Journal of Engineering and Applied Sciences 12 (7): 1738-1745, 2017
ISSN: 1816-949X

Robust Authentication Approach Based on Keyboard Graphical Password

Mehdi Ebady Manaa and Marwa K. Al-Rikaby
College of Information Technology, University of Babylon, Babil, Iraq

Abstract: Now a days, it is fairly clear that the curve of challenges of authorized access has been increased sharply. This is due to the modern technologies and the easy use of the global access to internet. This led to increase the numerous of malicious attacks each a part of time against the authorized access. The important point of the complexity is the widely spread of the Internet coincide with the existing of threats. This study combines the knowledge of the security and the building of high robust authentication access in order to avoid the brute force attack. A new authentication approach is presented in this study for the purpose of strengthen text password. This technique is used graphical password which is generated an extra robust authentication access without needed to any of the additional resources. That is in this technique, the Qwerty keyboard is used only. In the core of this research, the mathematical model and the euclidean distance are used for the designing and implementation of the proposed system into two main phases. Firstly, the registration phase which tell us that the users input all credential information and generate their graphical password.While, the second phase is "the logging in" which used the information registered in the registration phase. The saved graphical password is tested with the registration password by the euclidean distance. The existing results are addressed which showed that the average time of the users logging in about 9 sec.

Key words: Graphical password, information security, user authentication, security primitive, credential

INTRODUCTION

Computers consider the main tool that provide different services for a society via the Internet. They become an integral part of every aspects in our life. Information such as medical, criminal, personal and financial records which can be used to pay bill and mange other services are saved in these computers (Monrose and Rubin, 1997). Computer resources may exposure to threats which access to these resources in unauthorized way. Organization should be committed to provide the security criteria CIA (Confidentiality, Integrity and Availability). These criteria provide a securely data and should be available with no error for the people within these organizations. Confidentiality means protect data from imposter (attacker). Hence, losing any factor of CIA can cause significant harm on organizations (Bhaya and Manaa, 2014). To save a computer data from being attacked, users must provide a strong password and maintain the secrecy of their access control. Traditional password consists of a common words, phrases or terms. Generally, the traditional password consider weak because an intruder can guess it using a dictionary attack (Lee *et al*., 2007; Gokhale and Waghmare, 2016). Moving the attention to the authorized access, the common definition for user authentication is the process of preventing unauthorized access for reaching to computer data. It is categorized in three stages (access request, information extraction and authenticity process). Figure 1 shows the main techniques that be used with authentication process (Shanmugapriya and Padmavathi, 2009; Bhanushali *et al*., 2015).

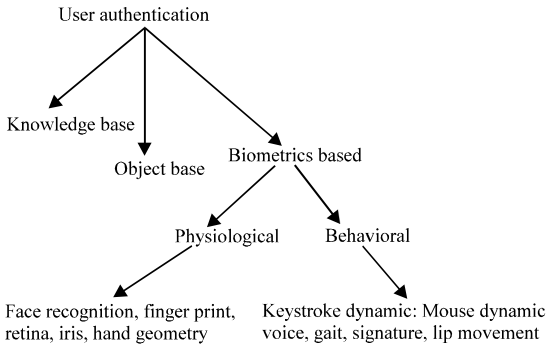

Fig. 1: User authentication techniques

The first technique is knowledge based or textual based authentication using username and password which stay a dominant technique currently. However, many resources show that this technique fairly weak and in a high risk of information leak. The common example of this technique is textual username and password which can be forgotten after a long time or stolen by the imposter. In addition, it vulnerable to attacks such as

Corresponding Author: Mehdi Ebady Manaa, College of Information Technology, University of Babylon, Babil, Iraq

Table 1: Authentication schemes comparison

	Authentication schemes				
			Graphical based click password		
Item	Traditional text based	Biometric/token based	Pass point	Cued Click Point (GCP)	Persuasive Cued Click (PCCP)
Security	Less secure	High secure	Less secure (hot spot points)	Less secure	Highest secure
Memoeability	Easy	Complex	Easiest	Easiest	Easiest
Cost	Small	High	Small	Small	Small
Usability	Easy	Complex	Easiest	Easiest	Easiest
GUI	Not attractive	Attractive	More attactive	More attactive	More attactive
Time to login	Small	High	High	Highest	High

shoulder surfing (Kumar *et al*., 2007; Mule and Mali, 2015; Borkar and Golar, 2015). Object based is categorized with someone has something or possession. It is commonly merged with user name and password authentication.

Graphical password comes to play a vital role in knowledge based techniques. It can be classified into three main categories: recognition based graphical password, recall based graphical password and cued-recall. In recognition schemes users need to recognize the images in a right sequence, recall schemes need to recall something that he/she has created during registration phase and final, cued-recall provide users with some clues to recall a password, registered before during registration phase (Oorschot and Wan, 2009; Khan *et al*., 2011; Pawar *et al*., 2015). The cued-recall schemes are divided into pass point, Cued Click Point (CCP) and Persuasive Cued Click Point (PCCP) (Mathew and Thomas, 2013).

In this study, we present a new approach to strengthen text password by generating graphical patterns of password from Qwerty keyboard which is called in this study Keyboard Based Graphical Password (KBGP). This approach satisfies the following contributions:

- Make use of all keys on the keyboard for authentication process
- It robust and resistance against brute force attack
- It depends on user pattern imagination rather than memorization. The short password is easy to remember but it helps attacker to gain access them through brute-force attack
- It generates huge numbers of patterns from the Qwerty keyboard
- The proposed method builds based on a mathematical formula and measuring distance that uses in other approach such as data mining clustering and classification

Comparison of authentications schemes: In this study authentication schemes are compared in term of security,memorable, cost, usability, Graphical User Interface (GUI) and time to login in Table 1. Usability means the system should be easy to use, time to login, time to register, accuracy and reliability. Security refers to the probability for the attacker to break down the proposed method (Shay *et al*., 2016).

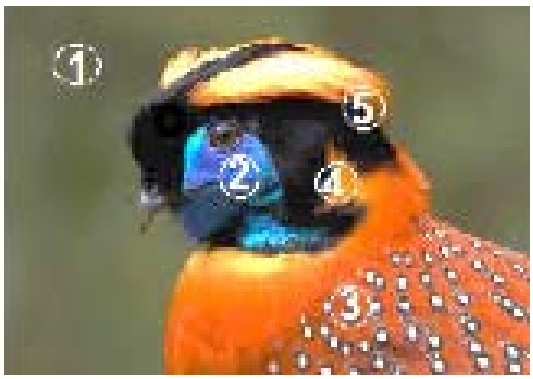

Fig. 2: Pass point graphical password

Fig. 3: Cued click point graphical password

The following pictures show the graphical pass point and Cued Click Point (CCP) in Fig. 2 and 3, respectively. In the Persuasive Cued Click Point (PCCP) shuffle and viewport functions are used. In addition, one image is used to select pass point in CCP while five or more images are used in PCCP.

Literature review: Table 2 shows some related research to the proposed system. It is presented the related research in terms of the method used, attack domain,

Table 2: Summary of related works

Paper work	Methods	Attack domain	Performance evaluation	Successful rates
Sahu (2015)	Graphical password using Cued click-points	Surfing attack	Tolerance and success rate	Moderate
Singh and Bomanware (2015)	Improved Ppersuasive Cued Click Point (IPCCP) with fingerprinting	Hotspot attack Shoulder surfing attack	Usability and security with 20 users	Moderate
Saeed and Umar (2015)	Graphical password using color image and color balls	Shoulder surfing attack	Feasibility	Moderate
Kayem (2016)	Recall and cued recall graphical password	Shoulder surfing attack	Usability memorability and security	Moderate
Anjitha and Rijin (2015)	Captcha as gRaphical Passwords (CaRP) with motion-video based CAPTHCA	Shoulder surfing attack Online attack Guess attack	Usability and security	High
Narhar and Joshi (2015)	Persuasive Cued click Point (PCCP) and fingerprinting biometric nail plate	NA	False Acceptance Rate (FAR) and False Rejected Rate (FRP)	High
Bianchi *et al.* (2016)	Graphical password using PassBYOP: Bring Your Own Picture scheme with live video	Shoulder surfing Camera based Observation Malware	Reliability Usability and security	High
Kolekar *et al.* (2015)	CaRP based recognition attack and recall schemes by using clickt text, animal grid, textpoints 4CR and shuffle text	Shoulder surfing attack Chosen-Pixel Attack (CPA) Key logger Software attack	Usability and security	Moderate
Haque *et al.* (2015)	Dynamic keystroke authentication scheme based on statistical approach	NA	False Acceptance Rate (FAR) and False Rejected Rate (FRP)	High
Jog and Student (2016)	Cued recall graphical password using fake cursor	Shoulder surfing attack	Success rate in term of percent	Moderate
Bhand *et al.* (2015)	Cued click point using image	Shoulder surfing attack	NA	Moderate

performance method and successful rate. Performance method includes usability and security. We classify the successful rate into three types: high, moderate and low. The most studies are presented graphical password based on different approach and in different media. The graphical password gain rapid interest because pictures can be remembered better than textual password and resistance to brute force-attack. In addition, bio-metric authentication techniques are slow, high cost and unreliable while the object based method is useless in case of losing the object (token).

MATERIALS AND METHODS

The propose model: The proposed approach handles the authentication Keyboard Based Graphical Password (KbGP) as a set of enclosed geometric shapes. Practically, the KBGP is a series of keys presses where each keyrepresent a node in a geometric shape within the set of shapes. The simplest KBGP is a set of one geometric shape that starts and ends in a unique node.

The geometric shape is consisted of n nodes and n edges since it is an enclosed shape. Mathematically, this n nodes shape is represented by a set X such that: $X = \{x_1, x_2, \ldots, x_n, x_{n+1}\}$ where none of the elements of X is repeated except the latest one, i.e., $x_{n+1} = x_1$ since it is the start\end node where the shape be completed and enclosed. Each two consecutive nodes draw a straight line of θ angle with the positive horizon (the line y = 0, x+); therefore, the KBGP is a set of consecutive angles rather than being a set of geometric figure sides. In another word, the geometric shape which can be constructed from the set X is in fact the set E which is the set of the edges between every two consecutive nodes in X such that:

$$E = \{x_1x_2, x_2x_3 \text{ and } x_ix_i+1, \ldots, x_nx_1\} \text{ and KBGP is the set of angles T such that: } T = \{\theta_1, \theta_2, \ldots, \theta_n\}$$

Where:

θ_i = The positive angle between the straight line

x_iX_{i+1} = The positive horizon

The way by which the geometric figure is exploited to be a robust and easily remembered authentication key is:

- The geometric shape is transformed into a set of points (keys presses events into (x, y) indices on the coordinates plane)
- Each two consecutive points are manipulated as a straight line that makes a positive angle θ with the positive horizon
- Eventually, the shape is a set of angles instead of being a set of fixed positions points or a set of fixed lengths lines

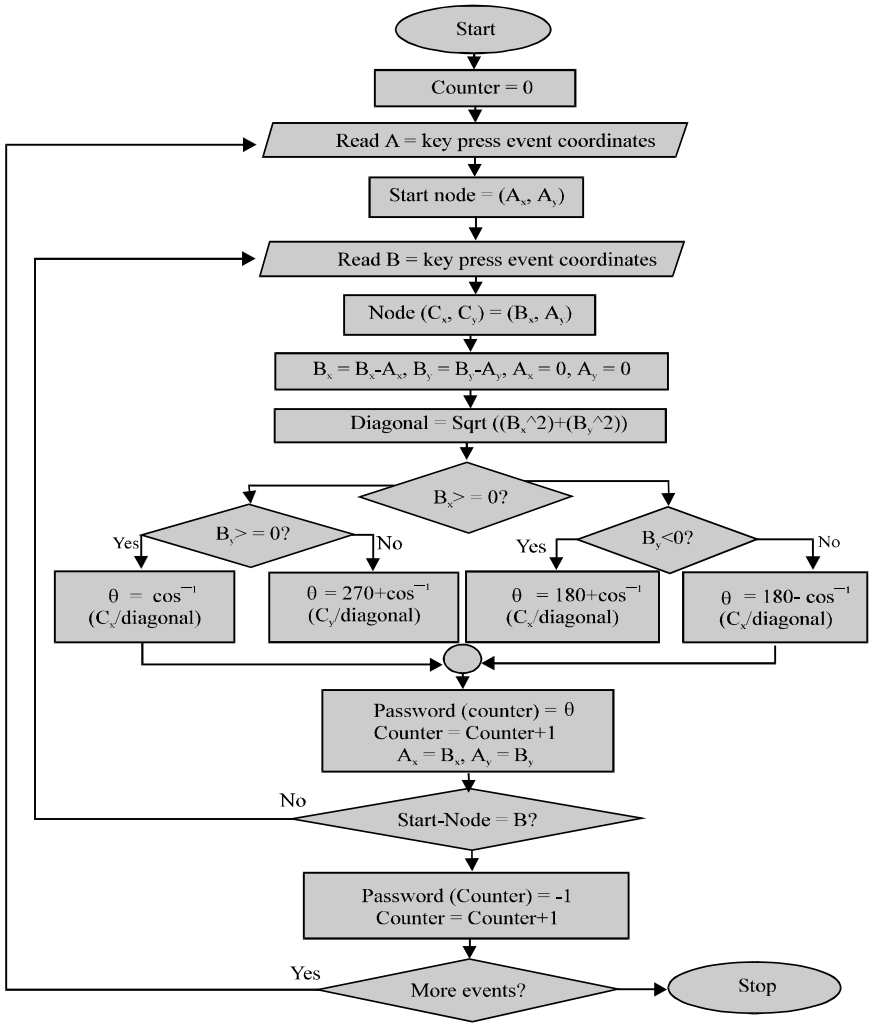

Fig. 4: Flowchart of KBGP authentication approach

- A user can authenticate his\her actual input by a similar input where the angles of the new input are similar to the angles of the actual shape; therefore, users can imagine their authentication keys as a set of shapes which can be larger, smalleror even on different coordinates positions

Algorithm 1 shows the main step of generating the KBGP into four main steps. Firstly, Pressing any key will consider as a node in two coordinate (A_x, A_y) to the second node (B_x, B_y). Secondly, the line between these two nodes will translate into point of origin (0, 0). Thirdly, we draw a third node ($C_x = B_x$, $C_y = A_y$) to consist a triangle between first, second and third nodes. Finally, we extract the θ angles from which quarter in the plane. These information is extracted during the registration phase that will be used next in the authentication process. The password will be saved in term of angles rather than textual from characters and others (Fig. 4).

During the authentication phase, the users need to remember the pattern instead of text and should satisfy the angles using an euclidean distance. User needs not match the same figure. For example, if the user forms a triangle from keyboard, it is not necessary to match the same size of previous triangle during the authentication. The main reason that we need the same angles that satisfy the triangle even if is big or small than the previous one during the registration phase.

Algorithm (Generating keyboard based graphical password):

Input: Series of key press events
Output: Geometric shapes defined by angles, array of passwords KBGP
Begin
Counter = 0
While not(Key_Press_Events is Empty)
Event_A = First_Key_Press_Event
Integer A_x = Horizontal Coordinate of Event_A
Integer A_y = Vertical Coordinate of Event_A

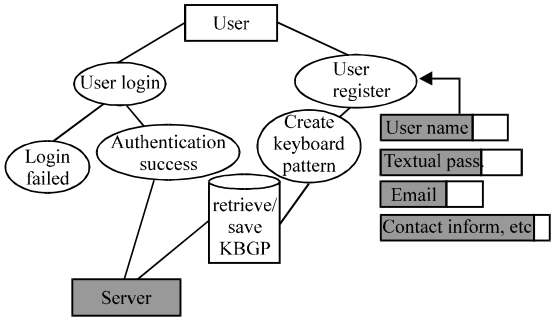

Fig. 5: Implementation of the proposed system

Start_node = (A_x, A_y)
Do
Event_B = Next_Key_Press_Event
Integer B_x = Horizontal Coordinate of Event_B
Integer B_y = Vertical Coordinate of Event_B
Translate A and B so that A matches the point of origin (0,0)
Bxnew = B_x-A_x, Bynew = B_y-A_y
A_x = 0,A_y = 0
Find Node C (the third Node of the triangle)
C_x = B_x,C_y = A_y
Diagonal = Sqrt((B_x^2)+(B_y^2))
Specify the location of the triangle ABC according to the x,y plane and calculate the angle of the diagonal AB
If(B_x> = 0 and B_y> = 0)// first quarter
θ = $\cos^{-1}$ (C_x/Diagonal)
If(B_x<0 and B_y> = 0)// second quarter
θ= 180-$\cos^{-1}$ (C_x/Diagonal)
If(B_x<0 and B_y<0)//third quarter
θ = 180+$\cos^{-1}$(Cx/Diagonal)
If(B_x>=0 and B_y<0)//fourth quarter
θ = 270+$\cos^{-1}$ (C_x/Diagonal)
Add θ to the Password KBGP [Counter] = θ
Counter = Counter+1
Move to the next node of the current shape
A_x = B_x, A_y = B_y
Until (Start_Node = B)
Assign the end of the current shape
KBGP[Counter] = -1
Counter = Counter+1
End while

The flow chart in Fig. 4 shows the main steps of this algorithm. We need to save angles values in database after extraction KBGP for next authentication. We use euclidean distance defined in Eq. 1 to match the saved angles with tested one. The distance value between the saved angles and the selected angles is authentication password:

$$d\left(\theta_i - \theta_j\right) = \sum_{i=1}^{x} \left\| \theta_i - \theta_j \right\|^2 \quad (1)$$

Where:
d = Distance between angles
θ_i = Angles in register phase
θ_j = Angles in authenticate phase
x = Number of angles

Evaluation methods: The proposed system consists of two main phases, registration and login phase. In registration phase the user needs to input his/her credential information like user name, password, email, contact information, textual password and then create keyboard based graphical password. Keyboard Based Graphical Password (KBGP) draw patterns from Qwerty keyboard such as triangle, square, rectangle, etc. The generated password is invisible to avoid shoulder surfing attack. Figure 5 shows the main registration and authentication process. The system is evaluated in term of usability and security.

RESULTS AND DISCUSSION

Security analysis and performance: The proposed algorithm can generate many possible graphical passwords. Password space can be defined as a set of all possible passwords that generated from the proposed algorithm. Resistance to brute-force attack such as dictionary attack depends on password space. We encode the standard alphanumeric qwerty keyboard in our system with a total keys of 87 including typewriters keys, function keys, enter keys, system keys, numeric keyboard, application keys and cursor control keys as in Fig. 6. The password space for our system is 87^N where, N is the length of password input. The password space in this research is defined as:

$$\sum_{N=1}^{L} (x * k * t)^N$$

Where:
L = Total number of key nodes
x = Total number of generated angles
k = Total number of edges
t = Time for login

The technology used in this program is implemented in Java 1.8 with MySQL and operating system is windows 7. The Software platform is JDK 8 from oracle. For example, to generate triangle keyboard based graphic password which is invisible as in Fig. 7, we need to press any three nodes in keyboard layout that generate the triangle such as (c, y, n and return to c). The pressing information are listed below in Table 3.

The successful login is depend on matching between the save angles and selected pattern angles using the euclidean distance that defined previously in Eq. 1. In another word, the strength of KBGP depends on the total number of nodes and angles between them.

Usability: Usability refers that the system is easy to use and implement by users. To carry out usability analysis, the login time for 20 users is recorded. The users have different skill to access for computer. We explained then the aim of this project. The login time represents the total time for the authenticated process to match the graphical password with database in server. In addition,

Table 3: Graphical password information during login phase

	Original (x,y) Layout points		Translation to point of origin (0,0)		
Input node	From	To	From	To	Angles
From Node1-2	(340, 320)	(490, 180)	(0, 0)	(150, -140)	316.95
From Node 2-3	(490, 180)	(550, 320)	(0, 0)	(60,140)	66.80
From Node 3-4	(550, 320)	(340, 320)	(0, 0)	(-210, 0)	180.00

Fig. 6: Layout keyboard based graphical password

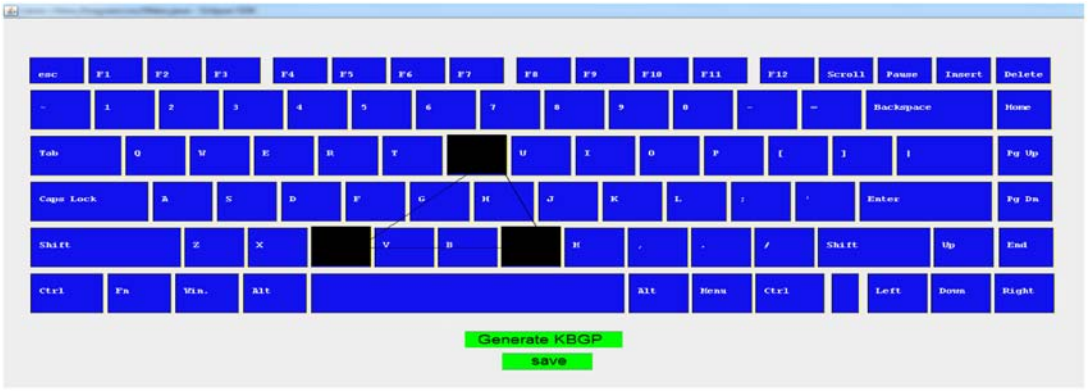

Fig. 7: Triangle password

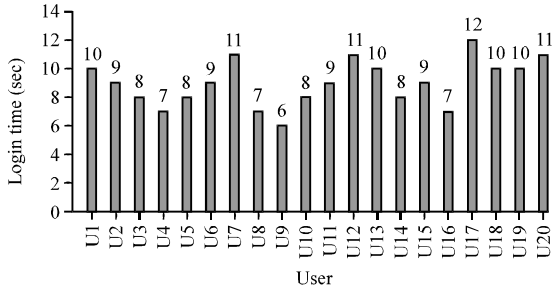

Fig. 8: Time of login

the time for user id and password is considered. Figure 8 shows the login time for 20 users. It can concluded from graph that the average time is 9 sec.

CONCLUSION

A keyboard based graphical password is designed and implemented as robust authentication approach using a mathematical formula. The proposed approach is necessary to overcome the drawbacks of traditional textual password that forgotten after period of time. The graphical password in this approach is invisible to avoid the shoulder surfing and capture attacks. KBGP consists of two phases, registration and login phases. In registration phase, user creates his graphical password and add information that will use in next login phase. We test system with 20 users in term of usability and security. It is clearly shown in the results that the brute force

attack takes time to analysis and breakdown the KBGP technique. In addition, the login time to use the system is very small compared with other authentication approaches.

RECOMMENDATIONS

For future research, it is necessary to apply the proposed system with mobile environment to be used as a hybrid approach for authentication process. We need to make the usability of the proposed system easy to access by the users with mobile environment. The mobile will become the dominant device that will use by the people in the next future.

ACKNOWLEDGEMENTS

The researchers would like to thank university of Babylon, college of Information Technology for their supporting and help.

REFERENCES

Anjitha, K. and I.K. Rijin, 2015. Captcha as graphical passwords-enhanced with video-based captcha for secure services. Proceedings of the 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), October 29-31, 2015, IEEE, Kannur, India, ISBN:978-1-4673-9223-5, pp: 213-217.

Bhand, A. V. Desale, S. Shirke and S.P. Shirke, 2015. Enhancement of password authentication system using graphical images. Proceedings of the International Conference on Information Processing (ICIP), December 16-19, 2015, IEEE, Mumbai, India, ISBN:978-1-4673-7758-4, pp: 217-219.

Bhanushali, A. B. Mange, H. Vyas, H. Bhanushali and P. Bhogle, 2015. Comparison of graphical password authentication techniques. Int. J. Comput. Appl. 116: 11-11.

Bhaya, W. and M.E. Manaa, 2014. Review clustering mechanisms of distributed denial of service attacks. J. Comput. Sci. 10: 2037-2046.

Bianchi, A. I. Oakley and H. Kim, 2016. PassBYOP: Bring your own picture for securing graphical passwords. IEEE. Trans. Hum. Mach. Syst. 46: 380-389.

Borkar, V.S. and P.C. Golar, 2015. Click based graphical password with text password authentication. Int. J. Comput. Sci. Network Secur. (IJCSNS.), 15: 76-79.

Gokhale, A.S. and V.S. Waghmare, 2016. The shoulder surfing resistant graphical password authentication technique. Procedia Comput. Sci. 79: 875-884.

Haque, M.A. N.Z. Khan and G. Khatoon, 2015. Authentication through keystrokes: What you type and how you type. Proceedings of the 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN.), November 20-22, 2015, IEEE, Aligarh, India, ISBN:978-1-4673-6735-6, pp: 257-261.

Jog, P.P. and A.B. Patankar, 2016. Graphical password authentication using a fake cursor approach. Int. J. Comput. Appl. 148: 35-40.

Kayem, A.V. 2016. Graphical passwords a discussion. Proceedings of the 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), March 23-25, 2016, IEEE, Cape Town, South Africa, ISBN:978-1-5090-2461-2, pp: 596-600.

Khan, W.Z. M.Y. Aalsalem and Y. Xiang, 2011. A graphical password based system for small mobile devices. Int. J. Comput. Sci. 8: 145-154.

Kolekar, V.K. and M.B. Vaidya, 2015. Click and session based captcha as graphical password authentication schemes for smart phone and web. Proceedings of the 2015 International Conference on Information Processing (ICIP), December 16-19, 2015, IEEE, Maharashtra, India, ISBN:978-1-4673-7758-4, pp: 669-674.

Kumar, M. T. Garfinkel, D. Boneh and T. Winograd, 2007. Reducing shoulder-surfing by using gaze-based password entry. Proceedings of the Symposium on Usable Privacy and Security (SOUPS), July 18-20, Pittsburgh, USA. pp: 1-7.

Lee, J.W. S.S. Choi and B.R. Moon, 2007. An evolutionary keystroke authentication based on ellipsoidal hypothesis space. Proceedings of the 9th Annual Conference on Genetic and Evolutionary Computation, July 7-11, 2007, ACM, London, England, ISBN:978-1-59593-697-4, pp: 2090-2097.

Mathew, G. and S. Thomas, 2013. A novel multifactor authentication system ensuring usability and security. Preprint, 2: 21-30.

Monrose, F. and A. Rubin, 1997. Authentication via keystroke dynamics. Proceedings of the 4th ACM Conference on Computer and Communications Security, April 1-4, 1997, ACM, Zurich, Switzerland, ISBN:0-89791-912-2, pp: 48-56.

Mule, S.S. H.B. Mali, 2015. Review on biometric authentication methods. Int. J. Adv. Res. Comput. Commun. Eng. 4: 252-255.

Narhar, U.K. and R.B. Joshi, 2015. Highly secure authentication scheme. Proceedings of the2015 International Conference on Computing Communication Control and Automation (ICCUBEA), February 26-27, 2015, IEEE, Pune, India, ISBN:978-1-4799-6892-3, pp: 270-274.

Oorschot, V.P.C. and T. Wan, 2009. TwoStep: An Authentication Method Combining Text and Graphical Passwords. In: E-Technologies: Innovation in an Open World, Gilbert, B. P. Kropf and M. Weiss (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-01186-3, pp: 233-239.

Pawar, T.S. R.G. Sawant, P.S. Bothe and S.A. Chopade, 2015. A survey on login authentication system using captcha as graphical password technquies. Int. J. Innovative Res. Comput. Commun. Eng. 3: 10131-10138.

Saeed, S. and M.S. Umar, 2015. A hybrid graphical user authentication scheme. Proceedings of the 2015 Conference on Communication Control and Intelligent Systems (CCIS), November 7-8, 2015, IEEE, Aligarh, India, ISBN:978-1-4673-7541-2, pp: 411-415.

Sahu, S.B. 2015. Secure user authentication and graphical password using cued click-points. Int. J. Comput. Technol. 18: 156-160.

Shanmugapriya, D. and G. Padmavathi, 2009. A survey of biometric keystroke dynamics: Approaches, security and challenges. Int. J. Comput. Sci. Inf. Secur. (IJCSIS.), 5: 115-119.

Shay, R. S. Komanduri, A.L. Durity, P.S. Huh and M.L. Mazurek *et al*., 2016. Designing password policies for strength and usability. ACM. Trans. Inf. Syst. Secur. (TISSEC.), 18: 1-34.

Singh, N. and N. Bomanwar, 2015. Improved authentication scheme using password enabled persuasive cued click points. Proceedings of the International Conference on Green Computing and Internet of Things (ICGCIoT), October 8-10, 2015, IEEE, Mumbai, India, ISBN:978-1-4673-7910-6, pp: 1394-1398.