the touch screen. Defining bad and easily crackable password and/or login using password in insecure environment mainly causes loopholes in password authentication security. There is a need of secured password authentication system which overcomes the drawbacks of existing text and image based password schemes. To overcome these problems biometrical password scheme is introduced. In biometric password authentication system user voice, retina, thumbprint, face are used as a passwords. There are various types of biometric sensors which as able to authenticate user. Such schemes are secured but hardware specific. Special sensor devices are required for authentication. It is impractical to have such authentication system to regular web based resources and such system installation and maintenance is costly. This proposed work provides a graphical authentication system. This system is able to restrict shoulder surfing attack. To resist shoulder surfing attack it uses session password technique. In session password user will add new password at every login attempt. The added password is valid for only single login session. Pass-matrix technique is proposed in this work. This technique uses pass-point clicking. This technique uses more than one image as a password. For every image it defines the click points as a pass-square. If user is not being able to click on correct pass square then system displays a wrong image for next pass input. This wrong image is treated as a warning to the user. To define session password for pass square click, a hint is provided to the user. Based on the given hint user will select the password for that session.

1.1 Related Work:

To provide more secured authentication system external hardware can be used such as: multi-touch monitor, voice recorder, some sensors like vibration sensor, gyroscope sensor, etc.[4][5][6] These systems provide better security than other password authentication system but such system are not affordable to every user. External hardware is required for every authentication and may not be applicable to web based systems. This work mainly focuses on graphical password authentication systems.

Draw-a-Secret (DAS) technique is proposed by Jermyn et al.[7] in 1999. In early days the handheld devices was not

graphically strong. The color and pixel quality was weak. DAS system is implemented by considering these limitations. In this scheme, user need to draw the predefined secret password on 2D graphical screen. For this scheme, the whole screen is divided in number of grids. User need to follow the greed selection sequence while drawing the password image.

In 2005, PassPoints[8] technique was proposed by Susan Wiedenbeck et al. The quality of handheld devices was improved in 2005. The high resolution graphical display was available in handheld devices. In this system image click points are used as a password. User need to select appropriate image click points from a password image in a predefined sequence. For point selection a tolerance square is defined.

Based on the gesture drawing process and DAS system[9], a new authentication system is proposed by I. Jermyn, this system contains finger-drawn doodles and pseudo-signatures. User needs to draw a doodle/ signature/ pattern on a touch screen handheld devices.

The above three techniques are vulnerable to shoulder surfing attack. The attacker can view the authentication secret as well as can view the drawing strategy.

To resist shoulder surfing attack, Roth et al. proposes a authentication system based on personal identification number-PIN[10]. In this scheme all characters are displayed in black or white color and randomly placed on a screen. User need to select the color sequence of PIN digit. The sequence is binary sequence. This system resists the shoulder surfing attacks of direct viewer attackers. But if attacker uses the video recording system to record the PIN entering process, attacker can easily crack the password.

To resist shoulder surfing attack with video capturing, the FakePointer[11] technique is proposed by T. Takada. In this system user get one answer indicator to enter the password. This answer indicator generates the hint which is different with every login session. In this system, 10 different numeric values are added in different shapes to generate a login keypad. This keypad is available to the user to enter the password. User has facility to rotate the digit but not the shapes. Shape value is provided as a login hint to the user. User need to rotate all the digits to fit the particular digit PIN in particular shape. This is robust to shoulder surfing attack. But the password space is limited to 10 digits.

To increase the password space, pass icon based technique is proposed by Wiedenback et al.[12]. This technique is based on the convex hull method. User identifies the set of pass icon on screen and click at the convex hull formed by these icons. Other icons are also inserted to increase the password space. This technique generates the crowd on screen and sometimes such display makes objects Indistinguishable.

A Color Rings technique is proposed by David Kim et al.. This technique is for table top applications. At a time this system displays 72 icons on the screen. User need to capture distinct key icons in to the correct color ring. The color of the assigned ring is fixed and hence it is vulnerable to attack. Attacker can predict the password by observing multiple login sessions.

Cued Click Points(CPP)[13] technique is proposed by Chiasson et al. This technique uses number of pass images and click points on each pass image as a password. This technique is useful to recollect the password. If user enters the wrong password then wrong pass image is displayed to the user. This technique is again vulnerable to shoulder surfing attack.

CAPTCHA-based method[14] is proposed by Uwe Aickelin. This method uses captcha text and image combinations for login phase. Multiple image sequence is the user password. User need to add some captcha characters present at predefined positions of password image.

A PassMatrix scheme[1] is proposed for authentication. This scheme uses combination of one time login indicator and multiple password images click points. The password is selected without touching the exact password click point. But this scheme uses same images for every login session.

1.2 Analysis and Problem Formulation:

In day to day life user uses mobile and web based systems to access their personal email accounts, online money transfer, upload and download personal data on cloud. Due to the internet availability, user accesses such systems anytime and anywhere. The use of such personal service access in public locations may cause security issues. User's personal password may be leaked unconsciously to the unknown user. People with malicious intent can make misuse of such information.

There is need to provide better security to access such personal services in public environment. Following are the research problems that need to be addressed:

Alleviate the shoulder surfing attack in authentication process in public environment.

- How to increase password space than existing PIN system
- How to provide an ease to find desired pass object from set of objects
- How to make password easy to memory and require less computation during authentication.
- How to make the system available for all kind of devices and affordable to every user.

2. System Overview:

Following fig. 1 shows the system architecture.

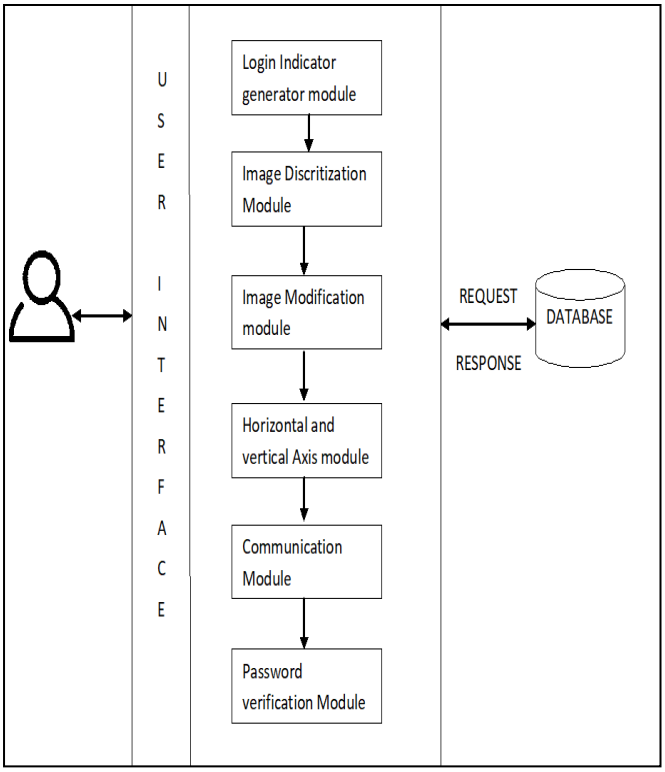

Fig 1: System Architecture

A novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks is proposed. The proposed system provides a new graphical password authentication system. This is android based system. Multiple images are used to define password. . For every login session, user needs to scroll circulative horizontal and vertical bars. A password hint is provided to the user to select desired image password grid. For password selection, password hint to set covering the entire scope of pass-images.

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.

To provide more secured authentication system, The base paper is extended with the following 2 techniques.

- If incorrect password grid is selected then for higher security system can display incorrect image for next pass selection.
- System can Change pass image for every login using: rotation and flipping.

I. Algorithms:

PASSmatrix-Authentication:

In registration phase, the user creates an account which contains a username and a password. The password consists of only one pass-square per image for a sequence of n images. It is assume that user will register to the system in secure environemnt.

For log into the passMatrix the user uses his/her username, password and login indicators. System selects user pass iamges based on the login name and provide a panel to select a password using horizontal and verical scroll bars. Based on predefined password and generated hint, user can generate a net password for every login session.

Algorithm Steps:

Input: Registration details

Username

Output: Authentication result

Processing:

1. Get pass images by matching the user name
2. Generate a random alphabet/ number as an hint and provide to the user using audio message.
3. For every login pass image
4. Discretize image in 6 *6 block. Rotate and flip image
5. Generate horizontal and vertical scroll bars
6. Accept user input
7. Check if user input matches to the registration details
8. Display next image and fllow steps from 4
9. Else disply incorrect input image to the user as a warning
10. If all clicks matches notify user with success message
11. If login attempts >3 then lock the system for next 5 min

Mathematical Model

System S can be defined as

S= {I, O,F}

Where,

I = {I1, I2, I3}, Set of inputs

I1 = Set of input images

I2 = Registration details

I3 = Image Clicks

O= {O1,O2} Set of outputs

O1 = Password selection Hints

O2 = Notification

F ={F1,F2,F3,F4,F5,F6,F7} Set of Functions

F1 = Registration Process

F2 = Login Process

F3 = Image Discritization

F4 = Pass image Rotation

F5 = Pass Image Flipping

F6 = Scroll Creation

F7 = Login Validator

F7 = Login Validator

II. Implementation

a) Experimental Setup:

A client server architecture is developed. For client end an android application is developed using android studio. The application is developed for android sdk version 5.1 and above. At the server end java application is developed to define web services. To store database mysql database is used.

b) Dataset:

For creating pass matrix grid images are required. Images are downloaded from flikr dataset[16]. Random images from these dataset are selected to define password of a system.

c) Performance Metric:

For testing 30 different users (15 male, 15 female)

are selected. These users test this system for 15 times. First 5 attempts are treated as practice sessions and next 10 sessions are treated as login attempts. The accuracy and usability is calculated using practice sessions and login attempts.

- Accuracy:
  1. Based on the practice sessions, accuracy of the system is calculated as:

$$\$practice\_acc = \frac{\text{successful practice attempts}}{\text{total practice attempts}}$$

  2. Based on the login sessions, accuracy of the system is calculated as:

$$\$login\_acc = \frac{\text{successful login attempts}}{\text{total login attempts}}$$

- Usability:

The usability of system measures the users' experience. It includes the total time required for registration and login phase for 3 pass images and 5 pass images. Based on the user type Mean and median is calculated for time required for each user type.

d) Graphical View:

Following Figure 2 shows the login interface of the system.

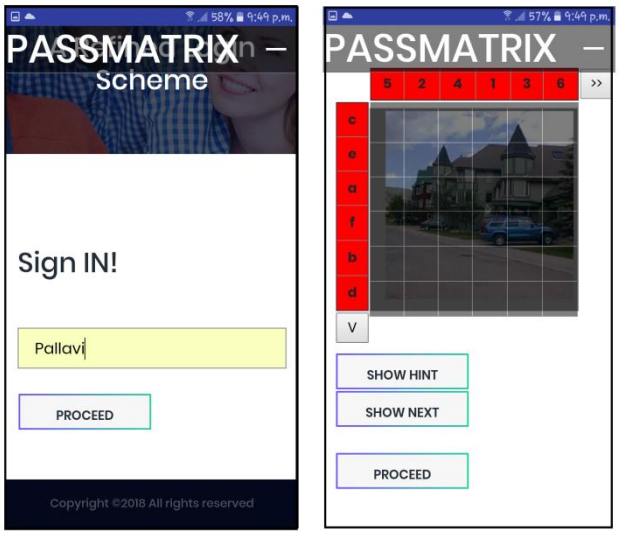

Fig 2: Login Screen

e) Result Analysis:

Table 1 describes the accuracy of the system for practice and login sessions with different user types. The total accuracy of the system is 0.775.

Table 1: Accuracy Evaluation

User Type	Test Type	Total Attempts	Successful Attempt	Accuracy
Male	Practice Session	5	4	0.8
	Login Session	10	8	0.8
Female	Practice Session	5	3	0.6
	Login Session	10	9	0.9

Table 2 describes the user experience in terms of time required for processing . After conducting 5 session of practice attempts and 10 sessions of login attempts mean and median is calculated. The average mean time is: 1.865 and the average median is 1.796

Table 2: Usability Evaluation

Test Type	Mean	Median	User Type
Practice Session (for 3 images)	1.78	1.3	Male
Login Session (for 3 images)	1.32	1.2	Male
Practice Session (for 3 images)	1.89	1.4	Female
Login Session (for 3 images)	1.67	1.65	Female
Practice Session (for 5 images)	2.09	2.25	Male
Login Session (for5 images)	2	2.2	Male
Practice Session (for 5 images)	2.22	2.27	Female
Login Session (for5 images)	1.95	2.1	Female

Figure 3 describes the graphical representation of table 2. It shows the mean and median variation as per the pass images and user types.

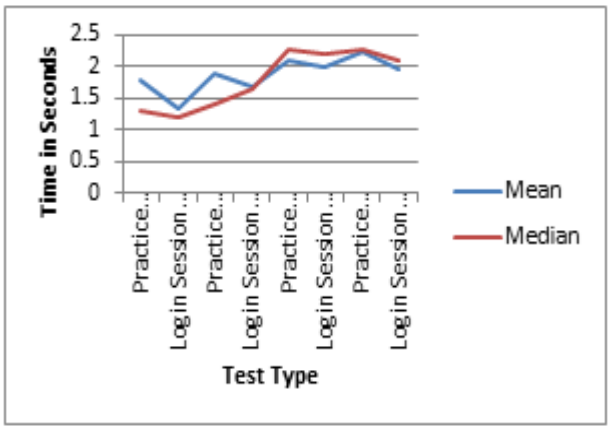

Fig 3: Usability Evaluation

The table 3 compares the proposed system with the existing pass matrix scheme[1]. The image processing is applied that flips the pass-image at the time of login. The flipping changes the grid selection positions at every login session.

Table 3: System Comparison

System	Grid Password Selection Scheme	Session Grid Selection	pass image Processing	Invalid Grid selection Handling
A Shoulder Surfing Resistant Graphical Authentication System[1]	yes	yes	-	-
PASSMATRIX - An Authentication System to Resist Shoulder Surfing Attacks	yes	yes	Flip	Display misleading Pass-images

3. CONCLUSION

The proposed system provide an authentication system for android devices. This system can resist shoulder surfing attack. This is click based password system. This technique contains pass-matrix. More than one image are used to set the password. This system follows the technique of session password. A password added in one login session can not be applicable for other sessions. In future, the system can be implemented for desktop application as well as Automated Teller Machine(ATM).

ACKNOWLEDGEMENT

First of all my special thanks to head of Department of Computer Engineering, SVIT, Chincholi, Nashik Prof. Prof. K. N. Shedge, principal Dr. S. N. Shelke for their kind support and suggestions. It would not have been possible without the kind support. We would like to extend our sincere thanks to all the faculty members the department of Computer Engineering for their help. We are also thankful to colleagues for moral support and encouragement. At the end, We are very much thankful to all for direct and indirect help.

REFERENCES

[1] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng,"A Shoulder Surfing Resistant Graphical Authentication System",IEEE Transactions on Dependable and Secure Computing, Vol.1 PP. 1, Issue: 99, March 2016

[2] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, 2005.

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

[4] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices," in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser.

[5] TEI '11. New York, NY, USA: ACM, 2011, pp. 197-200.

[6] Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: A tactile password system," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 1089-1092

[7] Oakley and A. Bianchi, "Multi-touch passwords for mobile device access," in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp '12. New York, NY, USA: ACM, 2012, pp. 611-612.

[8] 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.

[9] 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.

[10] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "Graphical passwordbased user authentication with free-form doodles," IEEE Transactions on Human-Machine Systems, vol. PP, no. 99, pp. 1-8, 2015.

[11] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in Proceedings of the 11th ACM conference on Computer and communications security, ser. CCS '04. New York, NY, USA: ACM, 2004, pp. 236-245.

[12] T. Takada, "fakepointer: An authentication scheme for improving security against peeping attacks using video cameras," in Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008. UBICOMM' 08. The Second International Conference on. IEEE, 2008, pp. 395-400.

[13] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proceedings of the working conference on Advanced visual interfaces, ser. AVI '06. New York, NY, USA: ACM, 2006, pp. 177-184.

[14] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," Computer Security-ESORICS 2007, pp. 359-374, 2007.

[15] 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.

[16] A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith, "Smudge attacks on smartphone touch screens," in USENIX 4th Workshop on Offensive Technologies, 2010.

[17] http://lear.inrialpes.fr/~jegou/data.php