Resisting Shoulder Surfing Attack Using Graphical Password

[1]Mayuri Gawandi, [2]Saloni Pate, [3]Snehal Pokharkar , [4]Prof. S. K. Said

BE Computer, Department of Computer Engineering,
Jaihind College of Engineering, Kuran , Pune, India

Abstract— **Authentication is required every time in order to protect users' digital property, they try to access their personal account and data. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Graphical passwords effectively used in authentication system to prevent unauthorized access to mobile device. The security of these mobile devices is decreased by shoulder surfing, it refer to direct observation techniques someone's shoulder to get information. Therefore, an authentication scheme should be designed to overcome these problems.**

In this system, we present a secure novel authentication system uses pair based techniques and PassMatrix prototype for web application that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time login indicators. PassMatrix is considered a novel and easy-to-use graphical password authentication system, which can effectively improve shoulder-surfing attacks. Most of the traditional authentication system has certain drawbacks for that reason graphical password base systems are most preferable authentication system where users click on images to authenticate themselves. Experimental result show that, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

***Keywords*— Authentication,Graphical Passwords, PassMatrix, Shoulder Surfing.**

I. Introduction

Authentication is very important in computer security and privacy. For providing security textual password have been most widely used these textual password are collection of numbers and alphabets these are strong enough to resist against shoulder surfing attack. However difficult textual password is hard to memorize and recollect[17]. The shoulder surfing attack can be performed by unauthorized person to obtain the user's password by watching over the user's shoulder as he enters his password. As conventional password schemes are easily detected by attacker. For Example Each time when user withdraws money from an ATM, he types the sequence of identical four-digit PIN number. Anyone who see this four-digit PIN e.g., by looking over the shoulder of a user, he can easily remember the PIN. In combination with stolen or skimmed material such as magnetic stripe cards, account numbers printed on receipts, criminals easily gain access e.g., to a victimized user's bank account services.

In order to protect users' digital property, authentication is required every time they try to access their personal account and data. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Even a more complex password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to validate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones or google glass. To overcome this problem, we proposed a shoulder surfing resistant authentication system based on graphical passwords, named PassMatrix and PairBased. Using a one-time login indicator per image, users can point out the location of their pass-square without directly clicking or touching it, which is an action vulnerable to shoulder surfing attacks. Because of the design of the horizontal and vertical bars that cover the entire pass image, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account.

Using graphical password user clicks on image to authenticate themselves rather than alphanumeric string. These graphical passwords are expected to be more robust than text-based passwords. Several studies have shown that humans remember images more easily compared to textual password. Different graphical password schemes [5],[10] were developed to address the vulnerability with textual password. Based on some research[14], [15] human have a better ability to remember images easily rather than textual or alphanumeric password. Graphical passwords hope to leverage visual information and in turn make it easier for users to select more secure passwords.

i. Authentication is the process to provide access to users to use particular system and resources.
ii. There are many authentication schemes in the current state like Token based authentication, Biometric based authentication, Knowledge based authentication.
iii. The traditional approach used for authentication is entering the user name and passwords. The textual passwords are short and they are easy to memorize and are predictable or if textual passwords are long then it is hard to memorize.
iv. In this system also we focus on a knowledge based approach using images as passwords
v. Graphical passwords have been proposed as a suitable alternative to text based password schemes, as it is possible for human to remember images better than text.

The main problem with existing system is it can be suffer by various attacks such as

1. Shoulder surfing attack
2. Dictionary attack
3. Bruit Force attack Etc.

To overcome all the problems of the existing system we have proposed novel approach of multilevel security.

Shoulder Surfing Attack:

Although we know the fact that shoulder surfing has been a real threat to authentication systems with either textual or graphical passwords, A number of novel authentication schemes were proposed to protect systems from this attack. Unfortunately, most of them were unsuccessful to find threat if the shoulder-surfing attack is camera-based. For instance, some schemes such as PIN-entry method and spyresistant keyboard were designed on the basis of short-term memory. Camera-based shoulder surfing attacks are used to crack the passwords of these schemes.

II. PROBLEM STATEMENT

To design and develop a system which uses novel authentication techniques Pair based & graphical password based on a concept of pass matrix to resist shoulder surfing attack.

III. MOTIVATION

Now a days we are using online transaction of money for the different purpose. The most commonly we use the ATM machine for this purpose for withdrawal of money. So we required the password for this purpose but now days shoulder surfing attacks are happen . The previous password schemes are most affected by shoulder surfing. We have proposed the graphical password scheme for resisting the shoulder surfing attack. This scheme provides high level of security and minimizes the possibility of happening the shoulder surfing attack.

- Shoulder surfing attack can be a happened on a mobile users privacy and confidentiality as number of mobile devices increased now a days.People may use different web services and apps in public areas to access their personal accounts on smart phones, tablets or public devices, like bank ATM.
- Attackers can observe how the user is entering the passwords with the help of reflecting glass windows, or video capturing in public places.Even if the password is complex, it can be exposed.Therefore a secure authentication scheme need to be develope for protecting a users privacy.
- Previous schemes also have the limitation of usability which contain different issues such as taking more time to log in, passwords being too difficult to recall after a period of time.
- Hence the main motive behind designing this system is to provide the higher level of security by maintaining the usability.

IV. OBJECTIVE

Authentication processes to keep information secure.

1. To secure user identity.
2. To protects users from becoming victims of shoulder surfing attacks.
3. To make a system will be applicable to all kinds of devices.
4. To achieves better resistance to shoulder surfing attacks while maintaining usability.
5. The existing 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 distracters to develop our PassMatrix authentication system that is resistant to shoulder surfing attacks.

V. PROPOSED SYSTEM

We proposed a system in which we done pair based techniques in which Key Pair can be used instead of passwords for authentication. We present a secure graphical authentication system named PassMatrix[1] by using number of images that protects users from becoming 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. The existing 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 distracters to develop our PassMatrix authentication system that is resistant to shoulder surfing attacks.

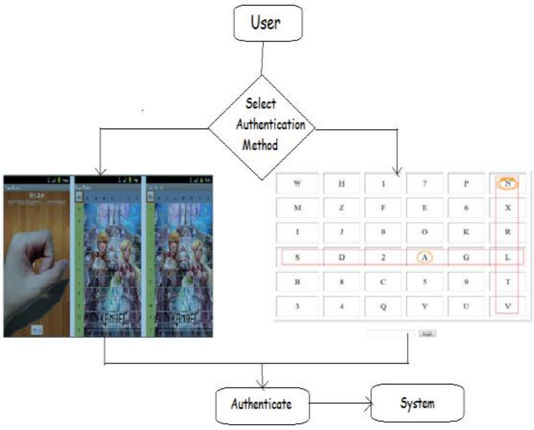


Fig.System Architectrure

Pass Matrix

In this system we divide image into blocks is known as pass matrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the Pass
Points scheme. Advantage of this is to secure login system for personal use of accounts. Limited usability of authentication schemes that can be applicable to some devices only.

Pair Based

8x8 matrix is used to represent alphabets, digits and special symbols to the user so user has to select session password by using grid. E.g. Length of the password is 8 and password is
ABCDEQRS. Now we will make pairs as AB CD EQ RS .so the session password length is 4. We will select row containing character A and column containing character B. And intersection of that row and column is inserted into the password field likewise all the pairs are selected into the grid and password is entered. This new password is valid only for that session and is stored in the user log on server. The session password and 8x8 grids is sent to the server. On the server side this session password is cross checked with the user's original password.

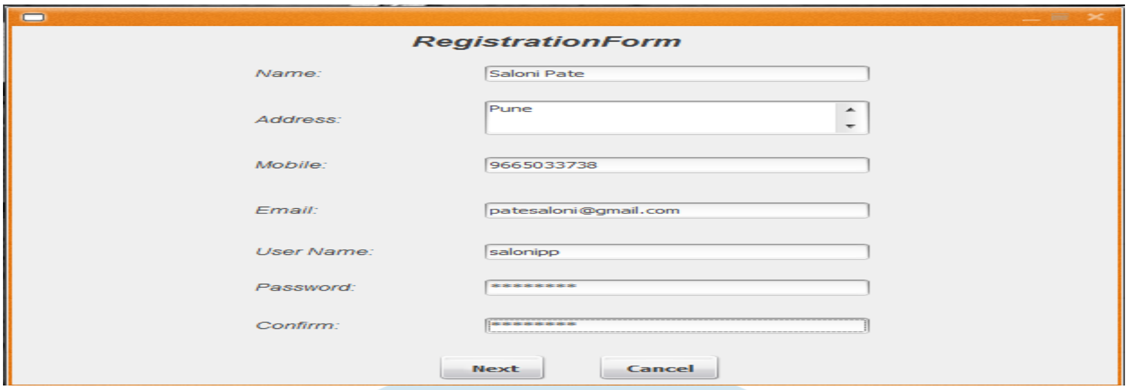
VI. SYSTEM MODULES

1. Image Descretization: First step is module divides each image into squares,from which users would choose one as the pass-square. Segmentation of image is perform by system.
2. Login Indicator: This module generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual materials (such as colors and icons) for users during the authentication phase.
3. 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. The bars are used to implicitly point out (or in other words, align the login indicator to) the location of the users pass-square.
4. 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 and thus, is safe from being eavesdropped and intercepted.
5. Password Verification: 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 authentication 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 passsquare will be described in the next section.
6. 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. Pass Matrix has all the required privileges to perform operations like insert, modify, delete and search.

VII. RESULT ANALYSIS

By studying these two techniques we get information that according to "time to login",the pair based textual authentication scheme is better the an color code authentication scheme, but according to more security e.g. If we are using this proposed system in banking for password of account, then color code based authentication scheme is better than pair based authentication scheme. Both scheme i.e. pair based textual authentication scheme and color co de based authentication scheme are good. The following table shows comparison with existing system.

User Registration



RegistrationForm

Name: Saloni Pate

Address: Pune

Mobile: 9665033738

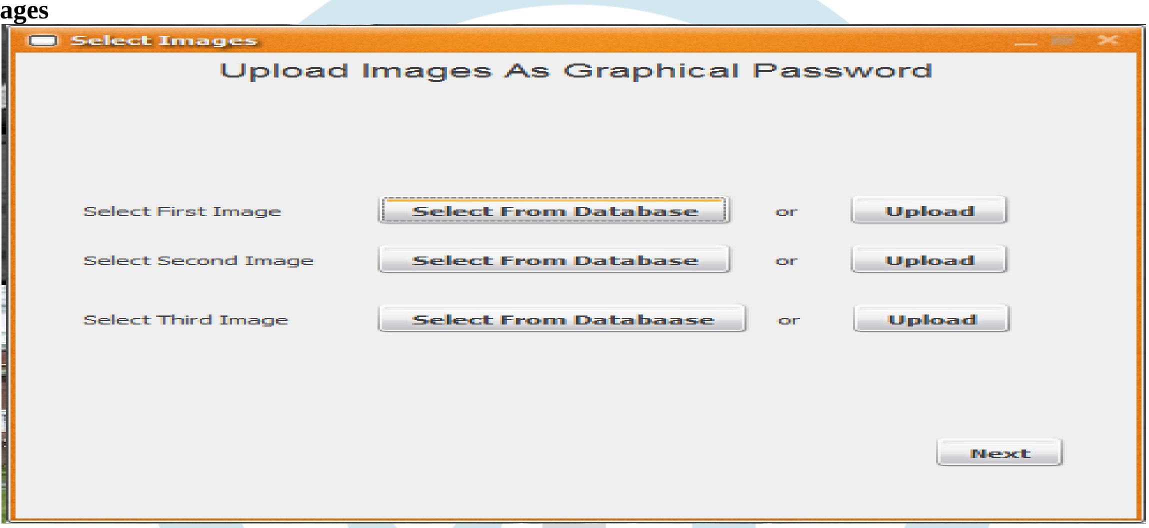
Email: patesaloni@gmail.com

User Name: salonipp

Password: *********

Confirm: *********

Upload Images



Select Images

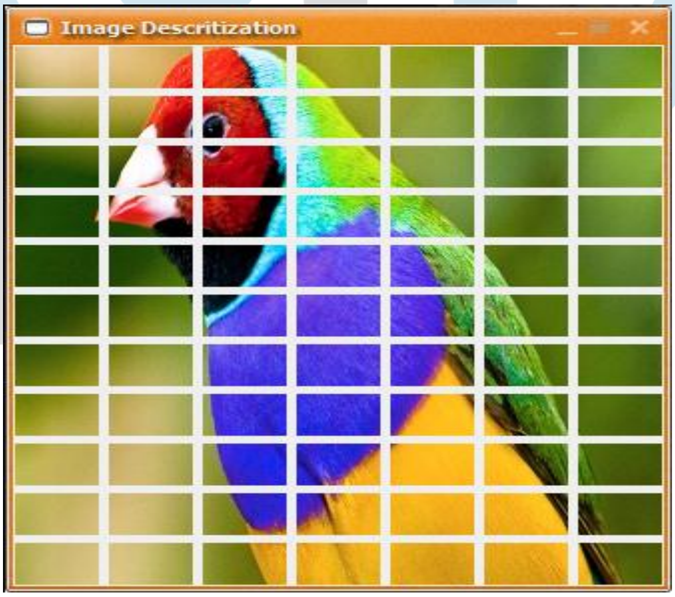
Upload Images As Graphical Password

Select First Image

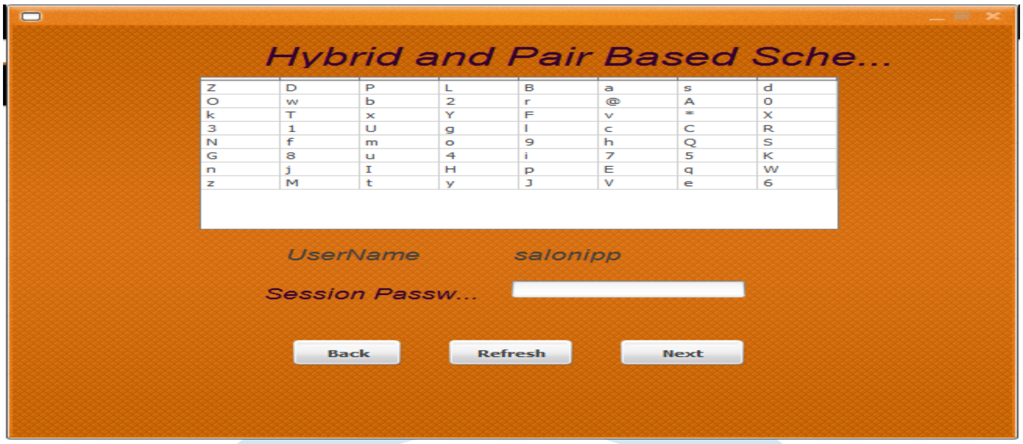
Select Second Image

Select Third Image

Image Descritization



Pair Base Login



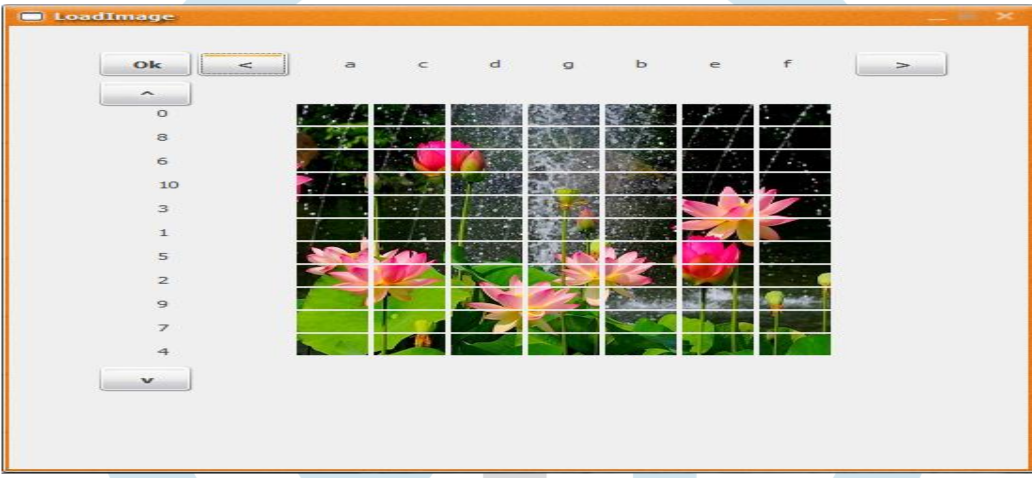
Hybrid and Pair Based Sche...

Z	D	P	L	B	a	s	d
O	w	b	2	r	@	A	0
k	T	x	Y	F	v	*	X
3	1	U	g	l	c	C	R
N	f	m	o	9	h	Q	S
G	8	u	4	i	7	5	K
n	j	I	H	p	E	q	W
z	M	t	y	J	V	e	6

UserName salonipp

Session Passw...

PassMatrix Login



VIII. CONCLUSION AND FUTURE SCOPE

In this system we are going to implement graphical password authentication scheme. We are going to develop a shoulder surfing resistant authentication system based on graphical passwords, named PassMatrix and PairBase technique. Using a one-time login indicator per image, users can point out the location of their pass-square without directly clicking or touching it, which is an action vulnerable to shoulder surfing attacks. Because of the design of the horizontal and vertical bars that cover the entire pass-image, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account. In PairBase we will generate the session password. Furthermore, we will test our system to evaluate memorability and usability.

In proposed system image grids are constant at particular location which leads to password guessing attack, so to overcome this limitation in future images grids are varied also numbers are varied this will be difficult to guess.

REFERENCES

[1]. “A Shoulder Surfing Resistant Graphical Authentication System”,Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng,2016

[2]. Bin B.Zhu, Jeff Yan,Gunabo Bao,Maowei Yangand Ning Xu, “Captcha as Graphical Password-A new Security Approach Based on Hard AI Problems", IEEE,June 2014.

[3]. David Kim, Paul Dunphy, and Pam Briggs, “A Shoulder Surfing Resistant Visual Authentication Scheme,” (Volume:PP , Issue: 99), April 10-15, 2010.

[4]. R.Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Comput. Surveys, vol. 44, no. 4, 2012.

[5]. 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.

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

[7]. 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.

[8]. B. Hartanto, B. Santoso, and S. Welly, “The usage of graphical password as a replacement to the alphanumerical password,” Informatika, vol. 7, no. 2, 2006, pp. 91-97.

[9]. S. Man, D. Hong, and M. Mathews, “A shoulder surfing resistant graphical password scheme,” Proc. of the 2003 Int.Conf. on Security and Management, June 2003, pp. 105-111 .

[10]. “Realuser,” http://www.realuser.com/.

[11]. Z. Zheng, X. Liu, L. Yin, and Z. Liu, “A stroke-based textual password authentication scheme,” Proc. of the FirstInt. Workshop.on Education Technology and ComputerScience, Mar. 2009, pp. 90-95.

[12]. T. Yamamoto, Y. Kojima, and M. Nishigaki, “A shoulder surfing-resistant image-based authentication system with temporal indirect image selection,” Proc. of the 2009 Int.Conf. on Security and Management, July 2009, pp. 188- 194.

[13]. H. Zhao and X. Li, “S3PAS: A scalable shoulder -surfing resistant textual-graphical password authentication scheme,” Proc. of 21st Int. Conf. on Advanced InformationNetworking and Applications Workshops, vol. 2, May 2007, pp. 467-472.

[14]. AA. Paivio, T. Rogers, and P. Smythe, “Why are pictures easier to recall than words?” Psychonomic Science, 1968.

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

[16]. S. H. Kim, J. W. Kim, S. Y. Kim, and H.G. Cho. “A new shoulder-surfing resistant password for mobile environments,” Proc. of 5th Int. Conf. on Ubiquitous Information Management and Communication, Feb. 2011.

[17].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.