ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Combination of PassMatrix with Improved AES for securing Text and Image Passwords

S.V. Jinisha[1], R. Kalaiselvi[2],

II Year ME CSE, Noorul Islam Centre For Higher Education, Kumaracoil, K.K District, Tamil Nadu, India[1]

Associate Professor, Noorul Islam Centre For Higher Education, Kumaracoil, K.K District, Tamil Nadu, India[2]

ABSTRACT: Security is one of the main area to protect data and other information from unauthorized access. The proposed system is applied based on two-way authentication techniques. Two-way authentication techniques are used to protect the data by using the text and graphical passwords. The Graphical password scheme is named as PassMatrix. In the text as well as graphical password, Improved Advanced Encryption Standard (IAES) algorithm is applied to provide better security. It means the system provides two-step authentications with the encryption technique. In IAES, one random generated key is called as SALT, is added with the AES key. By adding the Salt key with AES the number of combinations of attack will increase. Even if the database is compromised the attacker cannot gain the actual text password and PassMatrix of the graphical password. PassMatrix is used to resist shoulder surfing attacks. It protects users from shoulder surfing attacks by inputting passwords through the usage of one-time login indicators. A login indicator is randomly generated for each pass-image and not at all useless after the session terminates. Next, pass-image has been 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 moves the bars to align the pre-selected pass-square of the image with the login indicator. Finally, for each image, the password verifies the alignment between the pass square and the login indicator. Shoulder surfing attacks and dictionary attacks are removed totally.

KEYWORDS: Graphical Passwords, Authentication, Shoulder Surfing Attack.

I.INTRODUCTION

Textual passwords have become the most widely used authentication method for decades. Comprised of numbers upper and lower case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect[1]. Even worse, it is not a rare case that users may use only one user name and password for multiple accounts[2]. Various graphical password authentication schemes [4], [5], [6], [7] were developed to address the problems and weaknesses associated with textual passwords. Image-based passwords were proved to be easier to recollect in several user studies [10], [11], [12]. However, most of these image-based passwords are vulnerable to Shoulder Surfing Attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information [13], [14],[15].

This paper provides a secure graphical authentication system named as PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time login

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

indicators. A login indicator is randomly generated for each pass-image and will useless after the session terminates. The login indicator provides better security against shoulder surfing attacks.

1.1 Motivation

Shoulder surfing attacks have posed a great threat to user's privacy and confidentiality as mobile devices are becoming indispensable in modern life. People may log into web services and apps in public to access their personal accounts with their smartphones, 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. 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 is too complicated for users without proper education and practice.

II.BACKGROUND AND RELATED WORK

In the early days, the graphical capability of handheld devices was weak, the color and pixel it could show was limited. Under this limitation, the Draw-a-Secret(DAS)[6]technique was proposed by Jermyn et al. in 1999, where the user is required to re-draw a pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. Using the PassPoint scheme, the user has to click on a set of pre-defined pixels on the predestined photo, as shown in Figure 1(a), with a correct sequence and within their tolerant squares during the login stage. This authentication system is based on features that are extracted from the dynamics of the gesture drawing process.

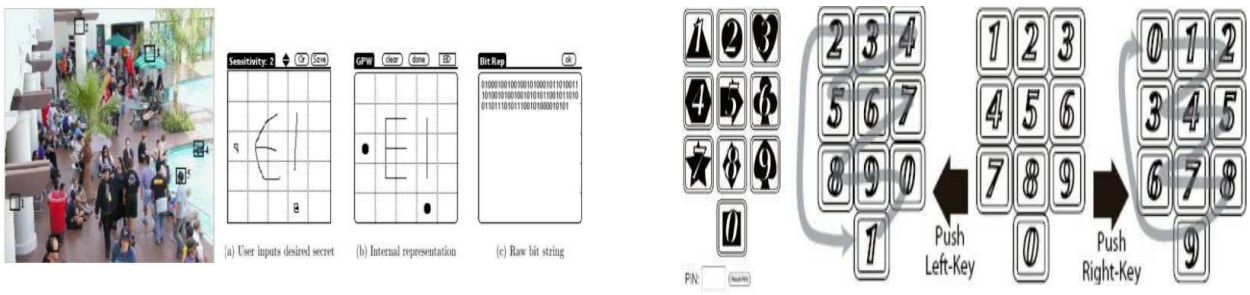


Figure 1. (a) Pixel squares selected by users as authentication passwords in PassPoints [7]. (b) Authentication password drew by users and the raw bits recorded by the system database[6].

In addition to graphical authentication schemes, there was some research on the extension of conventional personal identification number (PIN) entry authentication systems. In 2004, Roth et al. [34] presented an approach for PIN entry against shoulder surfing attacks by increasing the noise to observers. In their approach, the PIN digits are displayed in either black or white randomly in each round. The user must respond to the system by identifying the color for each password digit. After the user has made a series of binary choices (black or white), the system can figure out the PIN number the user intended to enter by intersecting the user's choices. This approach could confuse the observers if they just watch the screen without any help of video capturing devices. However, if observers can capture the whole authentication process, the passwords can be cracked easily. In addition to graphical authentication schemes, there was some research on the extension of conventional personal identification number (PIN) entry authentication systems. In 2004, Roth et al. [34] presented an approach for PIN entry against shoulder surfing attacks by increasing the noise to observers. In their approach, the PIN digits are displayed in either black or

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

white randomly in each round. The user must respond to the system by identifying the color for each password digit. After the user has made a series of binary choices (black or white), the system can figure out the PIN the user intended to enter by intersecting the user's choices. This approach could confuse the observers if they just watch the screen without any help of video capturing devices. However, if observers can capture the whole authentication process, the passwords can be cracked easily.

This scheme is resistant to shoulder surfing attacks using a convex hull method. The user needs to recognize a set of pass-icons on the screen and clicks inside the convex hull formed by all these pass-icons. To make the password hard to guess, a large number of other different icons are inserted into the screen to increase the password space.

In 2010, David Kim et al. [25] proposed a visual authentication scheme for tabletop interfaces called "Color Rings", where the user is assigned *i* authentication (key) icons, which are collectively assigned one of the four color-rings: red, green, blue, or pink. During login, *i* grids of icons are provided, with 72 icons being displayed per grid. There is only one key icon presented in each grid. The user must drag all four rings (ideally with index finger and thumb from two hands) concurrently and place them in the grid. The distinct key icon should be captured by the correct color ring while the rest of the rings just make decoy selections. The user confirms a selection by dropping the rings in position. The rings are large enough to include more than one icon and can thus obfuscate the direct observer. Unfortunately, these kinds of passwords can be cracked by intersecting the user's selections in each login because the color of the assigned ring is fixed and a ring can include at most seven icons. Thus, the attacker only requires a limited number of trials to guess the user's password.

Figure 3. (a) Color Rings method [25]. (b) Convex Hull method [36].

III.PROBLEM STATEMENT, ATTACK MODELAND ASSUMPTIONS

3.1Problem Statement

With the increasing amount of mobile devices and web services, users can access their personal accounts to send confidential business emails, upload photos to albums in the cloud or remit money from their e-bank accounts anytime and anywhere. While logging into these services in public, they may expose their passwords to unknown parties un-consciously.

3.1.1. Shoulder Surfing Attacks

Based on previous research [20], [21], [25],[34],[35], users' actions such as typing from their keyboard, or clicking on the pass-images or pass-points in public may reveal their passwords to people with bad intention. In this paper, based on the means the attackers use, we categorize shoulder-surfing attacks into three types as below:

1) Type-I: Naked eyes.
2) Type-II: Video captures the entire authentication process only once.
3) Type-III: Video captures the entire authentication process more than once.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

IV.PASSMATRIX

To overcome (1) the security weakness of the traditional PIN method, (2) the easiness of obtaining passwords by observers in public, and (3) the compatibility issues with devices, we introduced a graphical authentication system called PassMatrix. In PassMatrix, a password consists of only one PassSquare per pass-image and for a sequence of *n* images.

In PassMatrix, users choose one square per image for a sequence of *n* images rather than *n* squares in one image as that in the PassPoints[7]scheme. The CCP method does a good job of helping users recollect and remember their passwords. If the user clicks on an incorrect region within the image, a different image will show to give the user a warning feedback. However, aiming at alleviating shoulder surfing attacks, we do not recommend this approach since the feedback that is given to users might also be obtained by attackers.

PassMatrix is composed of the following components:

- Image Discretization Module
- Registration module
- Improved AES encryption
- Horizontal and Vertical Axis Control Module
- Password Verification Module

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 x 11 grid.

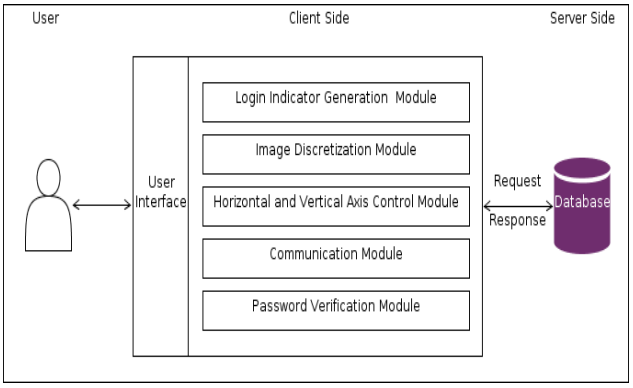


Figure 4. Overview of the PassMatrix system.

Registration Module:

In the registration phase , the password consists of only one PassSquare per images for a sequence of n images. Increase in number of images is considering the trade off between security and usability of the system. The user can choose images from a provided list or upload images from their device as pass-images. Then the user will pick a PassSquare for each selected pass-image from the grid using discretization module.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Improved AES Encryption:

The concept of salt key is used in AES to improve the performance of the encryption and decryption. Improved AES, system uses the 128 bits key and plain text. The salt key is used to enhance the combinations of the passwords. In first, plain text and salt key are concatenated together and then XOR is performed with new plain text and key.At the end, cipher text will be generated and at decryption reverse in order process is done.

Horizontal and Vertical axis control module:

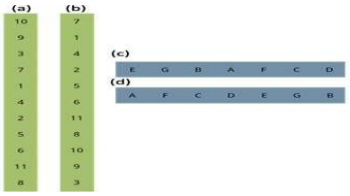


Figure 5. Horizontal and Vertical axis control module

There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with sequence of numbers. This control module provides fling functions for users to control both bars. Users can fling either bars using the button to shift one alphanumeric at a time. The bars are used to implicitly point out the location of the user's pass-square.

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.

V.IMPROVED ADVANCED ENCRYPTION STANDARD

IAES Algorithm is applied on the click points to remove the shoulder surfing attack and to provide the security on the click points of the user's password .the IAES encryption is applied in the text as well as image password .it means user's can be stored securely into the database. The Final registration process is the combination of all the four steps and the final registration process is completed after the successful completion of all four processes.

AES is one of the successful and strongest encryption algorithm. The concept of salt key is used in AES to improve the performance of the encryption and decryption. In AES symmetric key cryptography is used, symmetric-key cryptography used as the same key for both encryption and decryption. The key data for AES id 128 bits /192 bits/256 bits with the round of size 10,12,14 respectively. The size of the key is also the same, as the size of the data of AES. In this system, AES 128 bits are used with the improved features of AES. For enhancement in AES, the salt key is added with the AES key so the possible combinations of passwords are enhanced. IAES is used for encrypting text as well as graphical passwords of the users.

Salt key is used in an improved AES. A salt is random data that is used as an additional input to a one-way function that hashes a password. The primary function of salt is to defend against dictionary attacks versus a list of password hashes and pre-computed rainbow attacks. A new salt is randomly generated for each password. In a typical way, the salt and the password are processed and concatenated with a cryptographic hash function and the resulting output is stored with the salt in a database. For later authentication hashing permits while defending against compromise of the plain text password if the database is somehow compromised.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

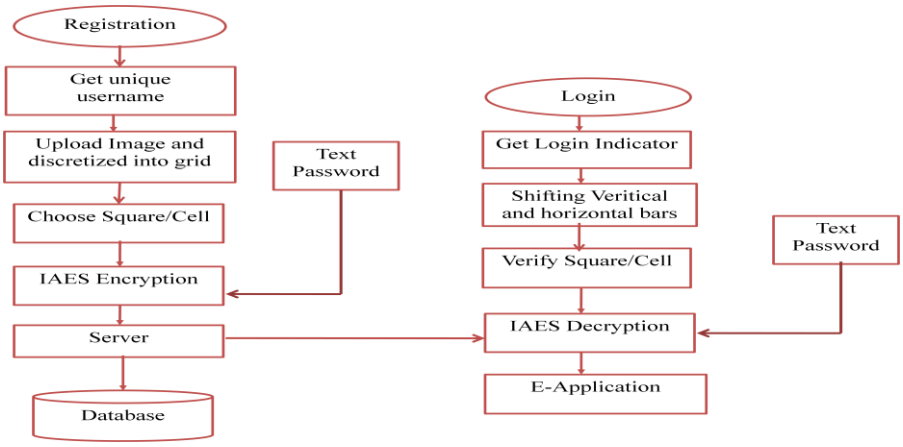


Figure 8. Block Diagram representation of proposed Architecture.

VI.IMPLEMENTATION AND USER STUDY

Although the PassMatrix prototype was implemented on an Android system that has a small screen, it is not limited to the applications on small screen devices, for example, screen locking.

6.1 Implementation

The PassMatrix prototype was built with Android SDK 2.3.3 since it was the mainstream version of the distribution in 2012[45]. After connecting to the Internet, users can register an account, log in a few times in practice mode, and then log in for the experiment with a client's device. In the client-side of our prototype, we used XML to build the user interface and used JAVA and Android API to implement functions, including username checking, pass- images listing, image discretization, pass-squares selection, login indicator delivery, and the horizontal and vertical bars circulation.

6.2 User Study

In this section, we introduce our user study experimental design, environment, participants and the detailed procedure that evaluates the accuracy and usability of PassMatrix.

All participants are either in Computer Science, Information System Management or other information technology majors. 76.67% of them have a background in information security. As Figure 13(b) shows, 73 % of participants have less than one year or no experience at all of using smart phones, whereas 20% of participants have more than one but less than two years of experience and the final 7% are veteran users with more than two years of experience. The survey showed that in the past, they went through authentication processes on an average of 12.6 times a day in public.

VII.COLLECTED RESULTS

We analyzed the collected data from our experiments and surveys to evaluate the effectiveness of the proposed system. The results are presented in two perspectives: accuracy and usability. The accuracy perspective focuses on the successful 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

7.1 Accuracy

In the practice phase of the first session, participants practiced the login process on an average of 4 times ranging from 1 to 14

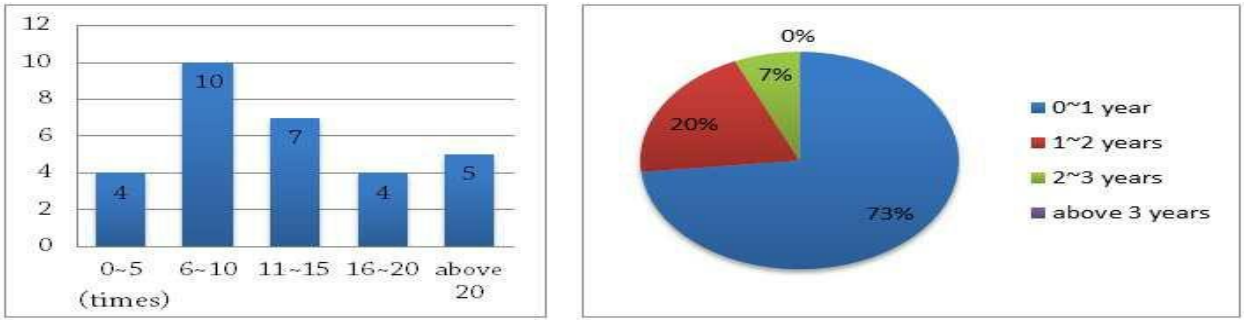


Figure 9. Trends of (a) Number of times a participant went through authentication processes in public per day, and (b) User experience in smartphones with touch screens. (excluding one outlier) and then moved onto the authentication (login) phase. As we defined in the previous section, participants can 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, can pass the authentication with a correct password. If all six tries failed, this attempt will be marked as a failure. Below, we define two terms First Accuracy and Total Accuracy that was used in our experiment:

$$\text{First Accuracy} = \frac{\text{Successful attempts in first try}}{\text{Total attempts}} \quad (1)$$

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

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 outof30(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 for the big drop in the First Accuracy and also analyzed those failed login attempts in the second session.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

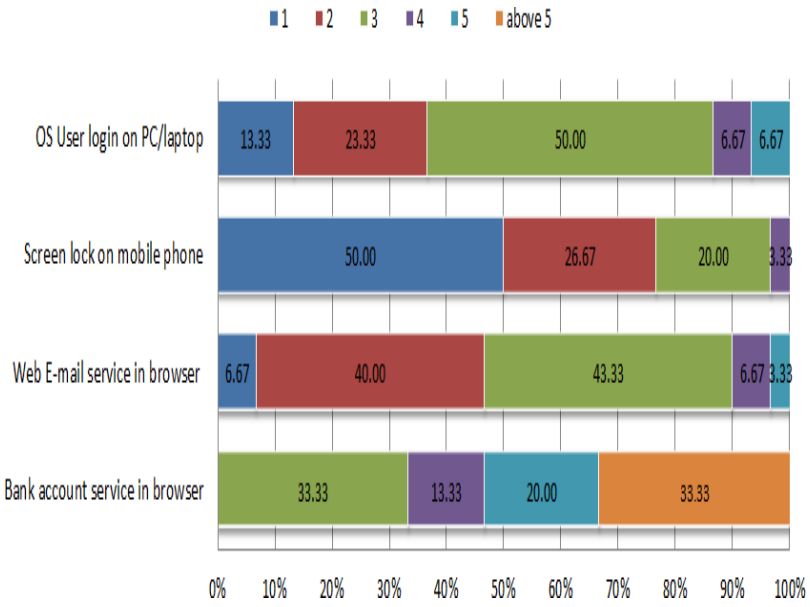


TABLE 2
The mean, median and standard deviation of the number of retries in a successful attempt.

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

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.

7.2 Usability

The number of shifts and the elapsed time per pass-image in our experiment to measure the usability of 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 not time-consuming and 10% of them said that they spent most of their

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

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.

VIII.COMPARISON OF PASSMATRIX AND PASSMATRIX+IAES TECHNIQUES

Method/Time(ms)	Create Time	Login Time	Confirm Time
PassMatrix	6.5	8.2	8
PassMatrix+IAES	6	7.8	7.6

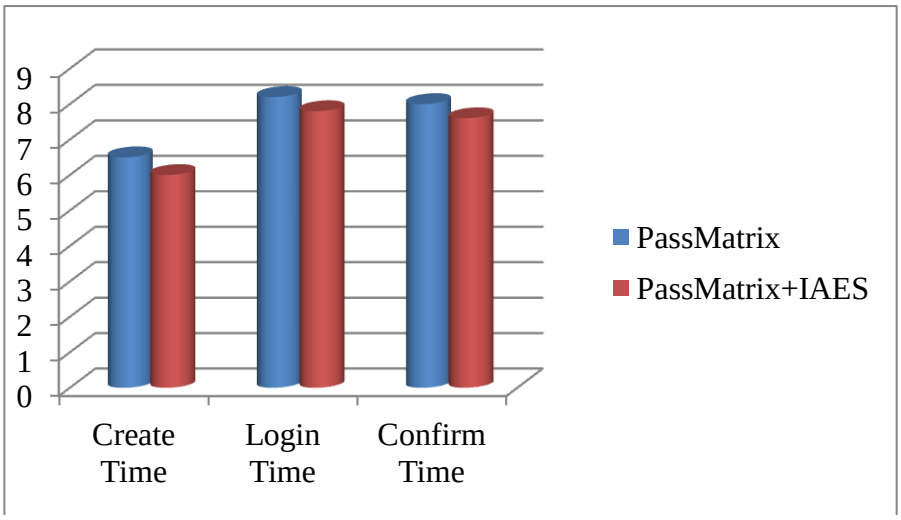


Figure 10. Number of pass-images users may accept in different authentication scenarios.

Security Level

No. Of Passwords	**Security Level (in %)**	
	PassMatrix +IAES	**PassMatrix**
1	40	35
2	55	42
3	60	49
4	72	58
5	76	65
6	85	72
7	90	78

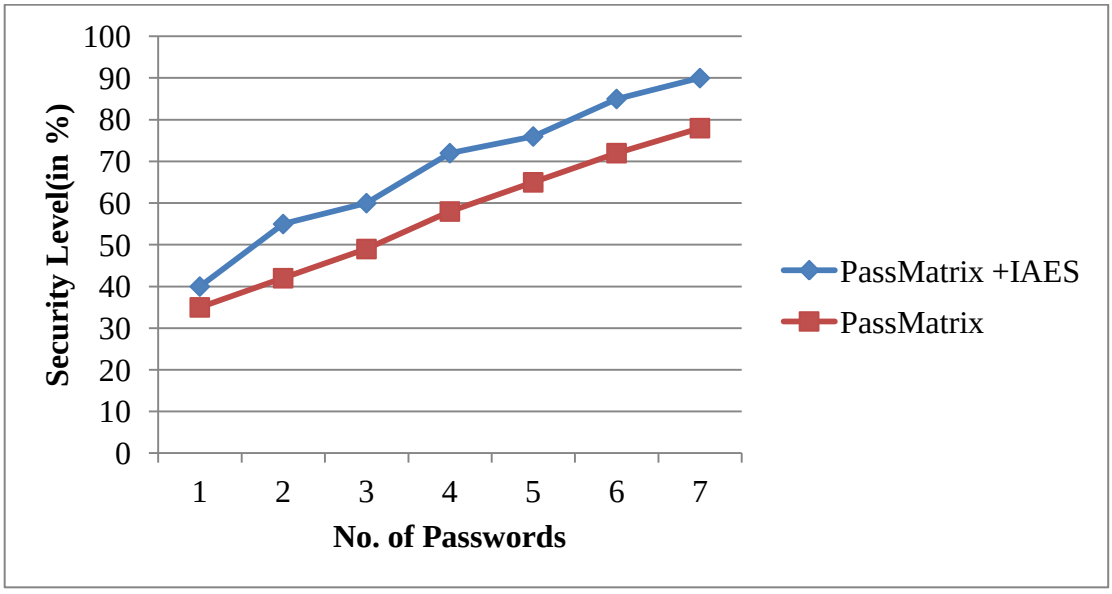
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020



IX.CONCLUSION

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. To protect user's digital property, authentication is required every time they try to access the accounts 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 traditional textual passwords or PIN methods, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over the shoulder or uses video recording devices such as cell phones.

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

The experimental result showed that users can log into the system with an average of 1.64 tries (Median=1), and the Total Accuracy of all login trials is 93.33% even two weeks after registration. The total time consumed to log into PassMatrix with an average of 3.2 pass-images is between 31.31 and 37.11 seconds and is considered acceptable by 83.33% of participants in our user study.

Based on the experimental results and survey data, PassMatrix is a novel and easy-to-use graphical password authentication system, which can effectively alleviate shoulder-surfing attacks. Also besides, PassMatrix can be applied to any authentication scenario and device with simple input and output capabilities.

By adding the features of PassMatrix with Improved Advanced Encryption Standard achieves better results in an authentication system as compare to PassMatrix & Advanced Encryption Standard Graphical authentication scheme is better to remember for the user. As the user has to choose only one image for the authentication purpose it is easier for the user to remember and difficult for the attacker to attack because it is difficult for the attacker to see at click points area of image.

In the future scope of this system, providing two ways for the image selection by the users so one more new option can provide to the users to use webcam to capture pictures at the time of registration.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

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, "Grasphical 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 Sbusiness," *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 designandanalysisofgraphicalpasswords,"in*Proceedingsofthe 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] 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.

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

[13] 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.

[14] 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.