A Symbol Based Graphical Schema Based on Position Value

T.Srinivasa Ravi Kiran[#1] , R.Satya Prasad[*2]
[#1] Lecturer,
Department of Computer Science, P.G Centre, P.B.Siddhatha College of Arts & Science,
Vijayawada, Andhra Pradesh, India, PIN: 520010
[1]kirantsr1@gmail.com
[*2]Associate Professor,
Department of Computer Science & Engineering, Acharya Nagarjuna University,
Nagarjuna Nagar, Andhra Pradesh, India, PIN: 522502
[2]profrsp@gmail.com

Abstract - The most common computer authentication method is to use alphanumerical usernames and passwords. Textual passwords are difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. 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. In this paper, we present 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.

Keywords: Authentication, Graphical Password, Login attempt, Symbol, Grid, Matching, Position

I. INTRODUCTION

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 [2]. 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 spyware attacks[21].

Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text [3]. A graphical password is a secret that a user inputs to a computer with the aid of the computer's graphical input (e.g. mouse, stylus or touch screen) [4].

A mouse tracking spyware can be an effective tool against graphical passwords. However, such a tool may not be an effective tool to break graphical passwords because the mouse information should be related with parameters such as window position and size. Compared to text-based passwords, it is not easy to give graphical passwords to another person especially over the phone.

If the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus most likely offer better resistance to dictionary attacks. Because of these advantages, there is a growing interest in graphical password. Graphical passwords require more space than text based passwords because of their sizes. The pictures also have to be maintained in a centralized database which implies that network transfer is an area of concern for graphical passwords. However, with the increased bandwidths and high computer storage space, this concern about graphical passwords is no longer a serious issue.

Graphical password schemes can be grouped and differentiated within four different fundamental ideas. As described by [5], [6] and [7] graphical password schemes are based on recall, recognition, cued recall or cued recognition.

II. RELATED WORK

Huanyu Zhao et al proposed S3PAS System[8] that 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.

Passface" is a technique developed by Real User Corporation. The basic idea is as follows. The user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees 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 the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures [9].

T.S.Ravi Kiran and Y.Rama Krihna[10] 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 number 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.

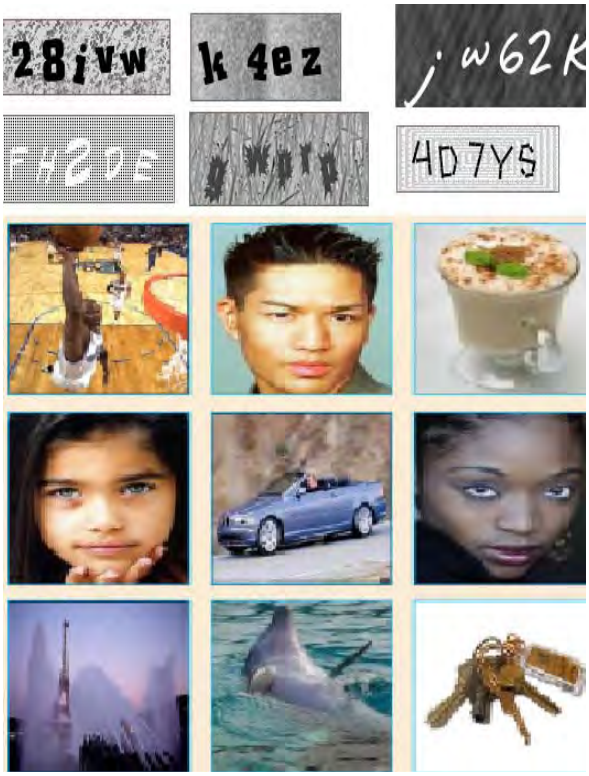

Fig 1.Proposed schema of user authentication approach combining CAPTCHA

T.Srinivasa Ravi Kiran, Dr.K.V.Samabasiva Rao, M.Kameswara Rao [11] proposed "A 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.

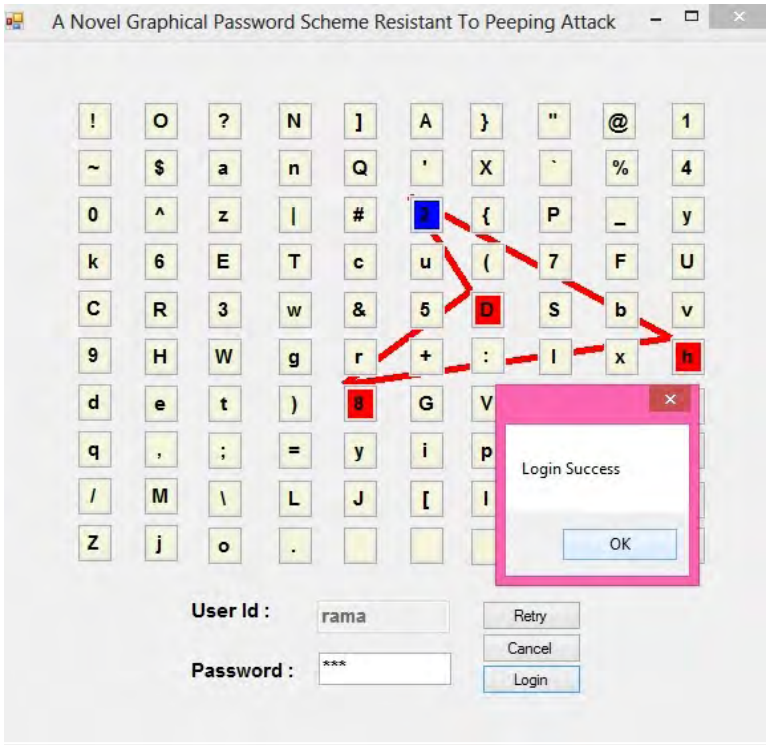

Fig 2. Quadruple formed by clicking on the Cells "2D8T2" for successful login attempt

T.Srinivasa Ravi Kiran, Dr.K.V.Samabasiva Rao, Dr.M.Kameswara Rao, A.Srisaila [12] 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.

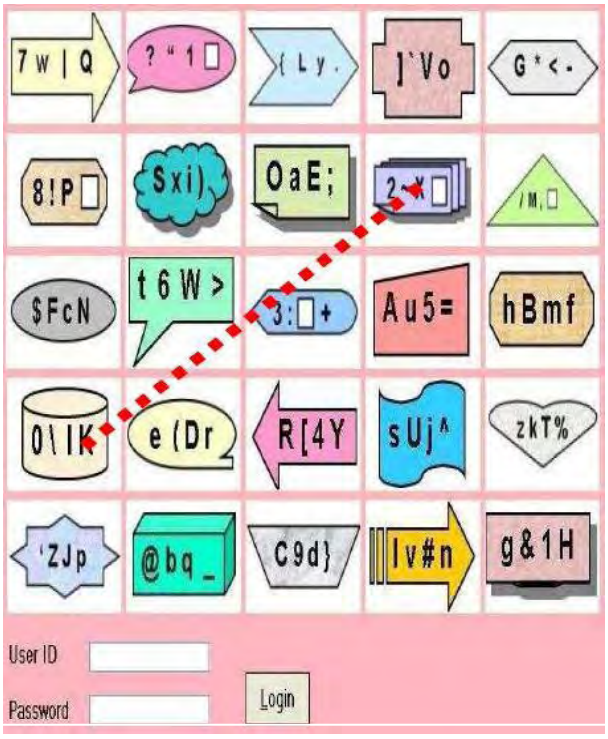

Fig 3. Password contains at least one character from each set of four characters depicted on the symbol of each block.

Dr. R.Satya Prasad and T.Srinivasa Ravi Kiran [13] 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 form 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.

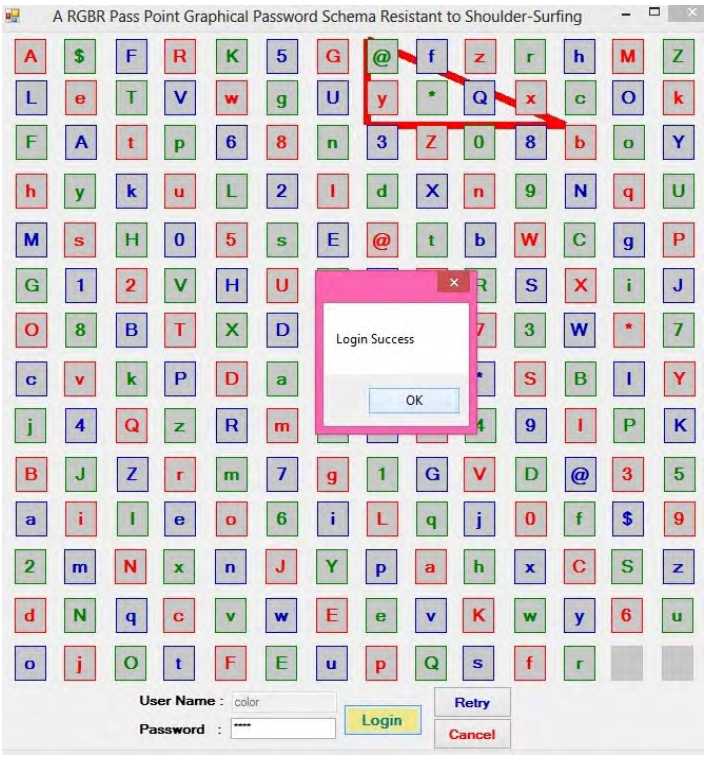

Fig 4.Triangle Formed by Clicking on the Cells “b@3b” Containing the Color Red, Green, Blue and Red Respectively for Second Login Attempt

T.Srinivasa Ravi Kiran and Dr. R.Satya Prasad [14] 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.

Fig 5. Login attempt is successful for fourth combination of password"8tN" and fourth combination of rotation transformations "90FlipX,90,180" in fourth login attempt.

III.PROPOSED WORK

The proposed scheme starts with the use of 5 × 5 grid formed using 25 blocks. Each block consists of a symbol. The symbol contains a set of four characters. The characters may numbers between 0 to 9, A to Z (Uppercase), a to z (Lowercase), Spaces and some special characters totally 95 character and 5 blank spaces are represented as shown in the Figure1. Passwords are input by typing or by mouse clicks.

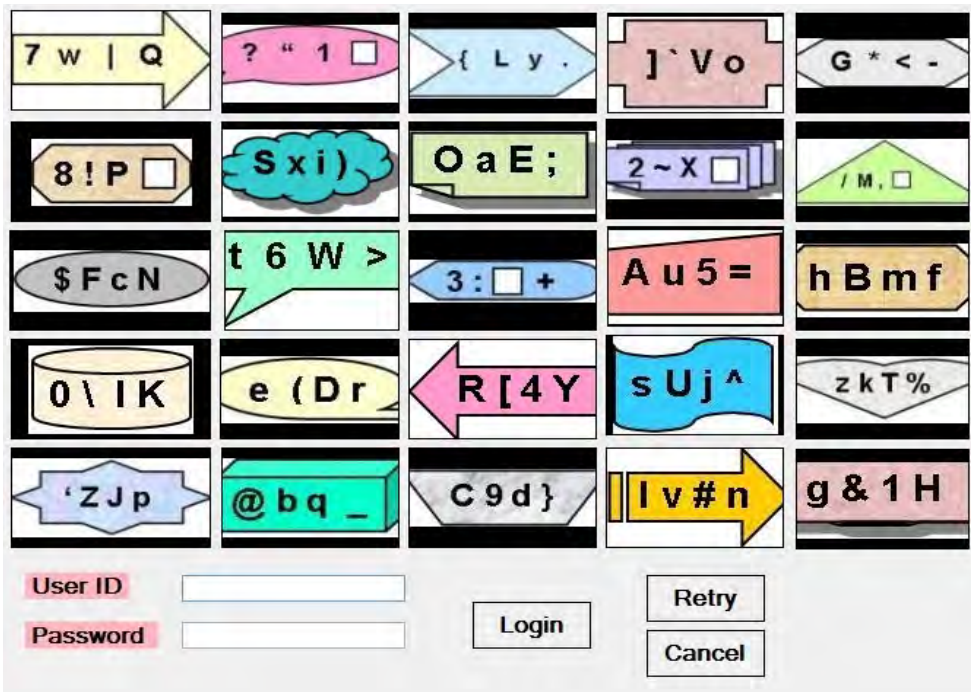

Fig 6: Proposed schema represented using 5 × 5 grid

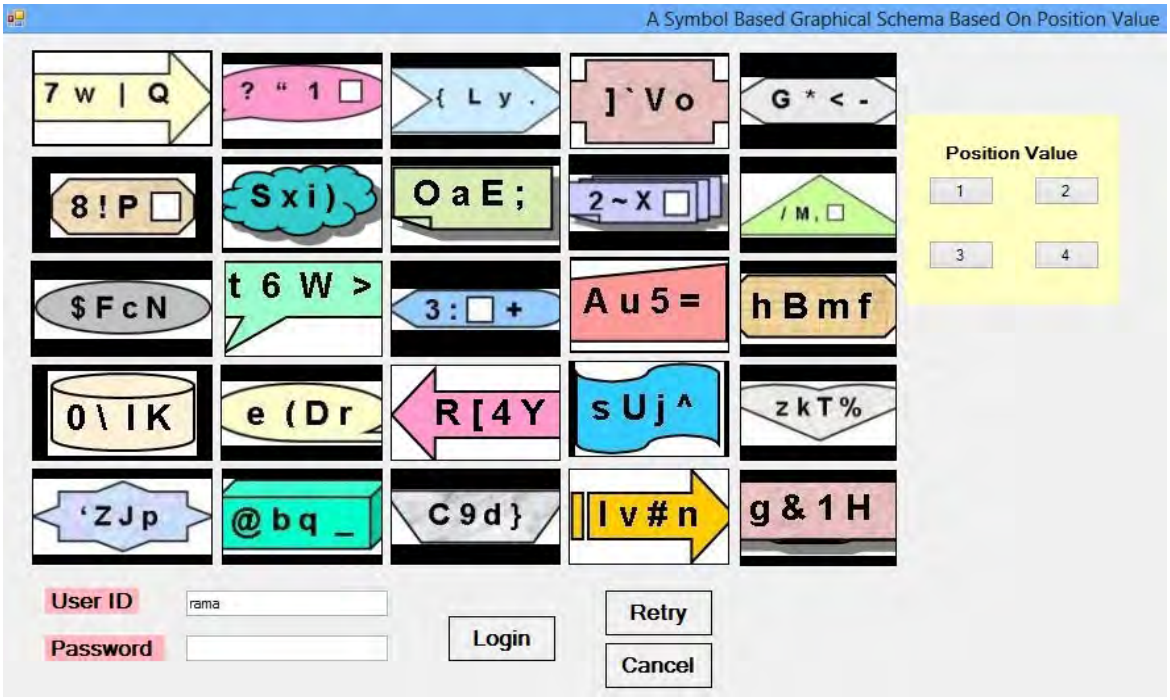

Fig 7.Schema to display position of the character from the symbol of the block from the 2 × 2 grid.

Algorithm for A Symbol Based Graphical Schema Based on Position Value

Step1. Start

Step2. Choose password character of length three

Step3. Select a block from 5 × 5 grid containing the first character

Step 4 . Select position of the first character of password from 2 × 2 grid in the same order per each login attempt

Step 5. Select a block from 5 × 5 grid containing the second character

Step 6. Select position of the second character of password from 2 × 2 grid in the same order per each login attempt

Step7. Select a block from 5 × 5 grid containing the third character

Step 8. Select position of the third character of password from 2 × 2 grid in the same order per each login attempt

Step 9. If three characters of password are identified in the symbols of 5 × 5 grid and matched with the corresponding positions of 2 × 2 grid then the login attempt is successful

Step10. 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 then the login attempt is failed

Step11. Stop

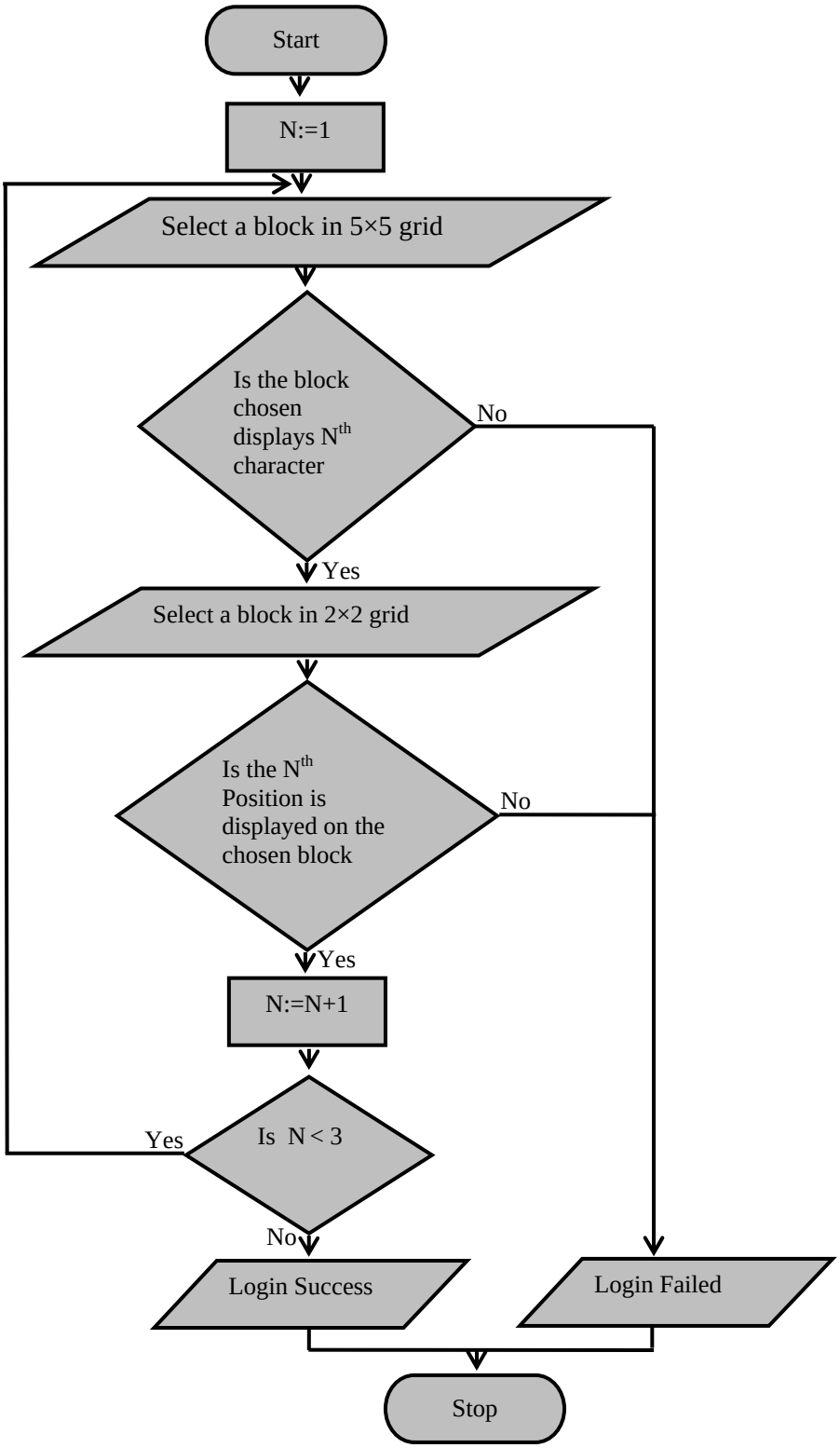

Fig 8. Flowchart Symbol Based Graphical Schema Based on Position Value

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.

Rule1: The user is supposed to select a block from the 5 × 5 grid so that the first character may be one of the characters from the set of four characters depicted on the symbol of the block.

E.g. The password selected at registration time is “7xD”. The first character 7 is depicted on the symbol of block from the row1, column1 of the 5 × 5 grid.

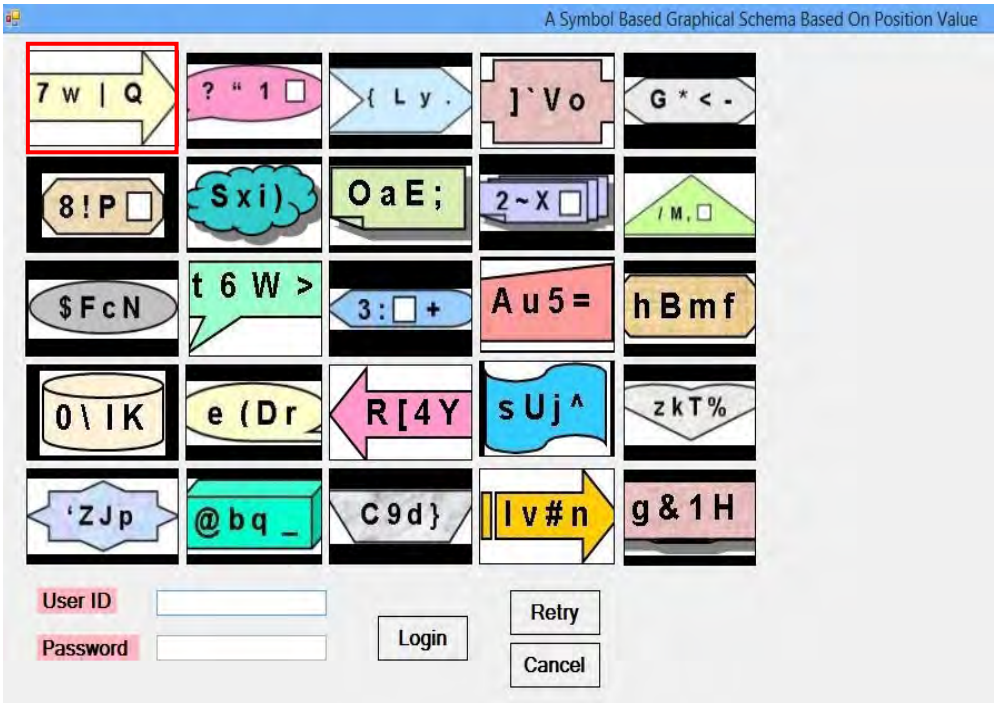

Fig 9. The first character 7 depicted on the symbol at row1, column1 of 5 × 5 grid

Rule2: The user is supposed to select the position of the character from the symbol of the block from the 2 × 2 grid.

E.g. The password selected at registration time is “7xD”. The position of first character of password 7 is depicted on first position on the symbol of block from the row1, column1 of the 2 × 2 grid.

Fig 10. The position of first character 7 depicted on row1, coiumn1 of 2 × 2 grid

Rule 3: The user is supposed to select a block from the 5 × 5 grid so that the second character may be one of the characters from the set of four characters depicted on the symbol of the block.
E.g. The password selected at registration time is “7xD”. The second character x is depicted on the symbol of block from the row2, column2 of the 5 × 5 grid.

Fig 11. The second character x depicted on the symbol at row2, column2 of 5 × 5 grid

Rule 4: The user is supposed to select the position of the character from the symbol of the block from the 2 × 2 grid.
E.g. The password selected at registration time is “7xD”. The position of second character of password x is depicted on second position on the symbol of block from the row1, column2 of the 2 × 2 grid.

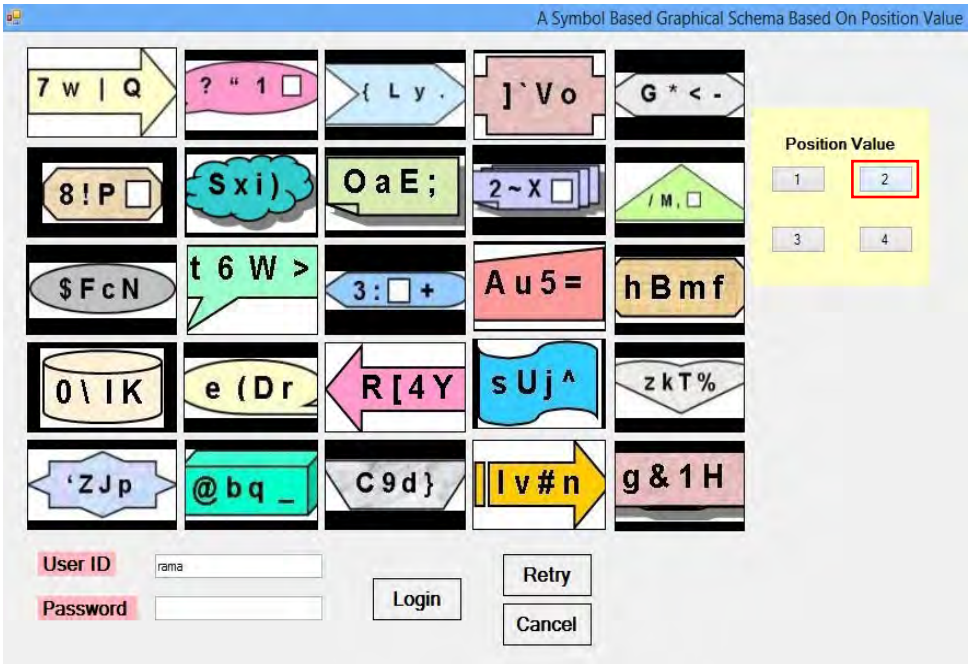

Fig 12. The position of second character x depicted on row1, coiumn2 of 2 × 2 grid

Rule 5: The user is supposed to select a block from the 5 × 5 grid so that the third character may be one of the characters from the set of four characters depicted on the symbol of the block.
E.g. The password selected at registration time is "7xD". The third character D is depicted on the symbol of block from the row4, column2 of the 5 × 5 grid.

Fig 13. The third character D depicted on the symbol at row4, column2 of 5 × 5 grid

Rule 6: The user is supposed to select the position of the character from the symbol of the block from the 2 × 2 grid.
E.g. The password selected at registration time is "7xD". The position of third character of password D is depicted on third position on the symbol of block from the row2, column1 of the 2 × 2 grid.

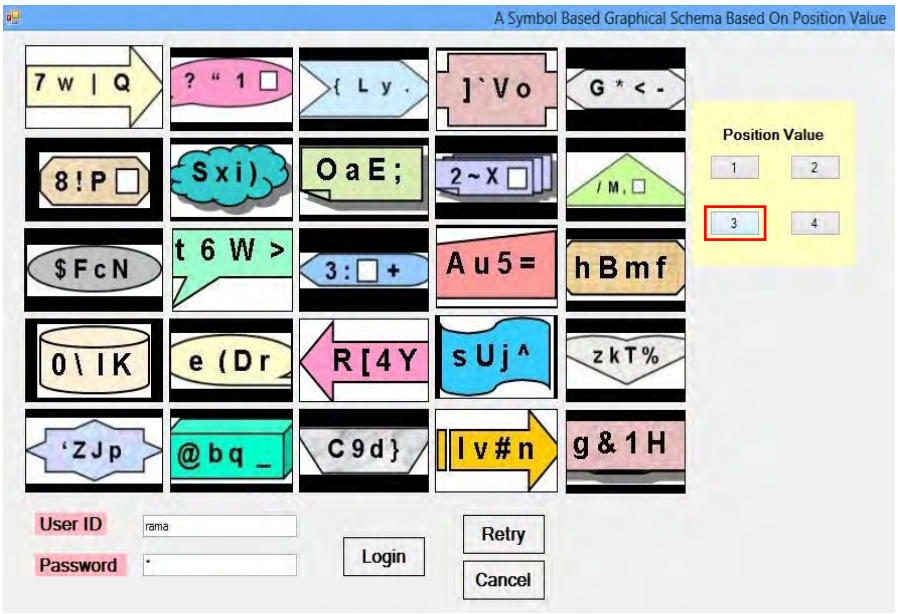

Fig 14. The position of third character D depicted on row2, column2 of 2 × 2 grid

Rule 7: Validate the login attempt after all the three characters of password are identified with the correct positions.
E.g. The login attempt is successful after matching the characters "7xD" of the password at positions one, two and three respectively.

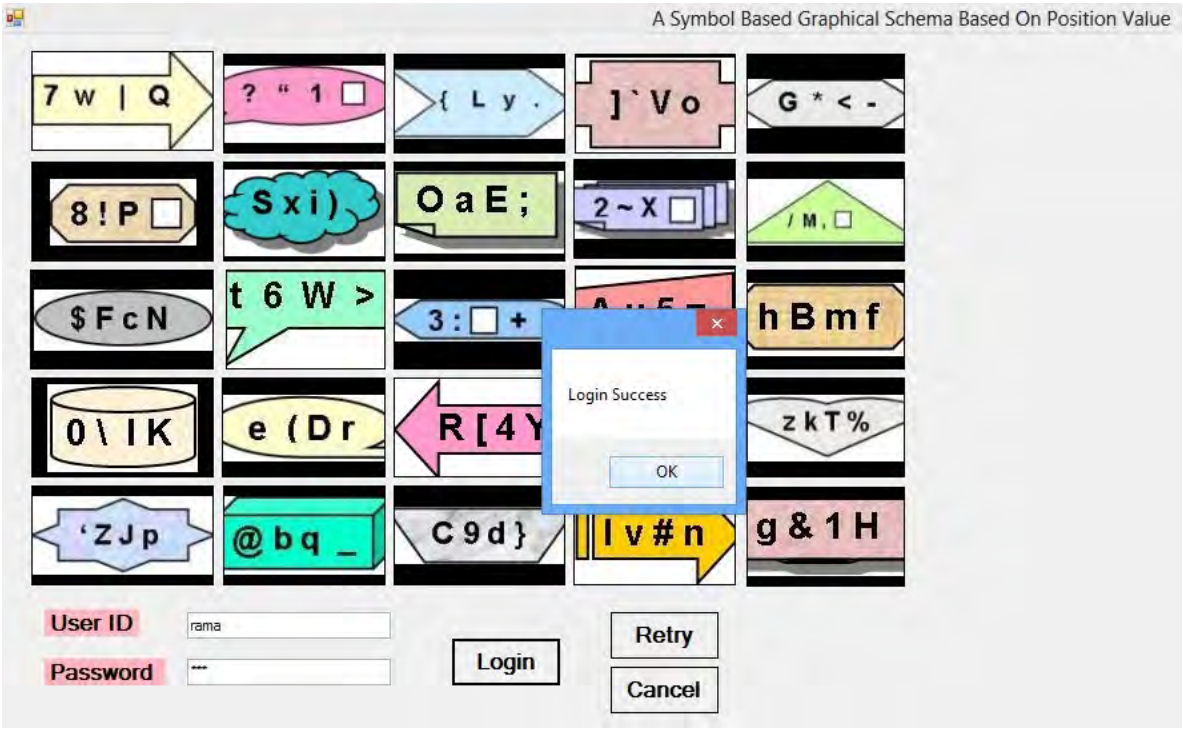

Fig 15. The login attempt successful after matching the characters "7xD" of the password at positions one, two and three respectively

Rule 8: 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.*

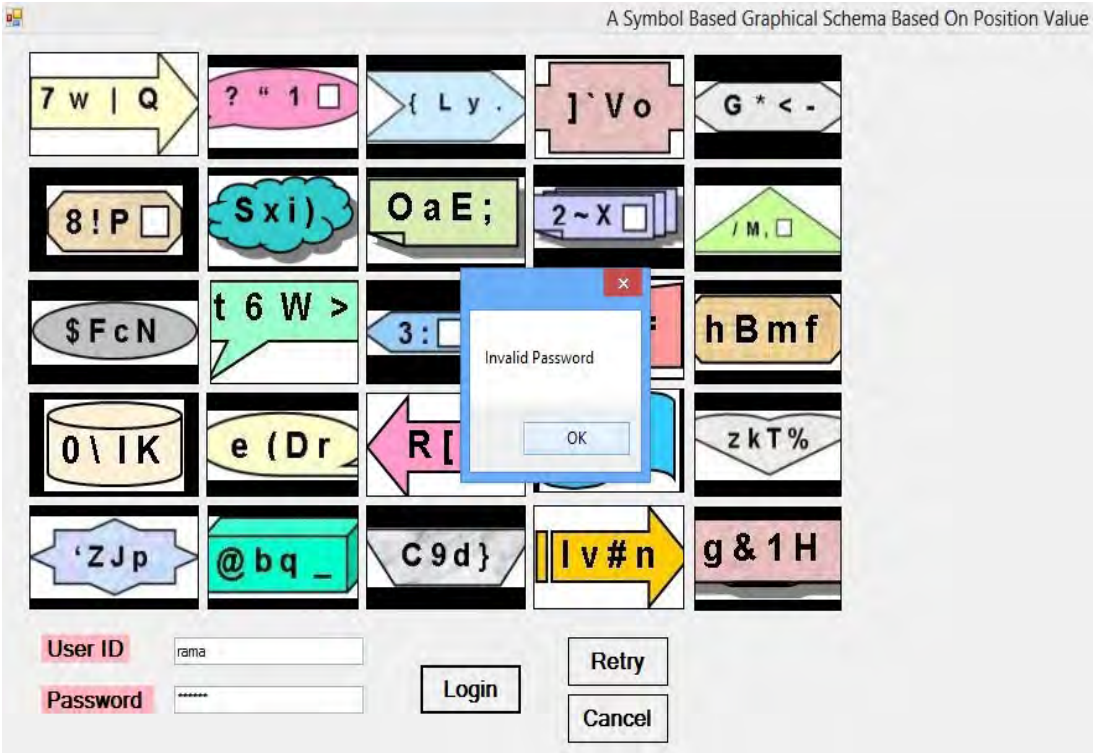

Fig 16. Login is invalid, if characters of password are not identified in the symbols of 5 × 5 grid or not matched with the corresponding positions of 2 × 2 grid.

IV. USABILITY STUDY & RESULTS

We conducted case study in lab with 30 participants out of which 5 were male and 25 were female. All the participants were post graduate students with their ages ranging from 23 to 25 years. A learning phase was conducted for practicing proposed on symbol based graphical schema. Initially they are given training explaining the concept of how to identify their password based on the rules proposed through the interface. The result was encouraging that trainee users were able to identify the characters of password from symbols of 5 × 5 grid and their positions from 2 × 2 grid.

The login attempt is successful for all the trainee users when three characters of password are identified in the symbols of 5 × 5 grid and matched with the corresponding positions of 2 × 2 grid. It took about 34.4 milliseconds on average to log in using i5 processor.

Peeping attack is the attack where an attacker gets the secret information through direct observation when the user is entering his or her password. 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 1: A Twelve point Recognization schema

SNo	Recognization Based Schema	A Twelve point scale of efficiency
1	G. E. Blonder	8
2	Passface	9
3	Jermyn, et al.	6
4	Hybrid User Authentication Approach	10
5	A Novel Graphical Scheme	10
6	A Symbol Based Graphical Schema	10
7	A RGBR Pass Point Graphical Password	10
8	Graphical Password Schema Based on Transformations	11
9	A Symbol Based Graphical Schema Based on Position Value	11

Table 2.Usability table of recognization 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	Applicable	R&A
1	G. E. Blonder	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N	N
2	Passface	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	Y
3	Jermyn, et al.	N	N	Y	N	Y	Y	Y	N	N	N	Y	Y
4	Hybrid User Authentication Approach	Y	Y	Y	N	Y	Y	Y	Y		N	Y	Y
5	A Novel Graphical Scheme	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
6	A Symbol Based Graphical Schema	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y
7	A RGBR Pass Point Graphical Password Schema	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
8	Graphical Password Schema Based on Transformations	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
9	A Symbol Based Graphical Scheme Based on Position Value	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Y - Yes N - No													

Table 3. Result of five trainee users

SNO	Login Name	Password	Location of first symbol in 5 × 5 grid (Row & Column wise)	Time to locate first symbol in 5 × 5 grid	Position of first character of the symbol from the 2 × 2 grid	Time in milliseconds to select position of first character from the 2 × 2 grid	Location of second symbol in 5 × 5 grid (Row & Column wise)	Time to locate second symbol in 5 × 5 grid	Position of second character of the symbol from the 2 × 2 grid	Time in milliseconds to select position of first character from the 2 × 2 grid	Location of third symbol in 5 × 5 grid (Row & Column wise)	Time to locate third symbol in 5 × 5 grid	Position of third character of the symbol from the 2 × 2 grid	Time in milliseconds to select position of third character from the 2 × 2 grid	Login time in milliseconds
1	rama	7xD	1 × 1	30	1	39	2 × 1	33	2	37	4 × 2	30	3	22	29
2	kiran	R+6	4 × 3	29	1	32	3 × 3	28	2	22	2 × 2	29	3	25	40
3	abhi	d%:	5 × 3	31	1	28	4 × 5	32	2	25	3 × 3	30	3	31	33
4	cherry	auT	3 × 3	29	1	31	4 × 4	33	2	32	4 × 5	30	3	33	34
5	satya	$9E	3 × 1	32	1	29	3 × 3	29	2	32	2 × 3	29	3	27	36
Mean time to *login* using i5 processor for the attempts by the trainee users															34.4

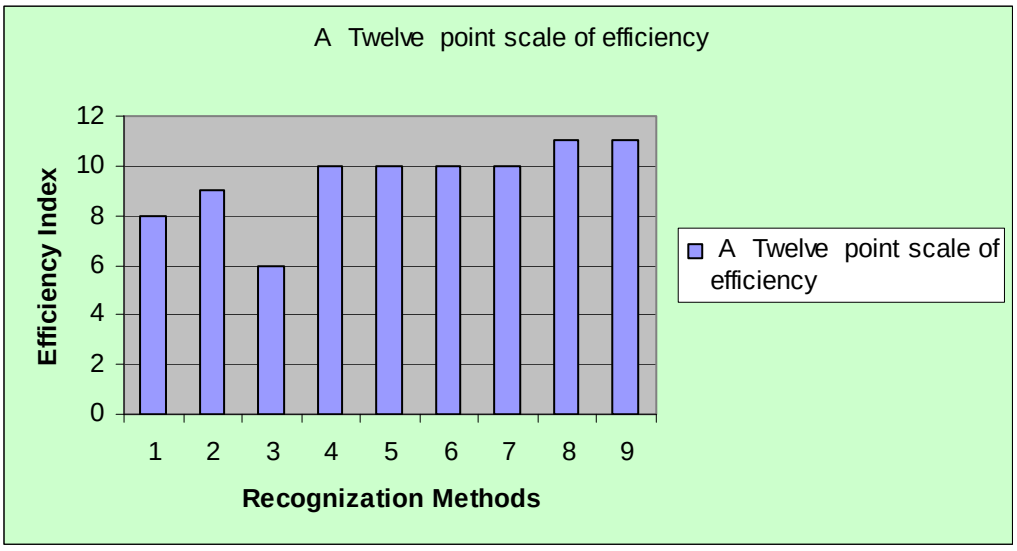

Fig 17. A histogram of twelve point scale of efficiency scale

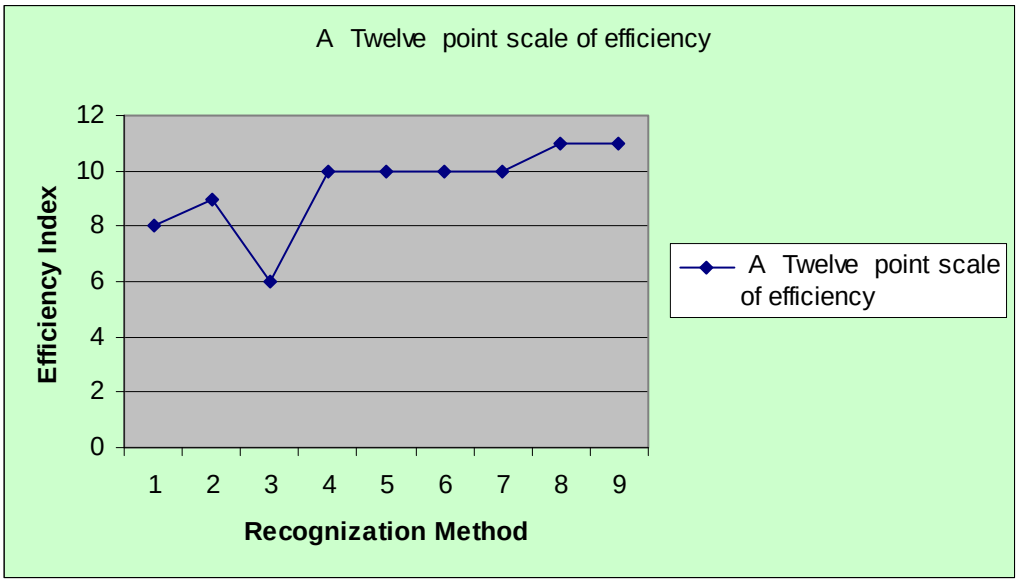

Fig 18. A line graph of twelve point scale of efficiency scale

V. CONCLUSION & FUTURE SCOPE

This work focused on the usability of graphical passwords over the alphanumerical passwords which seem to hold out the possibility of a much more secure system. The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords.

In this paper, 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 and then the user is supposed to select the position of the character from the symbol of the block from the 2 × 2 grid. The password length at registration time is three.

In future, the presented work can be extended to N-length password. The user can design N × N grid and each cell of the grid consisting of symbol containing N-number of characters.

VI.REFERENCES

[1] Saikat Chakrabarti et al., “Graphical Passwords: Drawing A Secret With Rotation As a New Degree Of Freedom”.
[2] Ziran Zheng Et Al, “A Hybrid Password Authentication Scheme Based On Shape And Text”, Journal Of Computers, Vol. 5, No. 5, May 2010.
[3] R. N. Shepard, “Recognition memory for words, sentences and pictures”, Journal of Verbal Learning and Verbal Behavior, 6:156–163, 1967.
[4] Michael Kimwele, “Strengths of a Colored Graphical Password Scheme”, International Journal of Reviews in Computing © 2009-2010 IJRIC& LLS, E-ISSN: 2076-331X.
[5] X. Suo, U. Direction, Y. Zhu, and X. Suo , “A design and analysis of graphical password”, 2006.
[6] R. Biddle, S. Chiasson, and P. van Oorschot, “Graphical passwords: learning from the first twelve years”, Technical report, 2011.
[7] R. A. Khot, K. Srinathan, and P. Kumaraguru.Marasim, “A novel jigsaw based authentication scheme using tagging”, In Proceedings of the 2011 annual conference on Human factors in computing systems,CHI 11, pages 2605-2614, New York, NY, USA, 2011,ACM.
[8] Dr. Manish Manoria and Ankur Jain, “Graphical User Authentication for E-Transaction”, International Journal of Computer Science and Network (IJCSN), Volume 1, Issue 5, October 2012 ,www.ijcsn.org, ISSN 2277-5420.
[9] Huanyu Zhao et al, “S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme”.
[10] T.S Ravi Kiran and Y.RamaKrishna, "Combining Captcha And Graphical Passwords For User Authentication ", IJRIM Volume 2, Issue 4, April 2012.
[11] 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.
[12] 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, No1, September 2013.
[13] Dr. R.Satya Prasad, T.Srinivasa Ravi Kiran, “A RGBR PASS POINT GRAPHICAL PASSWORD SCHEMA RESISTANT TO SHOULDERSURFING ”, IJCSE(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, 175-188© IASET, www.iaset.us.
[14] 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.
[15] Partha 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.
[16] D. Hong, S. Man, B. Hawes, and M. Mathews. “A password scheme strongly resistant to spyware”. In Proceedings of International conference on security and management, Las Vergas, NV, 2002.

[17] D. Nali and J. Thorpe, “Analyzing user choice in graphical passwords”. In Technical Report, School of Information Technology and Engineering, University of Ottawa, Canada, May 27 2004.
[18] J. Thorpe and P. C. v. Oorschot, “Graphical dictionaries and the memorable space of graphical passwords”. In proceedings of the 13th USENIX Security Symposium, San Deigo, CA, 2004.
[19] J. Thorpe and P. C. v. Oorschot, “Towards secure design choices for implementing graphical passwords”. In Proceedings of the 20th Annual Computer Security Applications Conference, Tucson, Arizona, 2004.
[20] Daniel LeBlanc, et al., “Guessing Click-Based Graphical Passwords by Eye Tracking”, 2010 Eighth Annual International Conference on Privacy, Security and Trust.
[21] M. K. Rao and S. Yalamanchili, “Novel shoulder-surfing resistant authentication schemes using text-graphical passwords”, International Journal of Information & Network Security, vol. 1, no. 3, pp. 163-170, Aug. 2012.

VII. AUTHOR PROFILES

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 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 five research papers in various international journals.

Dr. R. Satya Prasad Received Ph.D. degree in Computer Science in the faculty of Engineering in 2007 from Acharya Nagarjuna University, Andhra Pradesh. He received gold medal from Acharya Nagarjuna University for his outstanding performance in a first rank in Masters Degree. He is currently working as Associative Professor in the Department of Computer Science & Engineering, Acharya Nagarjuna University. His current research is focused on Software Engineering. He published 110 research papers in National & Intenational Journals. He received Dr.Abdul Kalam Lift Time Achievement Award for his remarkable achievements in the field of Teaching,Research and Publications.