International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2763
Issue 12, Volume 3 (December 2016) www.ijirae.com

Click Based Graphical Password Authentication Schema for Better Security in Cyber Space

[#1]Dr A.Srisaila,*[2] T.Srinivasa Ravi Kiran

[1]*Assistant Professor, VR Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India, PIN:520007, Department of Information Technology*

[2]*Lecturer, P.B.Siddhartha College of Arts & Science, Vijayawada, Andhra Pradesh, India, PIN:520007, Department of Computer Science*

Abstract - Now a days, password are used to gain access over the devices. Traditionally, passwords are alphanumeric, consisting of letters, numbers and symbols. Often, passwords are lengthy and have to be changed every few months to ensure computer security. This makes retention and recall difficult. Due to this problem, graphical passwords have been developed. The inspiration behind exploring a graphical password scheme was based on the remarkable ability of humans to recall pictures. In this paper, we present an innovative, user friendly recall based graphical scheme where the user starts with identifying click points for some combinations of password o n the presented interface. The user chooses the combinations in the same order cyclically per each login attempt. For example the user chooses first combination of password for first login in attempt, second combination of password for second login attempt, third combination of password for third login attempt, fourth combination of password for fourth login attempt, and fifth combination of password for fifth login attempt.

Keywords: Graphical Password, Security, Combination, Cyclically, Login attempt

I. INTRODUCTION

A password is a secret word or combination of alphabets used for user authentication to establish self identity. This password should be kept secret from those not allowed to access. Now-a-days data security is the most describing problem. Passwords provide security mechanism for authentication and protection services against unwanted access to resources. Authentication is the process of verifying a claim made by a subject that it should be allowed to act on behalf of a given person, computer, process, etc. User authentication is a most important component in most computer security. It provides user with access control and user accountability [1]

People are using passwords every day, many times for online banking accounts, for social network profiles and to check their emails from work. The password techniques used in market are very insecure. The textual passwords which we normally use suffer with both security and usability problems [2]. The majority of the digital systems have security measurements based on textual passwords. The vulnerabilities of the textual password have been well known. The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. It is almost impossible for a human to remember a long complicated string of characters to act as the secret. Hence, a user tends to choose a small and easy to remember textual password. Shorter textual passwords are easy to guess and longer passwords are harder to remember for the users themselves Ziran Zheng et al. [3]. If a password is not frequently used it will be even more susceptible to forgetting. Textual password is vulnerable to shoulder-surfing, hidden-camera and spy ware attacks. Passwords play a significant task in computer security to validate human users. Users rely on graphical passwords because it offers more security than the text-based passwords [4].

In addition, the possible password space of a graphical password scheme may exceed that of text based schemes and thus most probably offer 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. However, existing graphical passwords are far from perfect. Typically, system requirements and cost of communication for graphical passwords are significantly higher than text-based passwords. Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords [5].

The proposed model is also aimed at protecting the user and/or application privileges from being compromised due to hacking attempt [6]. During the password creation time, there is a small view port area that is randomly generated on the image. Users must select a click-point within the view port area [7].

II RELATED WORK

Based on Blonder's[8] original idea, Pass Points is a click-based graphical password system where a password consists of an ordered sequence of 5 click- points on a pixel-based image as shown in Figure 2.3.1 .To log in, a user must click within some system defined tolerance region for each click-point Blonder.

Jermyn et al.[9] presented a purely graphical pass- word selection and input scheme, which we call "Draw a Secret" (DAS). In this scheme, the password is a simple picture drawn on a grid. This approach is alphabet independent, thus making it equally accessible for speakers of any language. Users are freed from having to remember any kind of alphanumeric string Huanyu Zhao *et al* [10] proposed S3PAS system generates the login image locally and transmits the image specification (e.g., the coordinates of every character or icon in the image) instead of the entire image pixel-by-pixel from clients to servers, which greatly reduces communication overheads and authentication time. M. Kameswara Rao et al. [11] found PPC and TPPC methods. Each of these schemes supports two modes of input, namely, keyboard entry and mouse clicks. We refer to the former mode as the text mode and the latter as the graphical mode. The input image consists of a 10 × 10 grid of cells each of which represent the characters A-Z, a-z, 0-9 and other printable characters which are padded with spaces in a single color and randomly spaced on the grid. In this thesis, we refer to this as the basic character set and is used in the PPC scheme. The same character set in three colors randomly spaced and padded with spaces in a 17×17 grid is the color character set and is used as the input image in the TPPC scheme.

Sobrado and Birget [12] discussed a number of techniques which aim to solve the shoulder surfing problem. In the first technique (which they call "triangle scheme"), a number of pass-objects are presented, which were previously seen and selected by a user in the registration stage, along with many other "decoy" objects. Then the user is required to find the pass-objects and click inside the convex hull formed by all the pass-objects. Because the area of the convex hull can be large, the probability of successful login by random clicking for one single round can be high. Therefore, this particular scheme requires this process to be run for sufficient times (e.g. 10). In order to make the password space large enough, the authors also suggest 1000 objects to be displayed on the login interface. In other words, this scheme requires considerably large display space and significant patience to find pass-objects. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. Divyashree et al. [13] gone through different alternative methods and conclude that graphical passwords are most preferable authentication system. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice, encouraging user to select more random click point which is difficult to guess. The system is a combination of recognition and pure recall based techniques and that offers many advantages over the existing systems and may be more convenient for the user. Partha Pratim Ray [14] approach is resistant to shoulder surfing attack and many other attacks on graphical passwords. This scheme is proposed for smart hand held devices (like smart phones i.e. PDAs, ipod, iphone, etc) which are more handy and convenient to use than traditional desktop computer systems.

Justin D. Pierce et al. [15] discussed a conceptual frame work for an alternative authentication paradigm. The frame work attempts to reduce the complexity for the user as well as increase security at the network and application level. T.S.Ravi Kiran and Y.Rama Krihna[16] suggest "A Hybrid User Authentication Approach Combining CAPTCHA", The thought behind this is, users choose combination of CAPTCHA and images as their graphical passwords. For each round of verification, the specified numbers of text CAPTCHA's and images are randomly selected by the system from a database. A user then chooses a specified number of text CAPTCHA's and images as her graphical password. This process repeats for the specified number of rounds. T.Srinivasa Ravi Kiran, Dr.K.V.Samabasiva Rao, M.Kameswara Rao [17] proposed "Noval Graphical Scheme Resistent To Peeping Attack" which starts with identifying quadruplets formed from the user password starting with the first character and sliding to the right one character at a time wrapping around if necessary until the last a character in the password appears as the first character in a quadruplet. For example, if the password selected at registration time is "T2D8h" then the quadruplets formed are "T2D8T", "2D8h2", "D8hTD", "8hT28" and "hT2Dh". The user chooses the combinations in the same order cyclically per each login attempt.

T.Srinivasa Ravi Kiran, Dr.K.V.Samabasiva Rao, Dr.M.Kameswara Rao, A.Srisaila [18] proposed "A Symbol Based Graphical Schema Resistant to Peeping Attack" includes a 5 x 5 grid formed using 25 blocks. Each block consists of a symbol. The symbol contains a set of four characters. User are supposed to draws a line between adjacent blocks or non adjacent blocks then the character sets to be considered are taken from the block. Then the password contains at least one character from each set of four characters depicted on the symbol of each block. Dr. R.Satya Prasad and T.Srinivasa Ravi Kiran [19] proposed "A RGBR Pass Point Graphical Password Schema Resistant To Shoulder surfing" includes the scheme of authentication resistant to peeping attack starts with identifying triangle formed by clicking on the cells containing colors red, green, blue & red of the interface respectively.

At least one combination considered from the password definitely forms the triangle and the first character and last character is same. For example at first login the user chooses the combination "Qb@Q", for second login the user chooses the combination "b@3b", for third login the user chooses the combination "@3Q@", for fourth login the user chooses the combination "3Qb3", again for fifth login the user chooses the combination "Qb@Q" and so on.

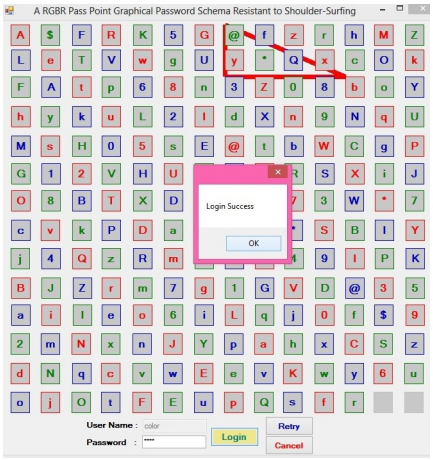


Fig.1.Triangle Formed by Clicking on the Cells b@3b Containing the Color Red, Green, Blue and Red Respectively for Second Login Attempt

T.Srinivasa Ravi Kiran and Dr. R.Satya Prasad [20] present a novel, user-friendly, recall-based graphical password scheme where the user starts with the identifying the individual transformation applied to every individual character of password combination. If expected combination of characters of password matches with expected transformations then the login attempt is successful otherwise login attempt is failed.

T.Srinivasa Ravi Kiran, R.Satya Prasad [21] presented an innovative, user-friendly, recall-based graphical password scheme where the user starts with the identifying the symbol from 5 × 5 grid formed using 25 blocks. The user is supposed to select three characters one by one by clicking on a single block from the 5 × 5 grid in such a way that the password contains at least one character from each set of four characters depicted on the symbol of the clicked block. The user chooses the characters of the password in the same order per each login attempt. The user is supposed to select the position of the each character depicted on the symbol of the clicked block from the 2 × 2 grid. The login attempt is successful after matching the characters of the password at positions one, two and three respectively. Login is invalid, if characters of password are not identified in the symbols of 5 × 5 grid or not matched with the corresponding positions of 2 × 2 grid.

III. PROPOSED WORK

In the proposed scheme, we use a 10x10 grid formed using the single color 94 printable character set added with spaces as shown in Figure2. Passwords are input by typing or by mouse clicks. The proposed scheme starts with identifying pass points clicking on the cells on the presented interface. The selection of specified pass points in the presented interface takes the user to the next level.

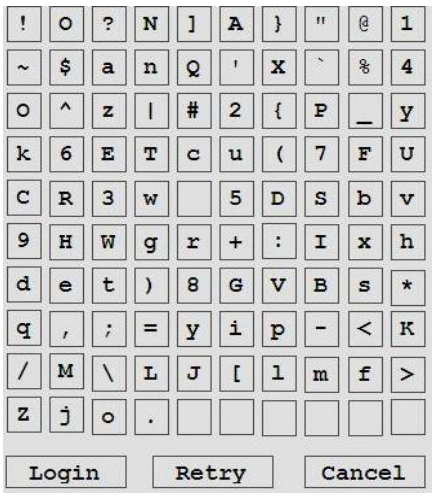


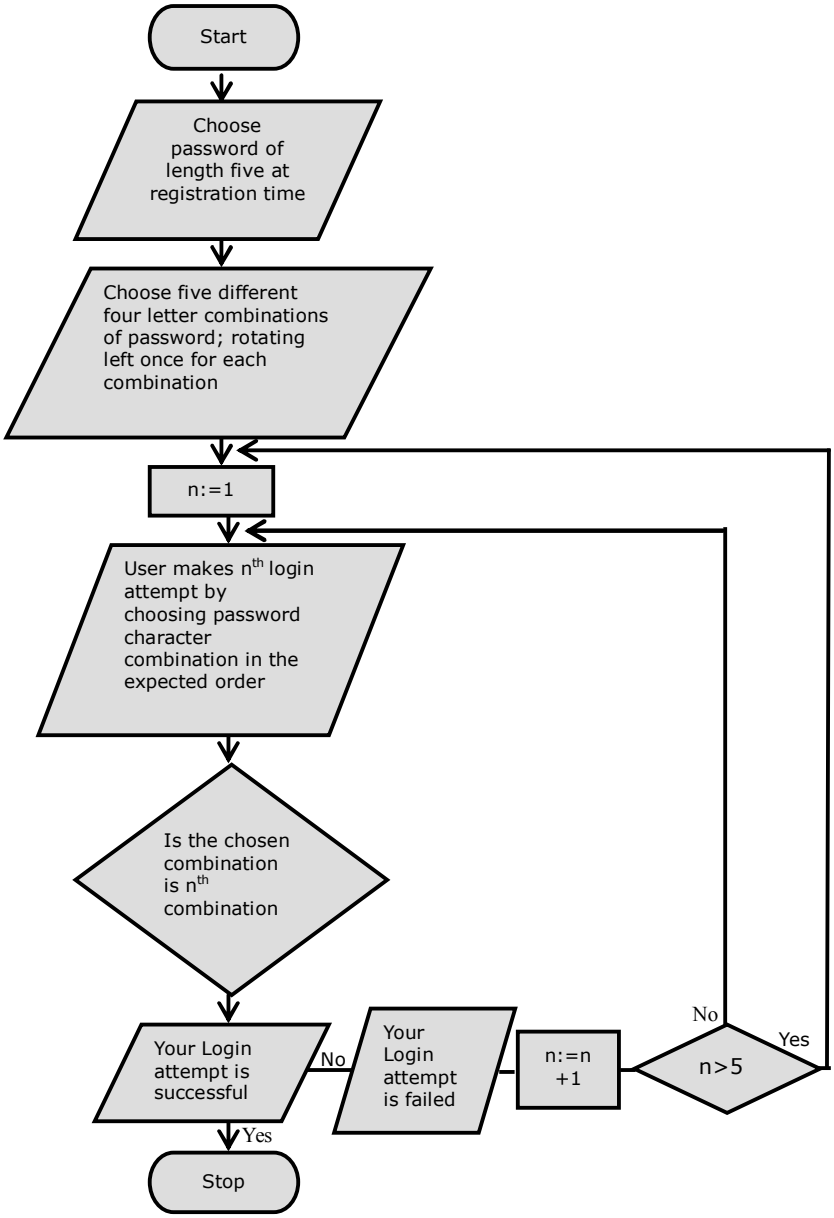
Fig.2. Proposed Schema

Passwords are input by four mouse clicks on the presented interface. For example, if the password selected at registration time is "T2D8h" then the possible combinations formed by clicking on the cells are "T2D8", "2D8h", "D8hT", "8hT2", "hT2D". The user chooses the combinations in the same order cyclically per each login attempt. For example at first login the user chooses the combination "T2D8", for second login the user chooses the combination "2D8h", for third login the user chooses the combination "D8hT", for fourth login the user chooses the combination "8hT2", for fifth login the user chooses the combination "hT2D".

ALGORITHM:

1. *Start*
2. *Choose password of length five at registration time*
3. *Choose five different four letter combinations of password, rotating left once for each combination.*
4. *User makes N^{th} login attempt by choosing password character combination in the expected order on the presented interface.*
5. *If the user chooses password character in the expected order then the login attempt are successful, validate the next combination.*
6. *If the user does not choose password character combination in the expected order then the login attempt is failed, ignore that combination of password character and choose another combination password character.*
7. *Stop*

Flow Chart



Step 1: Login attempt is successful for the combination "T2D8" for first login attempt

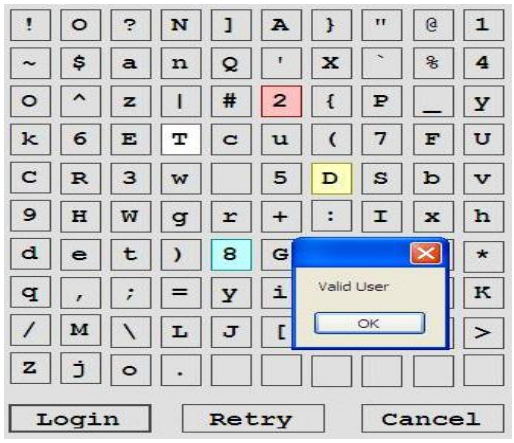


Fig.3.Verification of Authentication by Clicking on the Cells "T2D8 for first Login Attempt

Step 2: Login attempt is failed for the combination "T2D8" for second login attempt since the user does not choose correct combination.

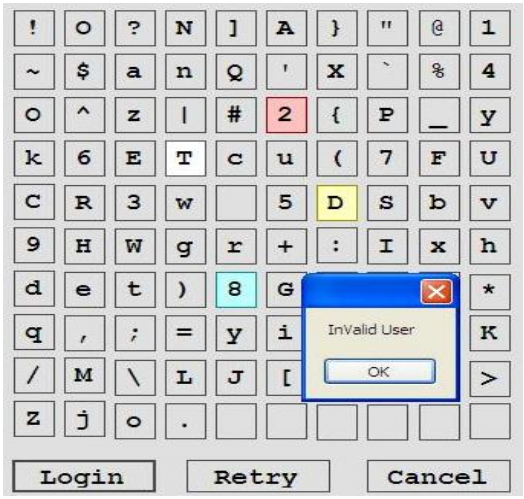


Fig.4.Login attempt is failed by Clicking on the Cells "T2D8" for second Login Attempt

Step 3: Login attempt is successful for the combination "2D8h" for second login attempt

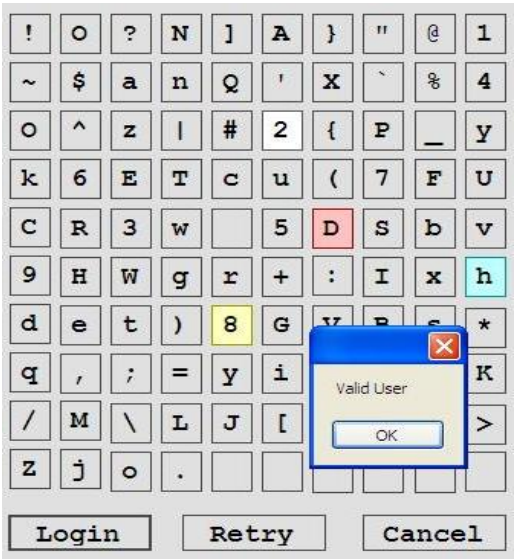


Fig.5.Verification of Authentication by Clicking on the Cells "2D8h" for Second Login Attempt

Step 4: Login attempt is successful for the combination "8hT2" for fourth login attempt.

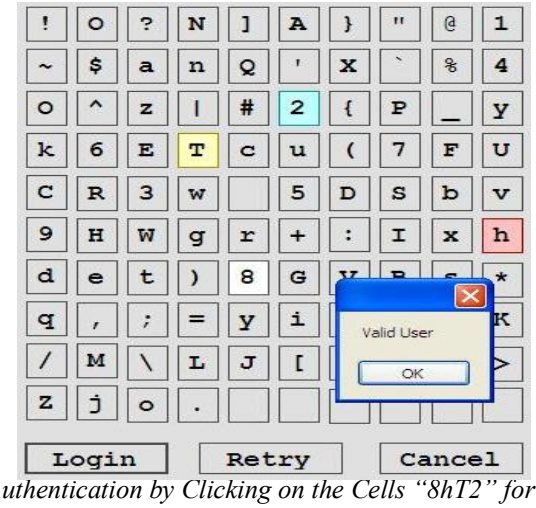


Fig.6.Verification of Authentication by Clicking on the Cells "8hT2" for fourth Login Attempt

Step 5: Login attempt is successful for the combination "hT2D" for fifth login attempt.

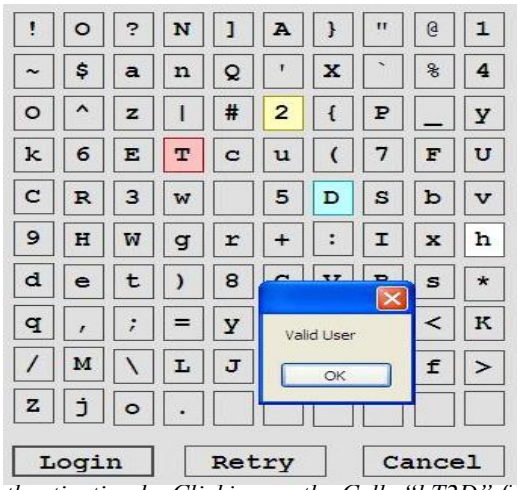


Fig.7.Verification of Authentication by Clicking on the Cells "hT2D" for fifth Login Attempt

IV. USABILITY STUDY & RESULTS

The result was encouraging that novice users were able to identify the pentagon formed by clicking on the cells in the specified order. It took about 37 milliseconds on average to log in. Peeping attack is the attack where an attacker gets the secret information through direct observation when the user is entering his or her password.

TABLE 1. A TWELVE POINT REORGANIZATION SCHEMA

S. NO	RECOGNIZATION BASED SCHEMA	A FOURTEEN POINT SCALE OF EFFICIENCY
1	G. E. Blonder	8
2	Passface	9
3	Jermyn, et al.	6
4	Hybrid User Authentication Approach	10
	A Novel Graphical cheme	11
6	A Symbol Based Graphical Schema	11
7	A RGBR Pass Point Schema	11
8	Transformations Based Schema	12
9	A Symbol Based Scheme Based on Position Value	12
10	A Click Based Graphical Password Authentication Schema	13

Alphanumeric systems are susceptible to peeping attack. In these attacks, typically the attacker gets a chance to observe the password entry for a short duration of time.

As alphanumeric passwords are typically small, the attacker may see the secret by looking just for a while. On the other hand, peeping attack is not feasible against our proposed scheme as the user types or clicks on non password characters.

TABLE 2.RESULT OF FIVE TRAINEE USERS

S No	Password	Pass1	Login time for pass1 in milliseconds	Pass2	Login time for pass2 in milliseconds	Pass3	Login time for pass3 in milliseconds	Pass 4	Login time for pass4 in milliseconds	Pass5	Login time for pass5 in milliseconds	Average login time in milliseconds for pass
1	T2D8h	T2D8	36	2D8h	39	D8hT	37	8hT2	38	hT2D	39	38
2	3x%4y	3x%4	37	x%4y	36	%4y3	35	4y3x	37	y3x%	35	36
3	,=3c%	,=3c	34	=3c%	36	3c%,	36	c%,=	37	%,=3	35	36
4	pB7#9	pB7#	38	B7#9	37	7#9p	36	#9pB	36	9pB7	37	37
5	ir+@1	ir+@	37	r+@1	38	+@1i	38	@1ir	35	1ir+	38	37
Mean time to login using i5 processor for the attempt by the trainee user												37

Fig.8. A histogram of fourteen point scale of efficiency scale

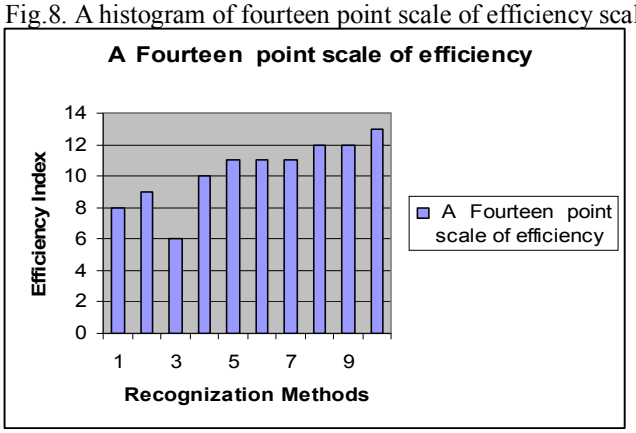


Fig.9. A line graph of fourteen point scale of efficiency scale

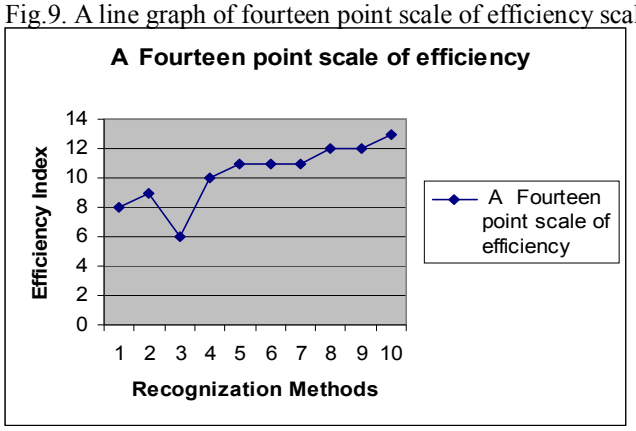


TABLE 3. USABILITY TABLE OF REORGANIZATION BASED SCHEMA

Row	Reorganization Based Schema	User Features													
		Satisfaction												Efficiency	Effectiveness
		Mouse usage	Create Simply	Meaningful	Assignable Image	Memorability	Simple steps	Nice Interface	Training Simply	Pleasant Picture	Applicability of Transformations	Selecting position of each character	Selecting Pentagon Patterns	Applicable	R&A
1	G. E. Blonder	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N

2	Passface	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	N	N	Y
3	Jermyn, et al.	N	N	Y	N	Y	Y	Y	N	N	N	N	N	Y	Y
4	Hybrid User Authentication approach	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y
5	A Novel Graphical Scheme	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y
6	A Symbol Based Graphical Schema	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y
7	A RGBR Pass Point Schema	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y
8	Transformations Based Schema	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y
9	A Symbol Based Scheme Based on Position Value	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y
10	Click Based Graphical Password Authentication Schema	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y
Y - Yes N - No															

V. COMPLEXITY

The password at registration time is "T2D8h" and out of possible combinations only the permutations "T2D8","2D8h","D8hT","8hT2" and "hT2D" are considered. There are five distinct characters in the password at registration time, therefore the length of the password is five. Total number of permutations of five length password is 5^5=3125. One permutation is favorable from 3125 possible permutations. The probability of compromising the security of password is (1/3125)×100 = 0.032%. Hence the robustness of the password is 100-0.032=99.968%.As the starting and ending letters in the chosen permutation fixed for the remaining three characters in the in the password there are six possible permutations. The probability of compromising the security of each permutation is (24/3125)×100=0.768%. Hence the robustness of the each password permutation is 100-0.078=99.23%.

VI. FUTURE SCOPE

We proposed a scalable shoulder-surfing resistant password authentication system. The results of proposed schema demonstrate desirable features of a secure authentication system being impervious to shoulder-surfing, hidden-camera, and spy ware attacks. The scheme provides a potential solution for the modern problems faced by the other graphical password schemes. The proposed scheme provides larger password space than traditional text based passwords. The extension of the proposed schemes is to identify the hexagon formed by clicking on the cells in the specified order on the presented interface as future work

VII. REFERENCES

[1]. W. Stallings, L. Brown," Computer Security: Principle and Practices", Pearson Education, 2008.
[2]. V. Bhusari,"Graphical Authentication Based Techniques", International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013 1 ISSN 2250-3153.
[3]. Ziran Zheng *et al*,"A Hybrid Password Authentication Scheme Based on Shape and Text", JOURNAL OF COMPUTERS, VOL. 5, NO. 5, MAY 2010.
[4]. X. Suo, Y. Zhu, G.S, "Owen. Graphical passwords: A survey", In Proceedings of Annual Computer Security Applications Conference, 2005, pp. 463–472.
[5]. R.P. Anto Kumar,"A New Implementation of Graphical Password Scheme for Captcha Based Security System",Middle-East Journal of Scientific Research 23 (7): 1353-1357, 2015,ISSN 1990-9233© IDOSI Publications, 2015,DOI: 10.5829/idosi.mejsr.2015.23.07.105
[6]. Shivangi et al,"Multi-tier Graphical Password Authentication for Foolproof Login in Cloud Applications", International journal of Science Technology & Management (IJSTM) ISSN: 2229-6646, Presented in National Conference on RTICCN-2015 at CGC-COE , Landran , Mohali(Punjab) on 26-27th March 2015
[7]. Poonam M.Khairnar et al,"Securing password against online password guessing attacks", Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-3, 2016 ISSN : 2454-1362 , http://www.onlinejournal.in
[8]. Blonder, "G.E. Graphical Passwords", United States Patent 5,559,961.1996
[9]. Ian Jermyn *et al.*, "The Design and Analysis of Graphical Passwords", Proceedings of the 8th USENIX Security Symposium, Washington, D.C., USA", August 23-26, 1999.
[10]. Huanyu Zhao *et al.*, "S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", Research paper published in Advanced Information Networking and Applications Workshops, AINAW '07. 21st International Conference on (Volume:2), 2007.

[11]. M.Kameswara Rao et al, "Novel Shoulder-Surfing Resistant Authentication Schemes using Text-Graphical Passwords", International Journal of Information & Network Security (IJINS) , Vol.1, No.3, August 2012, pp.163-170, ISSN:2089-3299.
[12]. SOBRADO L. and BIRGET J., "Graphical Passwords, the Rutgers Scholar", Rutgers University, Camden New Jersey 081024, 2002.
[13]. Divyashree V et al. (2014), "Adding Persuasive Features in Graphical Password to Increase the Capacity of Knowledge Based Authentication Mechanism", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 7, July 2014, ISSN: 2319-8753.
[14]. Partha Pratim Ray, " Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices", Journal of Information Engineering and Applications, Vol 2, No.2, 2012.
[15]. Justin D. Pierce (2003) et al. (2003) discussed a conceptual frame work for an alternative authentication paradigm. The frame work attempts to reduce the complexity for the user as well as increase security at the network and application level.
[16]. T.S.Ravi Kiran and Y.RamaKrishna, "COMBINING CAPTCHA AND GRAPHICAL PASSWORDS FOR USER AUTHENTICATION", International Journal of Research in IT & Management, Volume 2, Issue 4 (April 2012) (ISSN 2231-4334), http://www.mairec.org.
[17]. T.Srinivasa Ravi Kiran, Dr.K.V.Samabasiva Rao, M.Kameswara Rao, "A Novel Graphical Password Scheme Resistant To Peeping Attack", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5) ,2012, 5051-5054.
[18]. T.Srinivasa Ravi Kiran, Dr. K. V. Samabasiva Rao, Dr.M.Kameswara Rao,A.Srisaila, "A Symbol Based Graphical Schema Resistant to Peeping Attack", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 5, No 1, September 2013.
[19]. R.Satya Prasad et al., "A RGBR PASS POINT GRAPHICAL PASSWORD SCHEMA RESISTANT TO SHOULDERSURFING", JCSE(International Journal of Computer Science and Engineering) in association with IASET(International Academy of Science, Engineering and Technology), ISSN(P): 2278-9960; ISSN(E): 2278-9979,Vol. 3, Issue 4, July 2014, pp.175-188, IASET, ww.iaset.us.
[20]. T.Srinivasa Ravi Kiran, Dr. R.Satya Prasad, "A Shoulder Surfing Graphical Password Schema Based on Transformations", IJAER, "International Journal of Applied Engineering Research", ISSN: 0973-4562, Volume 9, Number 22 (2014) pp. 11977-11994 © Research India Publications, http://www.ripublication.com.
[21]. T.Srinivasa Ravi Kiran, R.Satya Prasad,"A Symbol Based Graphical Schema Based on Position Value", International Journal of Engineering and Technology (IJET), Vol 7 No 2 Apr-May 2015, ISSN: 0975-4024, pp514 to 529.

VIII. AUTHORS PROFILE

Dr.A.Srisaila received her M.Tech (Computer Science & Engineering) from Bapatla Engineering College and Ph.D in Computer Science & Engineering from Acharya Nagarjuna University. Presently she is working as Assistant Professor in Department of Information Technology in V.R.Siddhartha Engineering College. Her research area includes Software Reliability Engineering, Graphical Passwords, Human Computer Interaction and Big Data Analytics. She published ten research papers in various international journals. She published four research papers in various international journals.

Mr. T.Srinivasa Ravi Kiran received MCA from University of Madras in 1998, M.Phil., from Bharathidasan University in 2006 and M.Tech., (Computer Science & Engineering) from Acharya Nagarjuna University in 2010. Now he is pursuing Ph.D.,in Computer Science & Engineering from Acharya Nagarjuna University as Part-Time Research Scholar under the guidance of Dr. R.Satya Prasad. Currently, he is working as a Lecturer & Head of the Department at Post Graduate Centre of P.B.Siddhartha College of Arts&Science, Vijayawada, AP, India. His research interest lies in Graphical Passwords,Cryptography, Human Computer Interaction and Software Reliability Engineering. He published four research papers in various international journals.

