A Robust Scheme for Impervious Authentication

T. Srinivasa Ravi Kiran, A.Srisaila, A. Lakshmanrao

Abstract Abstract— Now a day's every one using the passwords for user authentication. Most often passwords are alphanumeric, consisting of letters, numbers and symbols. A shoulder surfer can easily watch the password if the password is too short. If the password too complex and lengthy it is difficult for the user to remember it. At the same time passwords have to be changed every few months to take care of security. To overcome these problems, graphical passwords are developed. The motivation behind selecting an authentication mechanism scheme was that persons can simply evoke pictures rather than remembering lengthy and complex text based passwords.

In this paper, we present a new, comprehensible, recall-based graphical password scheme where the user is required to recognize the pentagon for some specific permutations of secret characters on the existing display. The token holder is expected to select the certain password permutations in the same order cyclically per each login attempt.

For example the user go for first permutation of password for first login in attempt, second permutation of password for second login attempt, third permutation of password for third login attempt, fourth permutation of password for fourth login attempt, fifth permutation of password for fifth login attempt and sixth permutation of password for sixth login attempt.

Keywords—password, authentication, security, shoulder-surfing, interface, pentagon

INTRODUCTION

A password could be a confidential word used for user authentication to set up self identity. Today information security is the most depicting issue. Authentication is the method of validating a claim made by a person, computer or process etc. User confirmation is a most vital part in most PC privacy. It offers the client a means of access method and user accountability[1].Citizens are using passwords frequently, lot of times for doing online banking transactions, for social network access and to verify their emails. The existing password techniques are insecure. Most of the digital systems are still using textual passwords as a part of security. The technique of opting textual passwords has major drawbacks [2]. It is not possible for a human to memorize a long complex string of characters to operate as a secrete hence a user are likely to select a small and simple to remember textual token Ziran Zheng *et al.* [3]. If user does not use the passwords frequently he/she may vulnerable to forgetting. Textual passwords are open to shoulder-surfing, hidden-camera and spy ware attacks. People rely on graphical authentication methods as it presents higher security from text-based passwords [4]. The promising password space of a graphical password scheme is more than the text based schemes and consequently provides higher level of security. Due to this advantage, there is growing interest in graphical password. In Graphical Password schemes images are used as an alternative of alphanumerical passwords [5].The Graphical Password schemes are developed to protect the user and/or application privileges from hacking attempts [6].

Revised Manuscript Received on December 22, 2018.

Dr. T. Srinivasa Ravi Kiran, Department of Computer Science P.B.Siddhartha College of Arts & Science Vijayawada, India (e-mail : kirantsr1@gmail.com)

Dr. A.Srisaila, Department of Information Technology V.R.Siddhartha Engineering College Vijayawada, India (e-mail : sr.saila@gmail.com)

A. Lakshmanrao, Department of Computer Science & Engineering Pragati Engineering College Surampalem, India (e-mail : akshman.a@pragati.ac.in)

RELATED WORK

Blander [7] proposed a click based graphical password systems to login. The user is supposed to click ordered sequence of five pass points on the images of the presented interface as shown in the presented interface. According to Jermyn *et al.* [8], the client is supposed to "Draw a Secret" (DAS) on the grid of the presented interface. The password is the straightforward pattern presented in a grid. This method is key stroke independent and enables the user to draw the patter easily. Users are not required to remember the alphanumeric string. Sobrado and Birget [9] discussed "Triangle Scheme" in which a number of pass-objects are presented on the interface. The pass objects are chosen by the client during initial sign-up stage, along with lots of other "decoy" objects. After that point the client is required to discover the pass-questions and clicks inside the convex hull framed by all the pass-tokens. As the password space of the hull is huge, the likelihood of compromising the password is low.

The scheme S3PAS proposed by Huanyu Zhao *et al.* [10] displays 10×10 fixed grid containing 94 printable characters consisting of alphabets, digits and special symbols. The length of the password is fixed string of 4 characters such that any three character combination can form a triangle on the accessible grid. For example, if the password selected is "5Vgw" then consider the possible combinations viz.; "5Vg","Vgw","gw5" and "w5V" successfully form a triangular pattern on the existing interface separately. The client has to select in the interface in precise manner in order to be authenticated positively.

T.Srinivasa Ravi Kiran, *et al.* [11] proposed a graphical password authentication scheme resistant to peeping attack which initiate with recognizing quadruplets formed from the client combination starting with the initial character and rotating one character towards right such a manner that the last character in the password amalgamation come into view as the first character of the password combination. For instance, if the password chosen at the time of registration is "T2D8h" then the quadruplets formed are "T2D8T", "2D8h2", "D8hTD", "8hT28" and "hT2Dh". It is mandatory for the user to pick the arrangement of the password blends in the expected fashion rotated for every login attempt.

Dr. R.Satya Prasad *et al.* [12] proposed shoulder surfing resistant RGBR pass point graphical password schema starts with identifying triangle produced by selecting the button

having colors red, green, blue & red of the existing interface in the same way. In any case one permutation chosen from the secret have to outline the three sides and at the same time the initial and terminating tokens of password arrangement are matching. For instance the password selected at the phase of registration is “A2#4” on first, second, third, fourth, and fifth login endeavors the user selects the arrangements “A2#4A”, “2#4A2”, “#4A2#”, and “4A2#4” in the precise fashion.

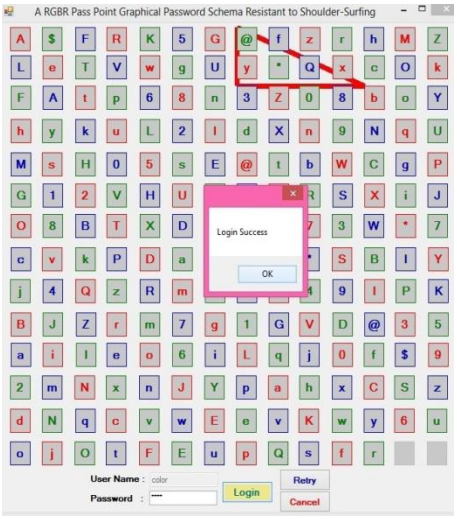


Fig.1. The three sides produced by means of tapping on the cells “b@3b” contains the colors red, green, blue and red correspondingly and login try is success.

II. PROJECTED SCHEME

In the anticipated plan, we make utilization of a 10×10 table created with 94 printable character set with spaces for separation as appearing in Figure1. Secret word amalgamations are approved utilizing by mouse taps. The arranged plan begins with recognizing pentagon shaped by tapping on the squares on display. Suppose a pentagon is not framed then that blend can be overlooked. The determination of explicit pentagon on the current display takes the client to the ensuing phase.

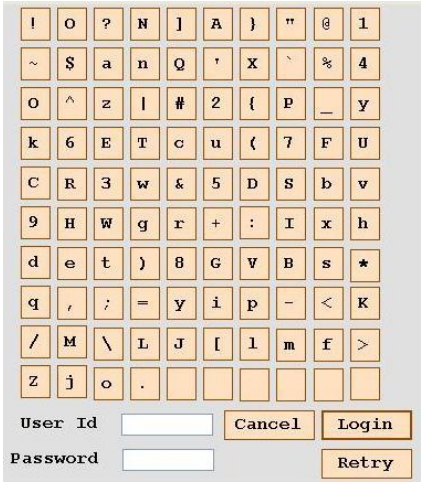
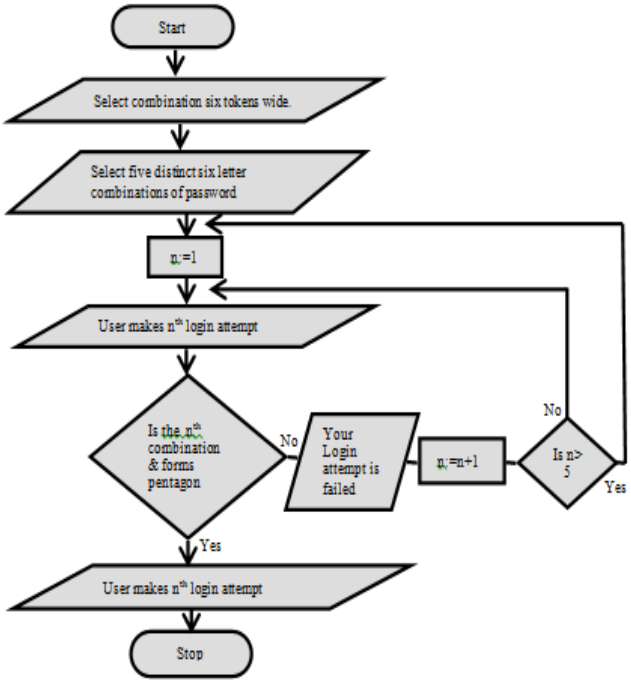


Fig.2. Actual Display.

Secret phrase combinations are contribution by six mouse taps on the exhibited screen. For instance, secret word chosen at sign-up time is "3#7:tH" at that point the plausible pentagons shaped by tapping on the cells are "3#7:t3", "#7:tH#", "7:tH37", ":tH3#:", "tH3#7t" that is pivoting unique secret key character blend one position from left to right consistently and first character must be same as the last character. The clients are instructed to enter the blend of password character episodically in the predictable order for every login. For instance at first, second, third, fourth, fifth and sixth login endeavors the user are relied upon to pick the blends "3#7:t3", "#7:tH#", "7:tH37",":tH3#:", "tH3#7t" and "3#7:t3, correspondingly. No less than one blend considered from the secret key certainly shapes the pentagon and the initial token and terminating token must be same. On the off chance that the blend of characters is with the end goal that a pentagon can't be shaped, that password blend can be disregarded. Pentagon can not be framed if client chooses a mix such that the primary token is not alike the terminal token.

Algorithm:

1. Start
2. Consider a secret word of six character length at sign-up
3. Select five distinct six character amalgamations of secret character, pivoting from left to right.
4. Client make N^{th} entry attempt via selecting secret word amalgamation in the predicted fashion in the accessible display.
5. Suppose the client opts secret word token amalgamation in the predicted fashion and it forms a pentagon then that entry endeavor is successful, evaluate the next amalgamation.
6. Suppose client does not choose secret token combination in the predicted fashion or does not form pentagon shape the entry process is foiled, ignore that amalgamation of secret tokens and choose next amalgamation of secret tokens so that all the amalgamations of secret word tokens form a pentagon.
7. Stop



Flow Chart:

Step 1: For first time, entry is valid for the amalgamation "3#7:t3".

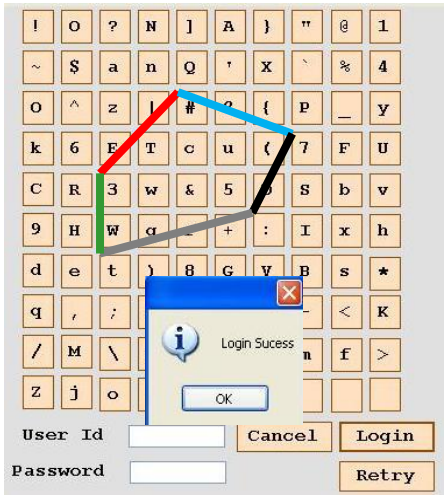


Fig.3. Entry passed by Clicking on the Cells "3#7:t3" for first time.

Step 2: Entry foiled for sequence "3#7:t3" at second entry since the client chooses wrong attempt.

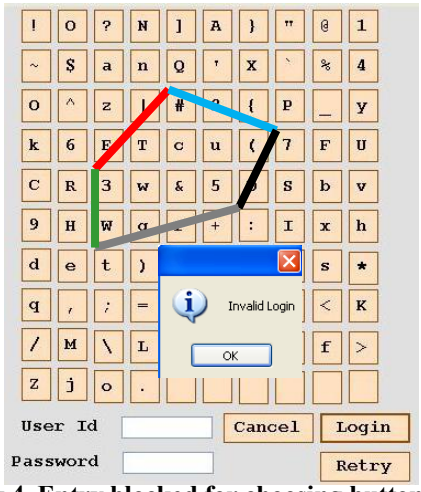


Fig.4. Entry blocked for choosing buttons "3#7:t3" at second attempt.

Step 3: Entry is valid for the combination "#7:tH#" at second time

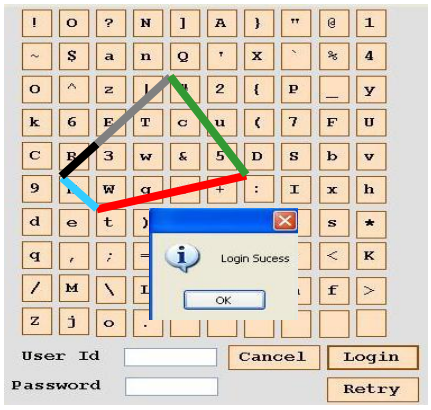


Fig.5. Entry passed Clicking on the Cells "#7:tH#" at second time.

Step 4: Entry successful for amalgamation "7:tH37" at third time

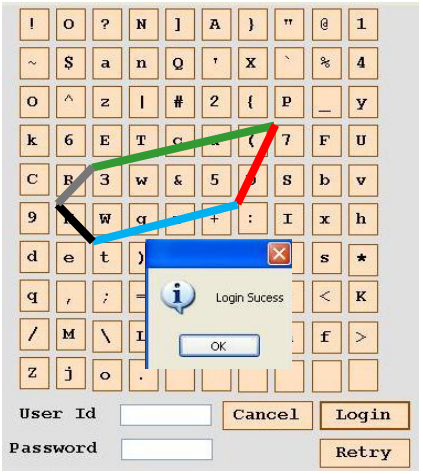


Fig.6. Formation of pentagon by choosing the buttons "7:tH37" at third time.

Step 5: Entry successful for amalgamation ":tH3#:" at fourth time

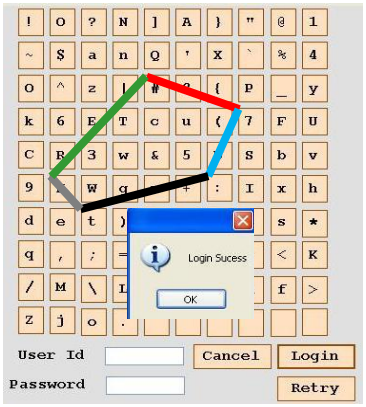


Fig.7. Formation of pentagon by choosing the buttons "#7:tH#" at fourth try

Step 6: Entry successful for amalgamation "tH3#7t" at fifth try

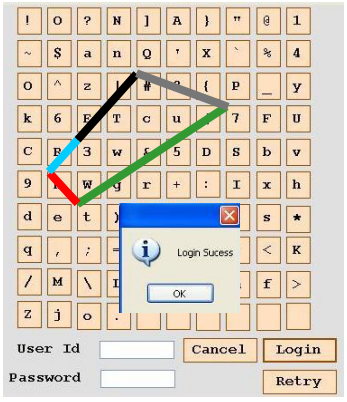


Fig.8. Formation of pentagon by choosing the buttons "tH3#7t" at Fifth try

Step 7: Entry successful for amalgamation “H3#7:H” at sixth try

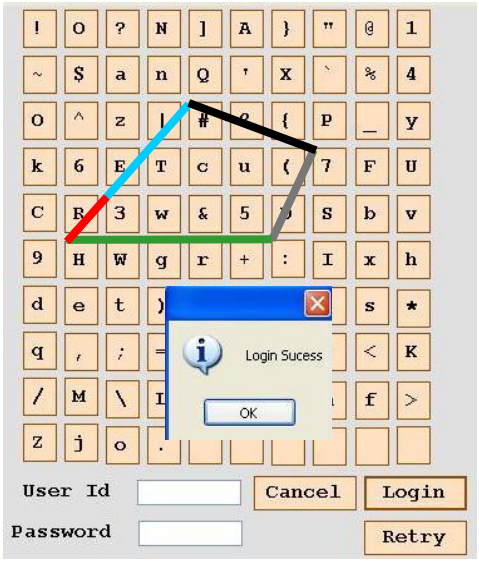


Fig.9. Formation of pentagon by choosing the buttons “H3#7:H” at Sixth try.

Step 8: If the initial token is different from terminal token it leads to a state where pentagon cannot be formed this amalgamation can be ignored. Select appropriate amalgamation of secret tokens in such a manner that a pentagon is formed.

E.g. Client selects buttons containing the tokens “3#7:tH” respectively, the initial token “3” is different from the terminal token “H” and a pentagon cannot be formed so the amalgamation is overlooked. Select proper amalgamation of tokens so that a pentagon is formed.

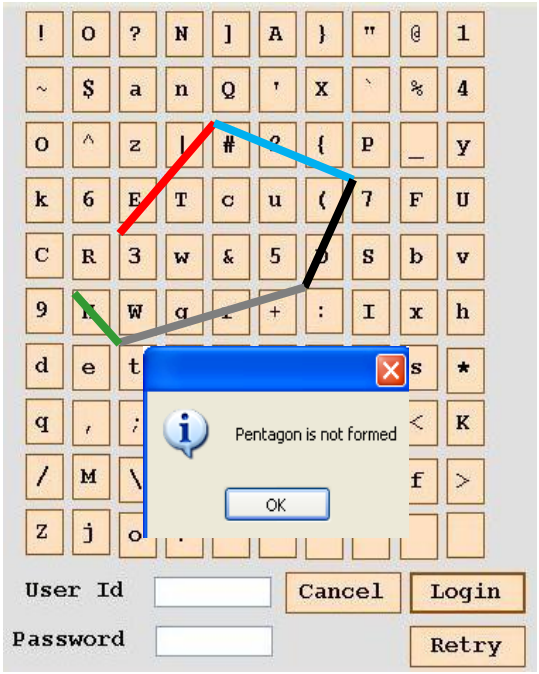


Fig.10. Pentagan not formed by selecting buttons “3#7:tH”. Amalgamation overlooked.

III. RESULTS & USEFULNESS STUDY

The outcomes were hopeful and clients recognized pentagons produced by tapping on the buttons in the specific manner. It takes 44 milliseconds on normal sign-in. Peeping attacks were blocked with the projected scheme since the client clicks on non secret token buttons.

S. No.	Login name	Password	Pass1	Login time for pass1 in milliseconds	Pass2	Login time for pass2 in milliseconds
1	navya	3#7:tH	3#7:t3	38	#7:tH#	39
2	sharvya	cS<8g w	cS<8gc	44	S<8gcS	45
3	saritha	a2+)R^	a2+)ra	45	2+)R^2	46
4	kvs	s-y8+b	s-y8+s	39	-y8+b-	40
5	asha	r5IpJ=	r5IpJr	45	5IpJr5	39
6	suresh	w8:#n6	w8:#n w	44	8:#nw8	42

Table.1. Login time for first & second passes

S. No.	Login name	Password	Pass3	Logintime for pass3 in milliseconds	Pass 4	Login time for pass4 in milliseconds
1	navya	3#7:tH	7:tH37	43	:tH3#:	44
2	sharvya	cS<8gw	<8gwc<	46	8gwcs8	46
3	saritha	a2+)R^	+)R^a+	47	)R^a2)	47
4	kvs	s-y8+b	y8+bsy	41	8+bs-8	39
5	asha	r5IpJ=	IpJ=rI	46	pJ=r5p	41
6	suresh	w8:#n6	:#n6w:	44	#n6w8#	43

Table.2. Login time for third & fourth passes

S. No.	Login name	Password	Pass5	Logintime for pass5 in milliseconds	Pass6	Login time for pass6 in milliseconds
1	navya	3#7:tH	tH3#7t	45	H3#7:H	43
2	sharvya	cS<8gw	gwcs<g	41	wcs8gw	42
3	saritha	a2+)R^	R^a2+R	42	^a2+)^	44
4	kvs	s-y8+b	+bs-y+	45	bs-y+b	47
5	asha	r5IpJ=	Jr5IpJ	47	=r5Ip=	46
6	suresh	w8:#n6	n6w8: n	46	6w8:#6	45

Table.3. Login time for third & fourth passes

S. No.	Login name	Password	Average login time in milliseconds for six pass
1	navya	3#7:tH	42
2	sharvya	cS<8gw	44
3	saritha	a2+)R^	45
4	kvs	s-y8+b	42
5	asha	r5IpJ=	44
6	suresh	w8:#n6	44
Average login time for 6 passes using i5 processor			44

Table.4. Login time for third & fourth passes

Row	ReorganizationBased Schema	User Features													
		Satisfaction												Efficiency	Effectiven
		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	Blonder Schema	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N
2	Jermyn Schema	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	N	N	Y
3	Sobrado& Biget Schema	N	N	Y	N	Y	Y	Y	N	N	N	N	N	Y	Y
4	Graphical Passwords:A Survey	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y
5	S3PASS	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y
6	Computer Security: Principle and Practices	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y
7	Shape & Text Based Schema	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y
8	A Novel Graphical Password Scheme	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y
9	RGBR Pass Point Scheme	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y
10	A Pattern Based Scheme	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y

Y - Yes N - No

Table .5. Usability table of recognization based schema

Row	Proposed schema	Is actual password protected?	Is login phase verified with password permutations?	Password space	Does the passwords permutations forms quadruplet?	Drawbacks	Security attacks pervious to	Impervious to security attacks	Average login time in milliseconds using i5 processor	Robustness of the password scheme	Robustness of each password permutation
1	Blonder	N	N	N	N	P1 P2	S D D	B S G	NS	NS	NS
2	Jermyn	N	N	4×4 Grid	N	P1 P2	D S B	S G	NS	NS	NS
3	Sobrado&Biget schema	N	N	10× 14 Grid	N	P2	N S	D S S	NS	NS	NS
4	Graphical Passwords :A Survey	N	N	NS	N	P1 P2	N S	B D	NS	NS	NS
5	S3-Pass	Y	Y	5×5 Grid	N	P1 L1	N S	S H P	NS	NS	NS
6	Computer Security: Principle and Practices	N	N	NS	N	P1 P2	N S	P	NS	NS	NS
7	Shape & Text Based Schema	Y	Y	NS	N	P2	N S	S H P	NS	NS	NS
8	A Novel Graphical Password Scheme	Y	Y	10× 10 Grid	N	N S	N S	S H R	38.46	99.96 %	99.23 %
9	RGBR Pass Point Scheme	N	N	14× 14 Grid	N	N S	N S	S H P	39.30	96.48 %	99.61 %
10	An Innovative graphical password scheme	Y	Y	10× 10 Grid	N	T	N S	R S H P B	44	99.96 %	99.23 %

NOTE: Y-Yes, N-No, NS-Not Specified

P1-Password space is small, P2-Password strength/ robustness not specified, L- Lengthier login processes, T- Little training is requires to memorize the password permutations

S- Spyware, B-Brute force, D-Dictionary, S-Shoulder surfing, G- Guessing, R-Random click attacks, H-Hidden camera, P-Spyware

Table.6. A comparative analysis of innovative graphical password schema.

IV. A COMPARATIVE ANALYSIS

The interface is a 10×10 grid where as the user is instructed to form a pentagon with password blends considered from the password chosen at sign-up. The type of evaluation is the first attempt in password authentication system.I have analyzed 9 schemas of graphical password authentications. Among all these schemas only three have explored the approach of considering password blends from the original password. The schemas of the other authors also did not attempt the robustness of the original password and password bends. In this proposed schema the robustness of the password and password blends are correctly have been defined and fixed at 99.968% and 99.23% respectively. The password and password blends reduce the probability of cracking by the shoulder surfers.

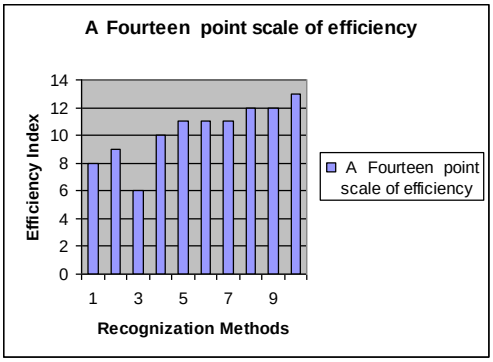


Fig.11. Histogram for fourteen point scale of efficiency.

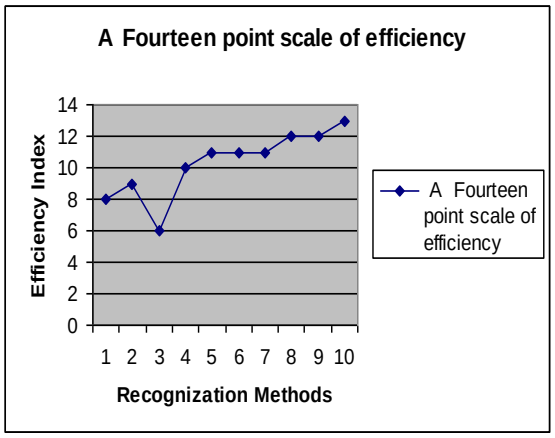


Fig.12. Line Graph for fourteen point scale of efficiency.

REFERENCES

1. Blonder, "G.E. Graphical Passwords", United States Patent 5,559,961.1996.
2. 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.
3. Sobrado L. and Birget J., "Graphical Passwords, the Rutgers Scholar", Rutgers University, Camden New Jersey 081024, 2002.
4. X. Suo et al., "Graphical Passwords:A Survey", In Proceedings of Annual Computer Security Applications Conference, 2005, pp. 463–472.
5. 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.
6. W. Stallings, L. Brown, "Computer Security: Principle and Practices", Pearson Education, 2008.
7. Ziran Zheng et al., "A Hybrid Password Authentication Scheme Based on Shape and Text", Journal of Computers, Vol. 5, No. 5, May 2010.
8. V. Bhusari, "Graphical Authentication Based Techniques", International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013, ISSN: 2250-3153.
9. 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
10. 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.
11. T.Srinivasa Ravi Kiran et al. "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. R.Satya Prasad et al., "A RGBR Pass Point Graphical Password Schema Resistant to Shoulder Surfing", 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, pp.175-188, IASET, ww.iaset.us.