Regular Article

Multi-level Scalable Textual-Graphical Password Authentication Scheme for Web based Applications

Umedha Behl, Divya Bhat, Neha Ubhaykar, Vaibhav Godbole, Saurabh Kulkarni

Department of Information Technology, Fr. Conceicao Rodrigues College of Engineering, Bandra (W), Mumbai: 400050, India

Correspondence: Vaibhav Godbole, vai.godbole@gmail.com

Manuscript communication: received 15 December 2013, accepted 17 March 2014

Abstract– **Nowadays, user authentication is one of the important topics in information security. Authentication is necessary in multi-user systems. User name and password are used to authenticate a user. Text-based strong password scheme can provide security to a certain degree. Users tend to pick short passwords or passwords that are easy to remember, which makes the passwords vulnerable for attackers to break. Furthermore, textual password is vulnerable to shoulder-surfing, hidden camera and spy-ware attacks. Graphical authentication has been proposed as a possible alternative solution to text-based authentication, motivated particularly by the fact that humans can remember images better than text. However, they are mostly vulnerable to shoulder surfing. In this paper, we propose a Multi-level Scalable Textual-Graphical Password Authentication Scheme for web based applications. This scheme integrates both graphical and textual password schemes, and provides multi-level authentication scheme as compared to previously proposed single level scheme. In this scheme multi-level authentication is obtained by making use of SMS service, hence provides more secure service. This scheme shows significant potential bridging the gap between conventional textual password and graphical password. Further enhancements of this scheme are proposed and briefly discussed.**

Keywords– **Multi-level authentication, multi-level security, SMS based security, intrusion prevention, shape based authentication.**

This work was supported by Fr. Conceicao Rodrigues College of Engineering.

1 Introduction

In the age of faceless e-commerce, Authentication provides crucial on line identity. The most simplest use of authentication is to validate users while accessing ATMs and email accounts. It involves confirming the identity of a person or software program. We use passwords for this purpose. In modern times, user names and passwords are commonly used by people during a log in process that control access to protected computer operating systems, mobile phones, cable TV decoders, ATM , etc. A typical computer user has passwords for many purposes: logging in to accounts, retrieving e-mail, accessing applications, databases, networks, web sites, and even reading the morning newspaper on line. Human brain has the remarkable ability of remembering things that it sees than abstract things like sequence of letters. This is true with passwords that contain sequence of letters and is evident from number of times we forget our passwords. The authentication system that is in use today is more convenient for machine than human beings. If we use an image related password then clearly it will be easy to remember [1].

A graphical password [2] is an authentication system that works by having the user select from images, in a specific order, presented in a Graphical User Interface (GUI). For this reason, the graphical-password approach is sometimes called Graphical User Authentication (GUA). Graphical passwords although less common are known to all. However,for sake of convenience in remembering textual passwords users generally tend to overlook their benefits. They tend to pick short passwords which makes passwords vulnerable to attacks [3]. Furthermore textual passwords [4] are prone to shoulder surfing, hidden camera and spy-ware attacks [5]. Graphical Password schemes have been proposed as an alternative to textual passwords, motivated partially by the fact that humans can remember pictures better than text [6]. Graphical passwords are particularly useful for systems that do not have keyboards. Graphical passwords allow users to click on certain areas of the screen that are then converted by the computer to be used for authentications. In addition, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably over higher level of security. It is also difficult to devise automated attacks for graphical passwords. As a result, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security. Due to these advantages, there is a growing interest in graphical password.

We propose to implement a Scalable Shoulder Surfing Resistant Textual Graphical Password Authentica-

tion System which has the following salient features:

- Shoulder-surfing, hidden-camera and spy-ware resistant. The secret cannot be stolen even when an attacker watches or camera-records the victim enter the password.
- It is immune to brute-force attacks through dynamic and volatile session passwords.
- It supports both keyboard and mouse as input devices.
- A 5 letter length password which can provide more security than a longer password.
- It provides additional security by forcing user to enter captcha and a secret key supplied to him on the user's registered mobile.

2 Literature Review

Textual alpha-numeric passwords were first introduced in the 1960s as a solution to security issues that became evident as the first multi-user operating systems were being developed [7].

A graphical password scheme, in which a password is generated through asking the user to click on a graphic or an image provided by the system, is designed by Blonder [8]. When creating a password, the user is asked to choose four images of human faces from a face database as their own password. In the authentication stage, users must click on the approximate areas of those locations. This method is considered as a more convenient password scheme than textual scheme, for the image can help users to recall their own passwords. Wiedenbeck, et al. [9] extended the approach and proposed a system called "PassPoint". It allows users to click on any locations on the image to create the passwords. The system will calculate a tolerance around each pixel which has been chosen. The users must click within the tolerance of the chosen pixels.

"Passface" is a technique developed by Real User Corporation based on the assumption that people can recall human faces easier than other pictures [10]. The basic idea is as follows. The user is asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user is presented with a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies all the faces.

Jermyn, et al. [8] proposed a technique call "Draw a Secret" (DAS). This system allows users to create their own passwords by drawing something on a 2D grid. When a user finishes the drawing, the system stores the coordinates of the grids occupied by the picture. During authentication, users must re-draw the picture which had been created by them [11, 12]. The user will be authenticated if the drawing touches the same gird in the right order. The password space of this scheme is proved to be larger than the full text-based password space.

Thorpe and van Oorschot [13] analyzed the memorable password space of the DAS. Graphical dictionaries were introduced and possibilities of a brute-force attack using dictionaries are studied. They showed that a significant fraction of users will choose mirror symmetric password, since people recall symmetric images better than asymmetric images. Thorpe and van Oorschot [13] also studied the impact of password length and stroke-count as a complexity property of the DAS scheme. In order to improve the security, a "Grid Selection" technique is proposed. It allows users to select a rectangle region as the drawing grid, in which they may input the password. This method increases the DAS password space significantly.

To address the issues in textual and graphical password system, Huanyu Zhao and Xiaolin Li [5] have proposed a textual graphical password system, named scalable shoulder-surfing resistant textual-graphical password authentication system, which seamlessly integrates the textual and graphical passwords.

In this scheme to login, the user finds all his/her original pass characters in the login image and then make some clicks inside the invisible triangles which are called pass-triangles created by 3 original pass characters following a certain click-rule. Alternatively, the user can input/type a textual character chosen from inside or on the border of the pass-triangle area instead of clicking by mouse. Such character is called session pass-character. Therefore, the final inputs could be either several session pass-clicks or several session pass-characters. These session pass-clicks or session pass-characters is a users session passwords. There are two kinds of passwords in the authentication system proposed by [5], the original passwords and the session passwords. Users choose their original passwords when creating their accounts. In every login process, users input different session passwords so that they can protect their original passwords from releasing. The click-rule for single-set scheme is as follows.

In this scheme for the users password string k, the first character is numbered in k as k_1, the second k_2, the third k_3, etc. The remaining characters were numbered as $k_1, k_2, k_3, \ldots, k_{n-1}, k_n, n = |k|$. To login, users finds $k_1, k_2, k_3, \ldots, k_{n-1}, k_n$ in the login image. Then the first click must be inside the pass-triangle formed by $k_1, k_2 and k_3$. The second click must be inside the pass-triangle formed by $k_2, k_3 and k_4$. Recursively, the i^{th} click must be inside the pass-triangle formed by $k_{imod|k|}$, $k_{(i+1)mod|k|}$ and $k_{(i+1)mod|k|}$ $i = 1 \ldots n$. This is the "basic click-rule".

The drawback in the above system is that there is an ambiguity that users face in deciding the center character of the pass-triangle. As shown in Figure 1, the user may not be able to decide between 'x' , '2' and 'A'.

Chun-Shien Lu et al. [14] has described an Image Retrieval Authentication System as a computer system for browsing, searching and retrieving images from a large database of digital images. It uses a password system proposed by [5] where login image is generated locally specification of image (eg. icon in the image) is

v	~	4	f	0	y	q
!	a	o	t	)	b	7
p	/	x	2	k	3	#
+	e	A	d	%	@	l
s	6	i	5	g	z	9
&	1	r	w	8	c	u
(	j	*	h	m	?	$

Figure 1. Ambiguity in selecting center character of pass-triangle

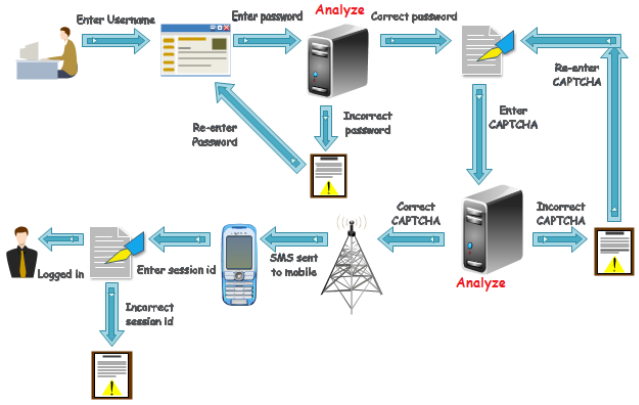


Figure 2. The work-flow of our password authentication system

transmitted instead of the entire image pixel by pixel from client to servers, which reduces authentication time and server overheads. It uses the same technique as explained above but instead of just alphabets, this system uses images which the users find easier to remember.

This problem can be overcome by our proposed system.

3 Our Proposed Scheme

Multi-level Scalable Textual-Graphical Password Authentication Scheme is designed to be used in client/server environments as most password authentication systems especially in systems that require high security to keep any confidential data secure, such as online banking sites. It is a textual-graphical password system which seamlessly integrates the textual and graphical passwords. It provides a way of making more human-friendly passwords while increasing the level of security. Algorithm 1 shows the algorithm for our proposed system and the Figure 2 shows the entire process of our password authentication system.

- We consider a large image which is actually a table consisting of alphabets, numbers and symbols. The alphabets are both in upper case as well as lower case. This large image is displayed to the user as a $9 \star 9$ grid containing the smaller images. Let us consider that all the available options of letters for making a password form a set T.
- There is a string k which is the users password containing a combination of alphabets, numbers and symbols previously chosen and memorized by the user, which is named as original password. The characters in k are called original pass-characters. Let $|k|$ denote the length of the users password k.
- Initially, the system randomly scatters the set T in the login image as shown in Figure 3.
- The user must find all his/her original pass-characters in the login image and then make some clicks inside the invisible squares which are called

Input: User name and a password
Output: Final login page

1: *Start*
2: **if** *User name exists in database* ***then***
3: *Go to step 7*
4: ***else***
5: *Go to step 2*
6: ***end if***
7: ***for*** $(i = 1, i \leq 3, i++)$ ***do***
8: ***if*** *password of length k entered by the user is correct* ***then***
9: *Go to step 15*
10: ***else***
11: *Go to step 7*
12: ***end if***
13: ***end for***
14: *Go to step 1*
15: *Generate display image*
16: ***for*** $(i = 1, i \leq \mid k \mid, i++)$ ***do***
17: *Enter session password*
18: ***if*** *Password is correct* ***then***
19: *Go to step 16*
20: ***else***
21: *Go to step 25*
22: ***end if***
23: ***end for***
24: *Go to step 31*
25: *Generate and display CAPTCHA*
26: ***if*** *CAPTCHA entered is correct* ***then***
27: *Go to step 1*
28: ***else***
29: *Go to step 1*
30: ***end if***
31: *Generate and display CAPTCHA*
32: ***if*** *CAPTCHA entered is correct* ***then***
33: *Go to step 37*
34: ***else***
35: *Go to step 1*
36: ***end if***
37: *Ask user to enter his mobile number*
38: *Send session id to this mobilw number via SMS*
39: ***if*** *The session id is correct* ***then***
40: *Go to step 44*
41: ***else***
42: *Go to step 1*
43: ***end if***
44: **Final login page**

Algorithm 1: Proposed System

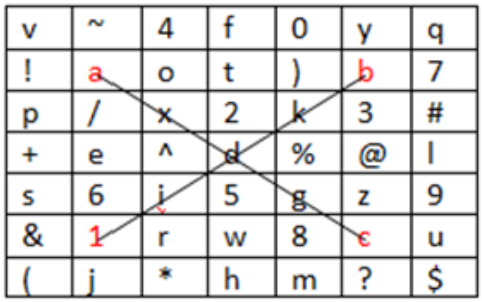


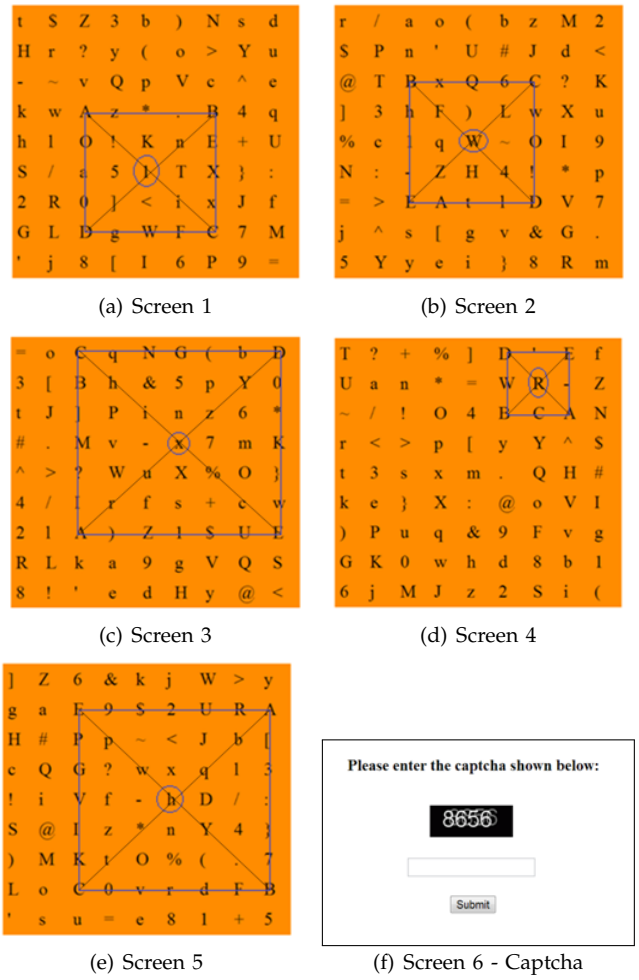
Figure 3. Table as seen in login image

pass-squares created by 4 original pass characters following a certain click-rule. Alternatively, the user can input/type a textual character chosen from inside of the pass-square area instead of clicking by mouse. Such character is called session pass-character. Therefore, the final inputs could be either several session pass-clicks or several session pass-characters. These session pass-clicks or session pass-characters is a users session passwords.

- There are two kinds of passwords in the our system, the original passwords and the session passwords. Users choose their original passwords when creating their accounts. In every login process, users input different session passwords so that they can protect their original passwords from releasing.
- The click-rule for single-set scheme is as follows. For the users password string k, we number the first character in k as k_1, the second k_2, the third k_3, the fourth k_4 and the fifth k_5. To login, users have to find out k_1, k_2, k_3, k_4, k_5 in the different login images. The first click must be in the centre of the pass-square (pass-square will always be an odd-ordered matrix i.e. $3 \star 3$ or $5 \star 5$ or $7 \star 7$ or $9 \star 9$) formed by k_1, k_2, k_3 and k_4. The second click must be inside the pass-square formed by k_2, k_3, k_4 and k_5. The third click must be in the center of the pass-square formed by k_3, k_4, k_5 and k_1. The fourth click must be in the center of the pass-square formed by k_4, k_5, k_1 and k_2. The fifth click must be in the center of the pass-square formed by k_5, k_1, k_2 and k_3.
  To show the login process let us consider an example:

We assume that the user Alice's original password k is "ABCDE". Since the length of the password is, $|k| = 5$, based on the basic click-rule, Alice has to click five times correctly in the right sequence to be authenticated. The five combinations of password in order are "ABCD", "BCDE", "CDEA", "DEAB" and "EABC". The login procedure consists of the following five steps and is also shown in the figures below:

1) Alice finds her pass-characters "A", "B", "C" and "D", then clicks on the letter(session pass-character) in the centre of the pass-square or types that pass-character (e.g., "1") as shown in Figure 4(a).
2) Alice finds her pass-characters "B", "C", "D" and "E", then clicks on the session pass-character in the centre of the pass-square or types that pass-character (e.g., "W") as shown in Figure 4(b).
3) Alice finds her pass-characters "C", "D", "E" and "A", then clicks on the session pass-character in the centre of the pass-square or types that pass-character (e.g., "x") as shown in Figure 4(c).
4) Alice finds her pass-characters "D", "E", "A" and "B", then clicks on the session pass-character in the centre of the pass-square or types that pass-character (e.g., "R") as shown in Figure 4(d).
5) Alice finds her pass-characters "E", "A", "B" and "C", then clicks on the session pass-character in the centre of the pass-square or types that pass-character (e.g., "h") as shown in Figure 4(e).
6) These five screens are followed by CAPTCHA [15] which has to be correctly entered by the user.
7) A verification in the form of an SMS will be sent to the user on his mobile number which is retrieved from the database of the system. This SMS contains [16] a randomly generated session id which is also been stored in the database. We ask the user to enter this session id. This is the last stage of authentication and once the correct session id is entered the user is allowed to login. Now user can see final logged screen as shown in Figure 5.



(a) Screen 1 (b) Screen 2

(c) Screen 3 (d) Screen 4

(e) Screen 5 (f) Screen 6 - Captcha

Figure 4. Login Process

Figure 5. The final logged in screen

Table I
Login Time (seconds) for All Correct Inputs at Session 1

Type	Avg. time
Our system	25.2
Scheme proposed in [5]	38.7

4 Testing

4.1 Methodology

To discuss the usability of our proposed system we invited 20 students from our institute to our lab. They were in the age range of 20 to 30 and none of them were familiar with graphical password schemes. We compare the performance of password system proposed in [5] with our proposed system.

The participants select a password and form an image from their passwords using both types of authentication systems. After a short delay (about 5 minutes), all the participants should log in repeatedly until ten successful logins were achieved.

For each participant, the corresponding scheme was instrumented to collect data on the number of correct and incorrect logins and the time for each login.

Two separate tests were carried out to calculate the avg. time taken by the participants to mark triangle and square on the image. This test is carried out in 10 consecutive lab sessions and the average time is noted down.

4.2 Login

All participants achieved the criterion of ten correct logins. With the scheme proposed in [5] seven of the ten participants accomplished the criterion in ten attempts with no errors. With our system eight of ten participants accomplished the criteria in ten attempts with no errors. This means that success rate using the technique proposed in [5] was 70% and that of using our system is 80%.

The mean time for correct password inputs was also analyzed. As shown in Table I the participants took less time to log in with our system than that with the scheme proposed in [5].

It is observed that the participants took more time in selecting triangle on the image, since the participants found it difficult to select a triangle on the image in such a way that the character appears exactly at the center of the triangle. The participants took lesser time to select square on the image in such a way that the character appears exactly at the center of the square. The observations are shown in Table II

Table II
Time in Seconds to Pass 5 Images for a 5 Character Password

Type	Avg. time
Our scheme	5.0
Scheme proposed in [5]	10.2

5 Analysis and Discussion

In our scheme, users have to find out their pass-characters and then click inside the pass-square areas. However, attackers have the chance to click the right areas just by random-click even though they do not really know the password. This kind of attack is called "random-click attack".

To resist random-click attack, users are required to click several times followed by some click-rule just like the basic scheme proposed in [5]. As explained with an example in Section 3, if the password is "ABCDE", the user has to click five times to login. The problem is that whether five-character password is long enough to resist the random-click attack? If the attacker is "lucky" enough, he/she might be able to click inside the correct triangle regions correctly just by random-clicks. We observe that the size of the pass-square area greatly affects our system's security level. If the size of every pass-square area is too large, attackers are able to click inside the right areas with higher probabilities. To evaluate the security level, we should find out the expected average size of the pass-square areas, which is an important measure of our scheme's security level.

Consider our basic scheme. Without loss of generality, we divide the login image region into $n \star n$ grids. We assume that each character in the set T , which consists of all the 94 available password characters, is placed randomly in the center of every grid. In addition, we assume the length of the border of the login image is L. The two vertices's of a pass-square hold coordinates: $B(X_1, Y_1)$ and $C(X_2, Y_2)$. X_1, Y_1, X_2, Y_2 are independent with each other. Each of them is distributed uniformly between L/n and L as shown in Figure 6. Two vertices's are sufficient to calculate the area of the square.

Considering the square selection as shown in Figure 6, its area can be calculated by applying distance formula is given by,

$$A = (X_2 - X_1)^2 + (Y_2 - Y_1)^2 \tag{1}$$

The expected average square area is,

$$E(A) = \sum_{f=1}^{n} \sum_{g=1}^{n} \sum_{i=1}^{n} \sum_{j=1}^{n} \left| \left(\frac{f}{n} - \frac{g}{n}\right)^2 + \left(\frac{i}{n} - \frac{j}{n}\right)^2 \right| \frac{1}{n^4} \tag{2}$$

In the basic password authentication scheme, we have 94 printable characters. As an example, $9 \star 9$ grids are able to contain all the characters. Setting $n = 9$ in

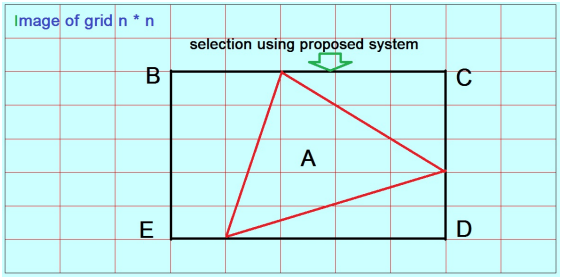


Figure 6. The analysis of square area selection

Table III
THE AREA OF PASS-SQUARE AS PER THE GRID NUMBER n

n	Square area
3	$0.2962962L^2$
5	$0.3199999L^2$
7	$0.3265300L^2$
9	$0.32921810L^2$

equation 2, we obtain, $E(A) = 0.32921810L^2 \approx 0.330L^2$. Based on E(A), we know that the success probability using the random-click attack is given by $P(A) = 0.330L^2/L^2 = 0.330$. For a password k, the probability to get authentication just by random-clicks is $0.330^{|k|}$. Recall the former example, the length of the password is five. For attackers, the probability of click the right area for all the five times is $P(S)^{|k|} = 0.330^5 \approx 0.003913539$.

This probability is pretty low. It is extremely hard for attackers to get such a "good luck" to get authentication just by random-clicks. Attackers are forced to use brute-force search to break the password. That is, they hope to try many times, so that even though the probability to break the system for one time is pretty low, they can get the authentication by large number of tries. We will show later how our scheme resists the brute-force search.

Since the value of $E(S)$ determines the scheme's security level, we should try to reduce the value of $E(A)$. From equation 2, we observe that the parameter n is an important factor affecting $E(A)$. To show the relationship between $E(A)$ and n, we calculate several $E(A)$ value according to different n. We get the following results as shown in Table III.

From the Table III we can have following corollary.

Corollary: *As the grid number n increases, the expected average area of a randomly-placed pass-square also increases; when n approaches infinity ($n \to \infty$), the expected average area of a square approaches a limit value.*

Based on the corollary, to achieve the best security level, we should make the average size of the squares as small as possible; thus, we should choose the smallest grid number that is large enough to host the set of all characters T.

Shoulder surfing is possible in-case of conventional textual and graphical password systems. This system is resistant to shoulder-surfing, hidden-camera and spyware attacks since at no point the user enters his original password. Hence there is no way that any one watching the login process can know the original password. Our proposed system takes less time to login as compared with system proposed in [5].

5.1 Random Click Attack

Our system prevents Random Click Attacks in the following ways

- If the user clicks/types a wrong entry he/she will be directed to a page enter CAPTCHA. This ensures that the user is human [17]. Now for CAPTCHA entry the user is provided a total of N (for eg N=3) chances which the user will be aware of. Suppose the user makes all N wrong CAPTCHA entries he will be directed straight to the login page.
- If the user enters the correct CAPTCHA he will be directed to the same screen wherein he had made a wrong entry. If again he makes a faulty entry the next time he will be automatically exited from the login process.

5.2 Brute Force Search Resistant

In our system, there are two kinds of passwords: the original passwords and dynamic session passwords. Therefore, there are mainly two ways to brute-force search our system's passwords: brute-force search original passwords and brute-force search session passwords.

Once the user has successfully entered the correct CAPTCHA, a message with a temporary session ID will be sent to the user's mobile phone which has to be entered by the user. The inclusion of this step of sending an SMS with the session ID is to ensure that only the genuine user has access to his/her account. If by chance an intruder is able to make all the right guesses using Brute Force Attack and reaches this stage, he will not gain access to the account as he/she will not have session ID.

6 CONCLUSION

Authentication is the need of the hour. With the rise in intrusion attacks in the various walks of life, a strong and flexible authentication system is a pre-requisite. Textual passwords, being easy to remember and implement, have the danger of being cracked due to their simplicity. Graphical passwords have their own disadvantages. Most common would be brute-force and dictionary attacks. However one cannot deny the fact that all good things come with a price. Although graphical passwords have their share of shortcomings they balance it out with their unique advantages.

The system that we have proposed adopts a visual login technique that matches the capabilities and limitations of most devices and provides a powerful technique to authenticate users. Our scheme demonstrates desirable features of a secure authentication system being immune to shoulder-surfing, hidden-camera and spyware attacks. Our system is scalable in that it seamlessly matches the conventional text-based passwords

and can accommodate various lengths of textual passwords, which requires zero-efforts for users to migrate their existing passwords to our scheme. This technique combines the advantages of both textual and graphical passwords to come up with a complex but promising and strong solution against intrusion.

7 Future Enhancements

A few additions and modifications can be made in our proposed system. Firstly, our system restricts to the use of a square boundary for asking the user to select the centre character. Quadrilaterals of different shapes and sizes can be used. The grid/ square that would form the selection boundary, as of now, is proposed to be a NxN matrix where N is an odd number. Eg :3⋆3, 7⋆7 and so on. Grids where N can be simply even or a combination of odd and even Eg: 3⋆4, 4⋆4 can be formed.

Secondly, the system can make use of pictures of alphabets, numbers and symbols or any images as graphical password entries in the pass-squares.

As our proposed system has overcome the problem of shoulder surfing attack, but the time required to login is incredibly more hence usability will decrease. Therefore more research has to be carried out as to achieve higher levels of usefulness.

References

[1] M. Sreelatha, M. Shashi, M. Anirudh, M. S. Ahamer, and V. M. Kumar, "Authentication schemes for session passwords using color and images," *International Journal of Multimedia & Its Applications*, vol. 5, no. 2, pp. 111–116, 2011.

[2] A. Almulhem, "A graphical password authentication system," in *World Congress on Internet Security (WorldCIS)*, 2011, pp. 223–225.

[3] G. Haichang, Z. Ren, C. Xiuling, L. Xiyang, and A. Uwe, "A new graphical password scheme resistant to shoulder-surfing," in *International Conference on Cyberworlds (CW), 2010*, 2010, pp. 194–199.

[4] S. Zhai and T. He, "Design and implementation of password-based identity authentication system," in *International Conference on Computer Application and System Modeling (ICCASM), 2010*, vol. 9, 2010, pp. 253–257.

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

[6] X. Suo, Y. Zhu, and G. Owen, "Graphical passwords: a survey," in *21st Annual Computer Security Applications Conference*, 2005, p. 472.

[7] H. Mohammad, I. Norafida, and P. Rezvan, "Multi touch graphical password: Usability features," *Asian Journal of Applied Sciences*, vol. 5, pp. 20–32, 2012.

[8] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin *et al.*, "The design and analysis of graphical passwords," *Proceedings of the 8th USENIX Security Symposium*, pp. 1–14, 1999.

[9] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *Proceedings of the 2005 Symposium on Usable Privacy and Security*, ser. SOUPS '05, 2005, pp. 1–12.

[10] D. Nali and J. Thorpe, "Analyzing user choice in graphical passwords," 2004, in technical Report, School of Information Technology and Engineering,University of Ottawa, Canada.

[11] M. Shahid and M. Qadeer, "Novel scheme for securing passwords," in *3rd IEEE International Conference on Digital Ecosystems and Technologies, 2009. DEST '09.*, 2009, pp. 223–227.

[12] W.-C. Ku and M.-J. Tsaur, "A remote user authentication scheme using strong graphical passwords," in *The IEEE Conference on Local Computer Networks, 2005. 30th Anniversary.*, 2005, pp. 351–357.

[13] J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and the memorable space of graphical passwords," in *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, ser. SSYM'04, 2004, pp. 10–10.

[14] C. hien Lu and H.-Y. Liao, "Structural digital signature for image authentication: an incidental distortion resistant scheme," *IEEE Transactions on Multimedia*, vol. 5, no. 2, pp. 161–173, 2003.

[15] C. Y. Chen, C. Y. Gun, and H. F. Lin, "A fair and dynamic password authentication system," in *2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)*, 2011, pp. 4505–4509.

[16] M. ArunPrakash and T. R. Gokul, "Network security-overcome password hacking through graphical password authentication," in *National Conference on Innovations in Emerging Technology (NCOIET)*, 2011, pp. 43–48.

[17] M. Dailey and C. Namprempre, "A text graphics character captcha for password authentication," in *TENCON 2004. 2004 IEEE Region 10 Conference*, 2004, pp. 45–48.

Umedha Bell received Bachelors Degree in Information Technology Engineering from Fr. Conceicao Rodrigues College of Engineering, Mumbai in the year 2013 She is currently working as a Assistant Systems Engineer at Tata Consultancy Services. She is into the area of software development. Her areas of interests are web designing and web development.

Divya Bhat received Bachelors Degree in Information Technology Engineering from Fr. Conceicao Rodrigues College of Engineering, Mumbai in the year 2013 She is currently working as a Assistant Systems Engineer at Tata Consultancy Services. She is into the area of software development. Her areas of interests are web design and web security

Neha Ubharkar received Bachelors Degree in Information Technology Engineering from Fr. Conceicao Rodrigues College of Engineering, Mumbai in the year 2013 She is currently placed at Godrej Security Solutions which is one of the flourishing divisions of Godrej and Boyce Manufacturing Company in the sales department. She would like to pursue her career in marketing and business development.

Vaibhav Godbole received Masters Degree in Electronics & Telecommunication Engineering from Sardar Patel Institute of Technology, Mumbai and Bachelors Degree in Electrical Engineering from Sardar Patel College of Engineering, Mumbai, Diploma in Industrial Electronics from S.B.M. Polytechnic, Mumbai and Diploma in Mechanical Engineering from Govt. Polytechnic, Mumbai.

He is currently working as a Assistant Professor at Fr. Conceicao Rodigues College Of Engineering, Mumbai. He is also a reviewer for IEEE Sensors Journal, IET Journal of Networks and IET Journal of Wireless Sensor Systems. His areas of interests are big data analysis using Hadoop, mobile & wireless communications, evolutionary algorithms, genetic algorithms, new algorithms for mobile ad-hoc networks and wireless sensor networks.

Saurabh Kulkarni was born in India on September 7,1987. He received BE in Information Technology from University of Mumbai,India in 2009 and M.Tech in Computer Science and Engineering from MIT, Manipal, India in 2012. He is currently working as Assistant Professor in Department of Information Technology in Fr. Conceicao Rodrigues College of Engineering, University Of Mumbai, India. He was working in Intel India Pvt. Ltd. as intern from June 2011 to June 2012 on database scrambling tool. His research interests include database security, Semantic web, Web link analysis.